Harvard Model Congress
Boston 2020

MANAGING VIRTUAL CURRENCIES AND THE DARK WEB

By Ryan Bayer

INTRODUCTION

Above is the display found on the Silk Road Website after its seisure by the FBI
Engadget.com

In October of 2013, the Federal Bureau of Investigation (FBI) shut down a surprising source of illicit trade that would redefine how the world viewed technology. Their investigation led them to discover that twenty-nine-year-old Ross William Ulbricht created an online marketplace and platform for individuals to anonymously conduct illegal trades on the internet. This marketplace, nicknamed The Silk Road, was discovered to be a channel for over $1.2 billion dollars in sales for over 150,000 customers.

Ulbricht, who went by the alias "Dread Pirate Roberts," received over $13 million in commissions for creating the platform and serving as its operator. In February of 2015, he was convicted of computer hacking, money laundering, and conspiracy to traffic narcotics. He is currently serving a double life sentence and an additional forty years without parole. The Court of Appeals upheld the conviction in 2017, while the Supreme Court declined to see the case in 2018.

Ulbricht's case is only the most widely known and tip of the iceberg when it comes to the types of activity that takes place on **the Dark Web**. The Dark Web is a part of the deep web or parts of the internet not accessible through a search engine. While primarily used for **drug trafficking**, other crimes such as selling stolen credit cards and hitman services were also found to take place on the site. In an age in which technology has allowed individuals to work outside of the reach of the law, how can the government protect Americans from the dangerous potential of the digital market?

The Dark Web *– content on the World Wide Web that is not indexed by search engines and requires specific software, configurations, or authorization to anonymously access*

EXPLANATION OF THE ISSUE

Drug trafficking *– the most popular classification for Dark Web websites, makes up an estimated 15% of all material in the Dark Web*

The deep web *— websites not accessible through a search engine. Said to be 400 to 500 times larger than the surface web*

The Onion Router (Tor) *— A system used to make it difficult to determine the IP address of a computer making a website request by sending site requests through three randomly chosen computers that each add a layer of anonymity*

Cryptocurrency *— a digital asset designed to work as a medium of exchange that uses cryptography to secure financial*

Historical Development

In the late 1990s the Naval Research Laboratory developed a system to ensure the anonymity of United States military personnel deployed abroad in intelligence operations. This system became known as **The Onion Router (Tor)** and was meant to make it difficult to determine the IP address requested of a website. The system sends a site request through at least three randomly chosen computers called relays. Jumping from one randomly chosen computer to the next adds a layer of anonymity similar to how an onion has many layers – the namesake of the system. The request leaves a final computer known as the exit relay in which hundreds of other requests might also take place. With hundreds of other computers going through this same computer and algorithms randomizing which relays users are sent to, this system allows individuals to be practically untraceable.

In October 2003, the military made the Tor accessible to others with specific software so as to protect information. In a sea of anonymous civilian users, military users were less likely to be found. Within a year, two problems with the Dark Web developed: how to navigate it and how to conduct transactions anonymously. These problems were solved with the Hidden wiki and Bitcoin. The Hidden wiki catalogues all Dark Web sites currently active and operating, like Wikipedia or other wiki websites. In addition, Tor-specific search engines specifically index hidden sites and sales.

Bitcoin was created in 2009 and is the standard currency of the Dark Web. The **cryptocurrency** has since become popular in the media as it has no central bank or administrator to monitor or verify its varying value. This final piece of the puzzle allowed individuals to make purchases anonymously, a major concern of the Dark Web, as it allows individuals to make purchases for illicit items such as drugs, child pornography, and weapons. Since the shutdown of the Silk Road, other darknet markets have also developed.

Scope of the Problem

An Unchecked Market

The anonymous websites on the Dark Web, when uncontrolled, are free to become the next Amazon of criminal activity. The few websites found have used their position of power to widely market stolen credit cards of innocent citizens, ransoms for hostages and kidnappings, pornography including the involvement of underaged children, cyber-crime kits to send malware and viruses, illicit and dangerous drugs, and prostitution and hitmen services. The

Over 30,000 websites are hacked every day through the Dark Web – a major threat to companies and computer users alike

***Whistleblowing** – exposing any kind of information or activity deemed illegal, unethical, or not correct within a private or public organization*

The image above shows the multilayers to the internet: the surface web includes anything you can find through Google or other search engines, the deep web includes websites and pages accessed only through passwords and encryption, while the Dark Web includes anonymous information
Hackernoon.com

***Hacktivism** – the use of technology to promote a political agenda or social change*

anonymity behind the Dark Web encourages these crimes and allows Americans to spread these dangers through technology.

