Table of Contents

Director's Letter

Welcome distinguished delegates,

My name is Paula Chu, and it is my utmost pleasure to be the director of the UNODC cybercrime committee. Alongside the chairs: Dasnoor Sidhu/Jason Liu, and the rest of the dais team, we sincerely welcome you to TMUN 2025.

As a student in grade 12, I cannot fathom the excitement that I have to have the opportunity to end my high school career in Model United Nations by sharing a fascinating, yet necessary topic. I believe it is safe to assume that all delegates participating have access to the internet, and despite the sheer number of people who have access to it every single day, cybercrime is often an issue that is not considered as much as it should be. As such, I am thrilled to be sharing this topic and its intricate technologies involved with it to others. I am by no means a computer science or technologically based student; however, I personally do find the mechanics of how certain features of the digital world to be extremely interesting, and I hope that delegates feel this way too. I have done a committee regarding cybercrime before in the past and loved the research process of it, but was unsatisfied with how the committee ran, therefore I wish to redesign the committee with topics that are both intriguing and unique. The complexity of this subject is immaculate, and I can promise that nobody will ever be feeling bored when debating it at any time whatsoever.

In 2024, I attended a TMUN conference, and was left with new friends, knowledge, and helpful insights. As TMUN is hosted in Sheraton Hotel, the conference is presented as sophisticated and welcoming: definitely a major component to leaving an impression that will amplify the memories you will make here. Similarly to what I received from TMUN, I additionally hope that after this conference, all delegates are left with an unforgettable experience, whether it be your first, one of many, or last.

As I have stated previously: cyber related topics are extremely complex, therefore, it is understandable if delegates struggle with finding a considerable amount of information regarding their respective nation, especially if it is a peripheral one. There is also recognition of the vast amount of terms and concepts that will be discovered when researching these topics, hence results of easy misunderstandings and confusion. With that said, please remember that me and the rest of the dais are here to support you with every step you take, so do feel free to reach out. If you have any questions or concerns, I can be reached at **546chu@gmail.com**; remember no question is too big or small to ask.

Best regards,

Paula Chu
Director of the United Nations of Drugs and Crime (UNODC) Committee
546chu@gmail.com

Content Warning/Disclaimer

As this is a UNODC committee where the majority of sub-topics discussed are crimes, and their repercussions, there may be content that could trigger some delegates. This is particularly concerned with topic two, the dark web. Though extreme, gruesome, and sensitive issues are avoided in this background guide, what is discussed is by no means light information. There is additionally no absolute way to stop delegates from bringing up topics that should be avoided. Of course those delegates will be warned, but what is said and heard cannot be undone. If any of the following are personal triggers, this may not be the committee for you: drugs, murder, death, corruption, child exploitation, scams, frauds, violence, war, neglect of physical/mental health, suicide, terrorism, guns, and data breaches. The committee is laid out so that none of the issues will be discussed too in depth; however, the significance of maintaining delegate experience always comes first.

Furthermore, as this is a cybercrime committee, there will be quite a few complex technologies explored. That being said, in order for delegates to thrive, some may find that researching purely about their assigned nation's position and actions may not be enough. These technologies can be confusing, and to ensure the committee runs smoothly, and that delegates can come up with resolutions that are accurate and resourceful, there may be that additional piece of extensive research. All technologies are thoroughly explained in this background guide, but it is always good to explore further, as those unfamiliar with them may struggle regardless. Although there are a lot of major technologies to be learned; new terminology and uncommonly known technologies were avoided in consideration for a good conference experience, thus delegates should not feel discouraged to participate in fear of difficulty.

Finally, although it will be explained later on how everybody can easily access the dark web, and that it is relatively safe; it does not mean you should. Going on the dark web to see what it is like personally is not a necessary action required to be fully prepared for this committee. It is, however, understandable that there will always be people curious about it, and that is perfectfully normal, so if there are any delegates that choose to go on it: research further on it, and always take precautions. With that, stay safe and remember to make wise choices on your own accord.