Law enforcement has taken multiple steps to protect citizens and target criminals who endanger others through these crimes in public. However, the Dark Web allows individuals to profit from these crimes without a trace as to how to arrest them or make them pay for their crimes. The takedown of websites such as the Silk Road took years of research and multiple undercover agents to find the source. By the time police are able to arrest those involved with such as website, thousands of illegal transactions could have taken place.

Whistleblowing

One of the controversial aspects of the Dark Web is **whistleblowing**. Whistleblowing is the exposing of any kind of information or activity deemed illegal, unethical, or not correct within a private or public organization. Whistleblowing may seem like a heroic act, yet individuals can face a great deal of backlash for turning against an organization, and in the case of revealing state or government secrets, individuals may be considered traitors. The Dark Web allows individuals to anonymously provide information regarding the ethical choices of organizations and check the power of such institutions while not facing the drawbacks of arrest or a ruined reputation.

Examples of whistleblowers who used the Dark Web are Chelsea Manning, Julian Assange, and Edward Snowden. These three are cited by some to have published important information through the Dark Web that questions the ethical choices of the government in balancing both security and human rights. However, some believe that their choices put our government at risk and exposed their upper hand against other countries in terms of international relations and security.

Hacktivism

Another controversial aspect of the Dark Web is the use of this anonymous technology or hacking to promote a political agenda – better known as **hacktivism**. The aim of hacktivists is sometimes debatable and can be for a good cause such as to question a tyrannical politician or to encourage action by the government in issues they frequently neglect. However, their actions are typically illegal. The Dark Web empowers these individuals to use hacking and other electronic means by which to access information about individuals. Once again, the aspect of anonymity protects these individuals from facing punishment for their crimes.

The hacktivist group **Anonymous** has been widely known for the use of the Dark Web to target a number of government institutions not only in the U.S., but in foreign countries as well. Israel, Tunisia, and Uganda have all faced attacks as well as major

Anonymous *— A widespread group that anonymously uses the Dark Web and their talent to hack others in order to seize, release, or use information against others, typically as a form of protest*

companies such as Visa, PayPal, and MasterCard. The group frequently makes threats against business and government leaders in order to put their power in check, however, it can also be seen by their list of victims that sometimes their actions are for profit.

Congressional Action

Despite the fact that this threat has been around for over a decade, there has been little done in terms of legislation until recently. The Fight Illicit Networks and Detect Trafficking (FIND) Act was passed in the House in January of 2019. The bill directs the Government Accountability Office to report on the use of virtual currencies, such as Bitcoin, and online marketplaces in sex and drug trafficking, including those within the Dark Web. The bill has been cosponsored by Rep. Ann Wagner (R-MO), Rep. Brian Fitzpatrick (R-PA), and Rep. Cynthia Axne (D-IA). It was received in the Senate and has since been referred to the Committee on Banking, Housing, and Urban Affairs.

The Department of Defense (DoD) is estimated to put forward $1.8 million in 2013 and $1.2 million in 2015 to find areas in the Dark Web related to national security and the safety of American citizens

Another bill introduced in the House is the FinCEN Modernization Act of 2018. This bill requires the Financial Crimes Enforcement Network (FinCEN) to establish programs dedicated to research relating to financial technology involving machine learning, data analytics, and cryptocurrency. This will allow the government to learn more about the modern uses of computer technology to conduct transactions and online payments. Both of these bills are relatively new and neither of them have passed in both the House and the Senate. However, both only seem to address the issue of payment in the Dark Web and choose to attack the issue of monitoring cryptocurrency. Neither of the bills chooses to address the utilization of the Onion Router or provide capabilities for the government to monitor anonymous activity.