Introduction to the Committee:

The United Nations Office on Drugs and Crimes is a branch that works towards international peace by contributing to the decline of injustices of all sorts: terrorism, human trafficking, the drug trade, cybercrime, and a plethora of others. It has been operating for over two decades with a commitment to offer assistance to member states; utilizing the help of transnationals to widen its networks in ensuring the reach of all regions across the globe.[1] In the case of this committee, the issue of cybercrime will be the main focus to be discussed and debated. The UNODC in particular for this matter, uses its specialization with criminal justice response to address the United Nations Sustainable Development Goals 16 (Peace, Justice, and Strong Institutions), and 17 (Partnerships for the Goals).[2]

In just four years, year 2029, it is estimated that the issue of cybercrime will cost the world approximately $15.63 trillion (US dollars), a startling number compared to the $9.22 trillion spent in 2024. This almost doubles the figures, proving it to be an extreme threat for the future.[3] With recognition of this: in 2019, the 74/247 Resolution, that was adopted by a General Assembly, was established to discuss the countering of criminal activity with technology. With this, the United Nations plans to draft a legally-binding international treaty; however, it has been over five years and negotiations are still ongoing. This is due to fear of the treaty being too broad. There are calls for more specification to confirm the protection of human rights, as a broad cybercrime law could unjustly subject individuals into apprehension.[4] Apart from the United Nations, the European Union, more specifically, the EUROPOL, and other superpowers have contributed greatly for this cause, but it is not enough. Although a considerable amount of cybercrime is committed in developed nations, as a majority of these criminals reside in places that have strong existences of technology, developing countries are arguably at the highest risk. Due to the restrictions in funding for technology in these nations, they typically have weak

---

[1] United Nations Office on Drugs and Crime. “United Nations Office on Drugs and Crime.” Unodc.org, 2019, www.unodc.org/.

[2] “Cybercrime.” United Nations : UNODC ROMENA, www.unodc.org/romena/en/cybercrime.html.

[3] Petrosyan, Ani. “Global Cybercrime Estimated Cost 2028.” Statista, 15 Nov. 2023, www.statista.com/forecasts/1280009/cost-cybercrime-worldwide.

[4] “Global Cybercrime Treaty: A Delicate Balance between Security and Human Rights | | UN News.” News.un.org, 25 Feb. 2024, news.un.org/en/interview/2024/02/1146772#:~:text=Recognizing%20the%20growing%20dangers%20of.

surveillance capacities, leading them to be the perfect grounds for cyberattacks.[5] In committee, these factors should always be considered. In spite of the fact that more technologically advanced nations (developed ones) are grappling with issues on how to deal with criminals that come from their countries, it is critical to remember that less advanced ones should not be neglected.

Topic 1 Overview - Cryptocurrencies

The concept of cryptocurrencies has existed for over forty years, with its first appearance of existence being in 1990, with David Chaum's eCash. This was a concept executed by him in hopes for a method of transaction that is both private and secure; however, his business went bankrupt. Since then, hundreds of other cryptocurrencies came into existence with Chaum's concept in mind, the most popular being: BitCoin, Ethereum, and Tether.[6] In the case of BitCoin, it was created in 2009, by an anonymous user after the name of "Satoshi Nakamoto" to introduce the world to a decentralized currency. This idea first emerged in 2008, as there was a financial crisis: the Great Recession. This was a major event that devastated the world, with it especially affecting North/South America, and Europe.[7] This crisis originally started in the United States, where the housing market bursted due to financial institutions providing risky mortgages to people in their country and to investors outside. The concept of BitCoin was considered as its decentralization creates the ability for individuals to rely more on themselves rather than financial institutions, to provide more security and stability.[8] Similarly, other cryptocurrencies were created with these good intentions. Unfortunately though, today, they are a widely debated concept that plagues the world, as people question whether they should be banned or not. Despite Chaum's hopes of creating a currency that helps protect individual's rights of privacy and increase stability, this idea has led to many misuses, resulting in a pool of crime.

Currently, cryptocurrencies are used for all sorts of illicit criminal activities: embezzlement, bribery, ransomware, money laundering, and purchases of illegal goods. Some

[5] United Nations. "Developing Countries Most Vulnerable to Cyberattacks – UN." UN News, 9 Dec. 2011, news.un.org/en/story/2011/12/397922.
[6] Reiff, Nathan. "Were There Cryptocurrencies before Bitcoin?" Investopedia, 26 Aug. 2021, www.investopedia.com/tech/were-there-cryptocurrencies-bitcoin/.
[7] "Why Was Bitcoin Created?" Crypto.com, crypto.com/bitcoin/why-was-bitcoin-created.
[8] Investopedia. "The Great Recession." Investopedia, 18 Dec. 2023, www.investopedia.com/terms/g/great-recession.asp.

nations have even started to use this currency to evade sanctions, or attempt to reduce damages of sanctions with them. Although it is difficult to calculate all the money that went through for illicit purposes with cryptocurrencies, due to its pseudonymous nature, there is no doubt about it that there are billions of dollars being used for unjust acts. In 2022 alone, there was a high of an estimated $39.6 billion of illegal transactions made, and seeing the patterns for the next few years, these trends do not appear to stop anytime soon.[9] Even though there is a lot of wrongdoing with cryptocurrencies, most nations are not banning it as they still see potential in this type of technology to create a better world. Whether it be hopes for a stronger economy, or better protection of human privacy, many are willing to see what this digital currency could offer. Regardless of whether it is banned or not, the fact is that people also see cryptocurrencies as an investment to make profit, so even if the government bans it, there will still be people finding illegal methods to bet on this currency. That being said, since this coin is decentralized, meaning that the government has no control over it, this then calls for new regulations, laws, and partnerships to ensure that this fiat currency does not get out of control.

DISCLAIMER: Although it is recognized that cryptomining is additionally another disadvantage with this currency, as it releases a great deal of greenhouse gas emissions- this is not the focus of the UNODC. The focus should mainly be about the goal of obtaining international peace and security. Do feel free to research it, since it is a fascinating topic, but it should not be considered in the sense of arguments when debating.

[9] Team, Chainalysis. “2024 Crypto Crime Trends from Chainalysis.” Chainalysis, 18 Jan. 2024, www.chainalysis.com/blog/2024-crypto-crime-report-introduction/.

How Cryptocurrencies Work

To be able to reach outstanding resolutions, it is crucial to thoroughly understand how this technology works. Cryptocurrencies are virtual assets secured by cryptography, which provides a system of storage and abilities to transmit data. As stated previously, this currency is decentralized, meaning that governments or banks do not have the ability to issue transactions made on these platforms, or operate them in any way. Instead, to confirm legitimacy, cryptocurrencies run on a system called blockchain, an arrangement of blocks that hold user/transaction data, which is exactly produced and revealed on computers using this technology. This is completely different from transactions with banks as they are the ones who process how much funds you have, validate them, and state the activities done on a single ledger that only the owner of the account can see. With blockchain, users can see one another's account balances to avoid scams, then personally go through with transactions, which their actions would then go on a ledger that everyone can see. Every transaction made is gone through a process called mining, which is an arrangement of computers that solve intricate mathematical problems to validate the cause forward. This concept of recording transactions across multiple devices, and mining, provides stronger data security. No matter the type of blockchain, whether it be public, private, permissioned, or permissionless, they all follow this ledger set up.[10] Unfortunately, due to the mass amount of proceedings made per day, along with the pseudonymity of cryptocurrencies, this is what makes it so difficult to capture criminals, despite the blocks.

When becoming a user of this tender, there has to be an investment made first. To have ownership of cryptocurrencies, it is simply done by purchasing it first through exchanges, brokerages, or payment services, then to put the newfound assets into a digital wallet. At this point, there are many risks that users must take into account: the inconveniences of the wallet, and the volatility of the coin. Starting with the digital wallet, it is a storage unit that can be accessed by the user through a password, thus when forgotten, the currencies locked in that wallet would unfortunately then be unable to be accessed. Furthermore, these wallets are able to be cyberattacked, resulting in the assets to possibly be stolen.[11] Secondly, cryptocurrencies are

[10] "What Is Cryptocurrency? | TD Direct Investing." Www.td.com, www.td.com/ca/en/investing/direct-investing/articles/cryptocurrency.
[11] Federal Trade Commission. "What to Know about Cryptocurrency and Scams." Consumer Advice, 21 Apr. 2021, consumer.ftc.gov/articles/what-know-about-cryptocurrency-and-scams.

extremely volatile. This means that it has no inherent value and that its worth is solely based on the demand for it. In a way, this could be compared to the stock market as its players take the risk to purchase stocks to gain profit whenever the value of their stocks go up; however, unlike stocks, crypto users do not own anything with definite value (in this example, like owning a part of a business through stocks), and it is most certainly difficult to logically make calculations for the demand of it. Take BitCoin for example, in November 2021, its value was around $65 000, but in just a year and a half, it dropped down to $20 000. Overall, despite the risks of losing an extreme amount of money, it is to be recognized that there are also the possibilities of gaining an absurd amount of money in just moments, which is why there are so many users today.[12]

Figure 1: Value of BitCoin Between 2020-2024[13]

[12] The Investopedia Team. "Cryptocurrency Explained with Pros and Cons for Investment." Investopedia, 15 June 2024, www.investopedia.com/terms/c/cryptocurrency.asp.

[13] CryptoPolitan, and CryptoRank. "Bitcoin trends mirror 2021, indicating potential downturn." *CryptoRank*, 23 Oct. 2024, cryptorank.io/news/feed/8d1b6-bitcoin-trends-mirror-2021.