The official emblem of Anonymous - the figure is supposed to represent anonyminity and the leaderlessness of the the organization
Mashable.com

Other Policy Action

In February of 2018, former Attorney General Jeff Sessions announced the Department of Justice's (DOJ) creation of the Joint Criminal Opioid Darknet Enforcement (J-CODE) team. There has not been much information released on the team or how it will operate in order to protect their methods from computer experts. However, an FBI spokesperson stated that the team will focus on "disrupting the sale of drugs via the darknet and dismantling criminal enterprises that facilitate this trafficking." The creation of this new team has faced criticism from experts over the fact that eliminating any site that does traffic drugs or partakes in other criminal activity means that the site can simply resurface in another form. Particularly, they cited the seizure of the Silk Road and creation of a new similar site AlphaBay.

As ironic as it might seem that the United States Navy developed the Onion Router, the Department of Defense (DoD) is estimated to put forward $1.8 million in 2013 and $1.2 million in 2015 to find areas in the Dark Web related to national security and the safety of American citizens. DoD also uses the Dark Web to monitor foreign countries and gain anonymous information from individuals under tyrannical rule by other world leaders.

In addition to these efforts, the FBI continues to monitor the Dark Web and has a series of agents closely analyze the activity that takes place within the Dark Web. As websites such as the Silk Road have been taken down, it has become more difficult to find them and to apprehend those responsible for the heinous crimes that take place in the digital world.

IDEOLOGICAL VIEWPOINTS

Conservative View

As there has not been much legislation yet on how to solve this recent issue in technology, conservatives have not developed an official stance on how to solve the issue of the Dark Web. However, a few Republicans have provided similar viewpoints in regard to how to manage the virtual finances used to make online payments outside of the surface web.

Republican sentiment on cryptocurrency has been relatively positive. Sen. Mike Crapo (R-ID) claimed that cryptocurrencies "have the potential to improve processes for things like smart contracts, payments and settlement, identity management and even things yet undiscovered." Sen. Pat Toomey (R-PA) felt similarly regarding cryptocurrency and commented that it is a great alternative to central banking. Conservatives have a typical "hands off" attitude when it comes to the government control on the market and monitoring purchases. However, conservatives are also strong proponents against nefarious activities such as those regarding terrorism, the sex industry, and drug use. For these reasons, conservatives are certainly against the illegal uses of the Dark Web while trying to maintain the freedom of the market and advance use of technology.

Liberal View

Initial coin offerings *— ICO; A public offering in the funding or investing in a type of cryptocurrency*

Democrats have remained more critical of **initial coin offerings** (ICOs). Sen. Sherrod Brown (D-OH) commented that "families are losing their money by investing in ICOs" and that more protection should go to monitoring them. Sen. Elizabeth Warren (D-MA) stated that the challenge with cryptocurrency is "maintaining the protection of consumers" and ensuring that safe transactions are

taking place. While Republicans seem more focused on developing research into this topic, Democrats are quick to retort that we should put the protection of individuals before we further the development of such currency and come close to recognizing it.

TechFreedom is an interest group that lobbies on behalf of the freedom of internet users and aims to constrict government control over technology

TechFreedom.org

AREAS OF DEBATE

The main reasons for the widespread debate regarding the Dark Web and digital currencies is that the technology is advanced and far ahead of that of the government. Thus, Congress is unsure how to best regulate two innovations meant to increase the freedom of Americans. While the Dark Web and the cryptocurrency used on its sites have been linked to an array of criminal activity in regard to drug trafficking and child pornography, it also allows journalists, abuse victims, and activists to provide justice and anonymously speak out to the crimes of oppressors. The solutions listed below are just some of the many options available to you, and many of these solutions can work together. You should do outside research and think about how these solutions can be most effectively combined to craft nuanced legislation.

Eliminate the Dark Web

A majority of Americans do not involve themselves with the Dark Web whatsoever, and to solve the problem of eliminating crime on the dark web, it seems the simplest solution is to remove it entirely. The Dark Web seems to cause nothing but fear and allow for illegal transactions to take place. As such, Congress could create a policy that makes it illegal to own special software that allows individuals to connect to Tor. This would ensure that all individuals are punished and held accountable for trying to access the Dark Web, regardless of their intentions.

It is true that this would take undercover work by the FBI to stop such individuals, as access to the Dark Web and ownership of Tor providing software is all underground. However, this also eliminates the benefits of the Dark Web and stops those who use it for its benefits. This would mean that oppressed individuals cannot use the Dark Web to communicate with the outside world and possibly stop other crimes from happening. In addition, the military still uses the Dark Web in order to communicate and research foreign countries without revealing their identities. Without access to the Dark Web, the DoD would need to either provide an alternative for the military or let them go without this technology.

An important reminder about this policy is that even if Congress stops Americans from using Tor and the Dark Web, the technology is still accessible to foreign countries. Should Americans be stopped by Congress from using the technology altogether, it is still possible that

other foreign countries will still be able to use it. This means that civilian foreigners will have access to this anonymous technology, allowing them to still be a threat in the digital world. Despite this, a motivating thought may be that China, Russia, and Austria have already limited the freedom of their citizens to access the Dark Web for their own political reasons.

Political Perspectives on this Solution

Liberals have been focused on trying to protect innocent civilians from the horrors of the Dark Web. Meanwhile, conservatives typically aim to focus on protecting the freedom of Americans and protecting the role of the military. While this policy has not been officially brought up in the House or the Senate, it would face debate from liberals and conservatives in their balance of protecting Americans and their freedom.

Interest group, TechFreedom is focused on ensuring the government is hands off the innovations of the internet and advocates for legislators to put the priorities of individual Americans above a firmer grasp on handling such technology. The group frequently advocates against policies such as this one that would ensure fewer Americans have access to the anonymous technology provided by the Dark Web.

One of the possible solutions to combating the type of activity that takes place on the Dark Web is to develop a task force of computer experts dedicated to monitoring and finding methods to prevent such activity

Phys.org

Regulate Cryptocurrencies

Most of the problems with the Dark Web come from the transactions that take place on them. Another possible solution to protecting Americans from the dangers of the Dark Web is to regulate currency used in the transactions. This could mean a number of things: the government could aim to eliminate this technology, or it could officially recognize the technology to become its **central administrator**. This would require the government to dictate to the U.S. Department of Treasury to recognize the currency as well as keep an amount owned by the government to regulate transactions and booms in exchange prices. However, simply recognizing the virtual currencies only removes the problems that unfold with having such a digital currency, not necessarily stopping the type of transactions that take place online. By just regulating the cryptocurrency, it does not mean the government is anymore well equipped in stopping the problems that come from the transactions of the anonymous Dark Web.

Central administrator *– When the government has control over the supply of currency and can control exchange rates*

Political Perspectives on this Solution

Democrats have reiterated that their number one priority in tackling the issues of cryptocurrency is to ensure the safety of Americans and that innocent civilians are not tricked into losses over the complexities behind this currency. At the same time, conservatives support the freedom of Americans to make these

transactions. This type of policy would adhere to the demands of both political parties but only in terms of protecting Americans from unregulated virtual currencies and not unregulated anonymous websites.

The Bitcoin Association and the Chamber of Digital Commerce are two interest groups that are focused on ensuring the regulated use of cryptocurrency to preserve innovation while also avoiding money laundering. Major economists, however, are fearful of the fact that the government regulating cryptocurrency would only ensure that we as Americans continue to recognize and support the use of such money for criminal transactions.

Dictate Responsibility

The Dark Web has never been officially tackled by the United States government and it technically does not fall into a specific committee or agency's jurisdiction. One of the first steps taken by Congress might be to develop a task force dedicated to monitoring the websites used by the Dark Web. Part of the challenge in creating this team is to dictate funding as well as their level of responsibilities and capabilities as a government body. What committee or branch of the government would this team fall under? How would they track individuals given the anonymous nature of the websites?

While the FBI was able to take down the Silk Road and AlphaBay, it took years and dozens of undercover agents. However, perhaps having a team entirely dedicated to monitoring the Dark Web would ease this process and make it so the government can hold such individuals responsible for illegal transactions.

Political Perspectives on this Solution

With a more open-ended policy such as this one, Democrats and Republicans might not fit neatly into whether such a team should be created. However, **libertarians** might be more adamantly against such a team. Libertarians typically prefer less control by the government and would rather they do not infringe on the rights of Americans to freely and anonymously partake in business through the Dark Web. While such a team may seek to help monitor the legal and illegal activity of the Dark Web, there are those who would suggest that the government should not do anything at all. Individuals of this political philosophy and related interest groups would urge lawmakers to halt the creation of such a team as they see it as an infringement on the rights of Americans.

Libertarian *— An individual who practices the collected political philosophies dedicated to upholding liberty and freedom from the government*

Fund Research

The Dark Web is a complex issue, and it might take more years of understanding the problem before the government can come up with a proper solution. Another possible solution for lawmakers to solve

the problem is to fund research in the field of computer science in order to better understand how to come up with a way to monitor illicit transactions while also protecting the freedom of Americans. Congress is significantly behind technologically compared to many of the hackers on the Dark Web. It may be in the best interest of the country for the Federal Government to hire advanced hackers and computer scientists to fully understand the scope of what is happening on the Dark Web and offer suggestions accordingly.

Political Perspectives on this Solution

Some may argue that while this solution is more of a "middle of the aisle" and does not impede on any of the political parties or philosophy's goals, it does not necessarily lead to a proper solution. By the time the United States government develops one solution, it could be outdated compared to the skills and abilities developed by computer users in using the Dark Web. Another problem is how much money should be contributed in order to properly fund such research and who will provide the money. Conservatives in particular are concerned with fiscal responsibility and want to limit government spending as much as possible.

BUDGETARY CONSIDERATIONS

There are a number of budgetary considerations with any policy dedicated to solving this pressing technological issue. It costs a lot of money to pay computer programmers dedicated to government service as the average annual salary is of a computer programmer is $96,145 a year. In addition, it took years to take down the website the Silk Road and AlphaBay. Despite the work of the government, it will take time to individually take down these websites which means more money. The DoD already puts forth $1.2 million annually to take down websites and this clearly has not completely stopped these sites from coming forward. If the United States government is going to stop the Dark Web, it will certainly take a lot of money from Congress.

Also consider how any decision you make legislatively will impact the economy. Every policy has a direct cost which must be considered, but also think about how your choices will impact taxpayers and therefore the tax base. Millions of dollars are moved through the Dark Web every year. Think about how your solution will impact this flow of currency.

CONCLUSION

There are a number of issues presented with this topic that Congress must balance. The first is that Congress must determine how much control they wish to have over managing the technology surrounding the Dark Web. In addition, Congress must decide how it wishes to tackle the issue of currency used in virtual transactions that seem to flow easily across the border of the surface and Dark Web. Republicans feel the need to allow such a currency to have a presence in society and that it may be a worthwhile investment, but they also worry about enforcing the rule of law and protecting national security. Democrats, on the other hand, feel the need to protect everyday citizens from the unknown dangers of this currency and investing in it. While there may be a number of party lines and philosophies lawmakers must overcome when making a decision, they must also evaluate both the benefits and drawbacks of such technology.

Anonymity allows individuals to make illicit purchases and spread the use of crime without punishment from the federal government, however, it also allows for individuals to anonymously tackle corrupt systems and oppressors in the real world. In understanding and correcting the problems of the Dark Web and cryptocurrency, it is important to balance all of these ideas. The world is changing rapidly, and it is your job as a legislator to think critically about how the government can keep up in regulating this new virtual world. Without proper regulation, the internet can become a wild-west for illegal and illicit activity, but if the government oversteps, they may infringe on freedoms and prevent future technological innovation. Think critically as you balance these issues and craft your own legislation.

GUIDE TO FURTHER RESEARCH

It is important to conduct further research beyond that within this briefing, as the issue continually unfolds with the innovations in technology. An important aspect of this topic is to understand that there are many hoaxes and fears as to what happens on the Dark Web compared to what happens through the anonymous technology. It is a good idea to evaluate the trustworthiness behind sources and ensure they are factually correct. Solving this issue not only pertains to crime but the privacy of computer users. As such, it is important to read a few opinion pieces about the Dark Web in order to understand the public opinion regarding the matter. In order to check whether a site is trustworthy, look at who is publishing the

website, and verify to see if the information they are releasing can be verified by other sources.

Take time to look at your Congress person's website to see what their views are related to the dark web and cryptocurrency. If they have not explicitly spoken on the subject, look into how they feel about privacy, technology, and regulating markets. This may give you a starting point to think about how this philosophy would translate over to their feelings about the Dark Web.

GLOSSARY

Anonymous — A widespread group that anonymously uses the Dark Web and their talent to hack others in order to seize, release, or use information against others typically as a form of protest

Central administrator — When the government has control over the supply of currency and can control exchange rates

Cryptocurrency — a digital asset designed to work as a medium of exchange that uses cryptography to secure financial transactions

The Dark Web — content on the World Wide Web that is not indexed by search engines and requires specific software, configurations, or authorization to access

Hacktivism — the use of technology to promote a political agenda or social changes

Initial coin offerings — ICO; A public offering in the funding or investing in a type of cryptocurrency

Libertarian — An individual who practices the collected political philosophies dedicated to upholding liberty and freedom from the government

The Onion Router (Tor) — A system used to make it difficult to determine the IP address of a computer making a website request by sending site requests through three randomly chosen computers that each add a layer of anonymity

Whistleblowing — exposing any kind of information or activity deemed illegal, unethical, or not correct within a private or public organization

BIBLIOGRAPHY

"5 Inherent Risks of Cryptocurrency." FEI, www.financialexecutives.org/FEI-Daily/July-2018/5-Inherent-Risks-of-Cryptocurrency.aspx.

"A Public Policy Perspective of the Dark Web." Taylor & Francis, www.tandfonline.com/doi/full/10.1080/23738871.2017.1298643.

Buckley, Sean. "FBI Says It Located the Silk Road by Exploiting an Error with the Server's Login Page." Engadget, 14 July 2016, www.engadget.com/2014/09/05/how-fbi-found-silk-road/.

Budd, and Ted. "H.R.6721 - 115th Congress (2017-2018): FinCEN Modernization Act of 2018." Congress.gov, 6 Sept. 2018, www.congress.gov/bill/115th-congress/house-bill/6721?q=%7B%22search%22%3A%5B%22cryptocurrencies%22%5D%7D&s=1&r=2.

Chandler, Nathan. "How Anonymous Works." HowStuffWorks, HowStuffWorks, 12 Mar. 2013, computer.howstuffworks.com/anonymous.htm.

"Cryptocurrency Lobbying Groups: Money, Influence and Blockchain in DC." CoinIQ, 12 Oct. 2018, coiniq.com/cryptocurrency-lobbying-groups/.

Juan. "H.R.502 - 116th Congress (2019-2020): FIND Trafficking Act." Congress.gov, 29 Jan. 2019, www.congress.gov/bill/116th-congress/house-bill/502.

Kathryncasteel. "The DOJ Wants To Stop Drug Sales On The Dark Web, But That's A Tough Task." FiveThirtyEight, FiveThirtyEight, 27 Feb. 2018, fivethirtyeight.com/features/the-doj-wants-to-stop-drug-sales-on-the-dark-web-but-thats-a-tough-task/.

Knutson, Ted. "Elizabeth Warren Lays Into Crypto." Forbes, Forbes Magazine, 14 Oct. 2018, www.forbes.com/sites/tedknutson/2018/10/11/elizabeth-warren-cryptocurrency-is-easy-to-steal/#6f4380341249.

Owen, Gareth, and Nick Savage. "Empirical Analysis of Tor Hidden Services." IET Information Security, vol. 10, no. 3, 2016, pp. 113–118., doi:10.1049/iet-ifs.2015.0121.

Reilly, Claire. “Inside the Dark Web: A Guide to the Badlands of the Internet.” CNET, CNET, 30 Nov. 2017, www.cnet.com/news/darknet-dark-web-101-your-guide-to-the-badlands-of-the-internet-tor-bitcoin/.

“Techquake: The Biggest Threat to California's Tech-Sector May Lie Directly Beneath Its Feet.” TechFreedom, 23 Apr. 2019, techfreedom.org/techquake-the-biggest-threat-to-californias-tech-sector-may-lie-directly-beneath-its-feet/.

“US Government Funds Controversial Dark Web Effort.” CGTN America, 10 Oct. 2017, america.cgtn.com/2017/10/09/us-government-funds-controversial-dark-web-effort.

Weiss, Bari, and Damon Winter. “Meet the Renegades of the Intellectual Dark Web.” The New York Times, The New York Times, 8 May 2018, www.nytimes.com/2018/05/08/opinion/intellectual-dark-web.html.

Wilson, Emily. “One Year after Massive Takedowns, Dark Web Marketplaces Are Thriving.” The Next Web, 4 Mar. 2019, thenextweb.com/contributors/2018/07/21/dark-web-marketplaces-police-bitcoin/.