Illicit Activities: Bribery

Bribery is the act of offering something of value to another to influence their actions for one's own personal benefits: a clear cut component to fueling the existence of corruption in the world. On October 31st, 2003, the United Nations Convention Against Corruption was adopted, and serves today as the only universal legally binding statement for anti-corruption. This convention works as a crucial tool to unite nations all across the globe with the common goal of dismantling criminalization, and strengthening international cooperation to create preventive measures and better law enforcement.[14] In articles 15 and 16 of this convention, it focuses on bribery, stating that states must enforce measures on those offering bribes, and those receiving them, as criminal offenses. It additionally states that this must also be done when foreign officials are involved with such acts.[15]

In the past, bribery was dealt by providence of physical money, because if it was not dealt by cash, it would have been traceable, as banks would have had the power to simply check the transactions made by the suspects for evidence. This is why criminals are choosing to use cryptocurrencies to take advantage of the pseudonymity of their bribes being sent out, or recieved. The Association of Certified Fraud Examiners found that 8% of fraud cases worldwide in 2021 used cryptocurrencies, in which 48% of these were bribes.[16]

Case Study: 2022 Use of Bribery by Officers in China

In 2022, two Chinese intelligence officers were found guilty of offering bribes to interrupt a US federal investigation. Their goal was to silence witnesses and to destroy any evidence that could be used in the investigation. This was planned to proceed with the use of cryptocurrencies as the beneficiary, however, they were caught by US authorities. This sparks questions about their root of intentions as the investigation being conducted involved a hacking

---

[14] "Learn about UNCAC." United Nations : Office on Drugs and Crime, www.unodc.org/corruption/en/uncac/learn-about-uncac.html.
[15] UNITED NATIONS CONVENTION against CORRUPTION. 2004, www.unodc.org/documents/treaties/UNCAC/Publications/Convention/08-50026_E.pdf.

[16] "Cryptocurrencies, Corruption and Organised Crime." U4 Anti-Corruption Resource Centre, 2022, www.u4.no/publications/cryptocurrencies-corruption-and-organised-crime/fullversion#the-role-of-cryptocurrencies-in-facilitating-corruption.

group called APT10, which has relations to the Chinese Ministry of State Security.[17] This case reflects the issue of cryptocurrencies and how corruption could be increased as a result of their existence.

Illicit Activities: Embezzlement

Article 17 of the United Nations Convention Against Corruption states embezzlement as "misappropriation or other diversion of property by a public official."[18] The convention, with its focus being anti-corruption, directs its attention on public officials; however, its definition fits perfectfully for embezzlement in general. To describe embezzlement in simpler words: it is theft, and cryptocurrencies provide new opportunities to steal millions of dollars from other crypto users. For example, a worker in a company may transfer company funds to their own personal funds, and be able to get away with it. This issue stands hand to hand with bribery in terms of criminals taking advantage of the pseudonymity to get away with breaking the law.

Illicit Activities: Money Laundering

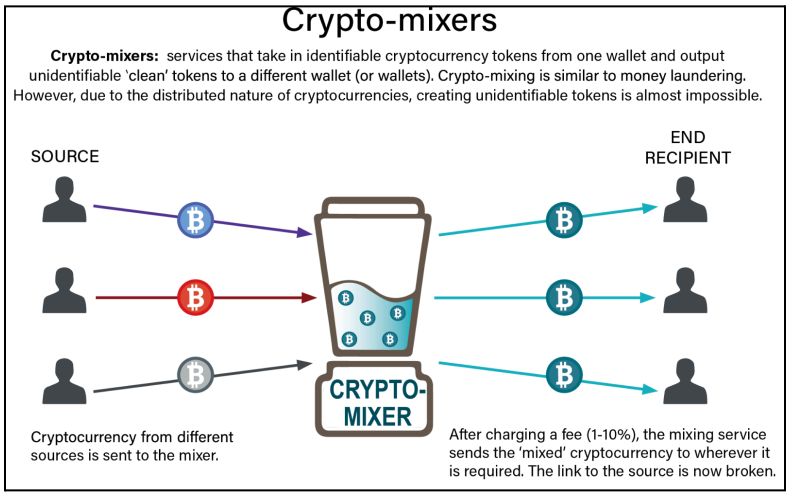
The existence of the digital world serves as a powerful tool for individuals to use for their own benefits, however, this unfortunately also includes criminals. As technology improves, more and more illegal activities that once occurred just in person, are now transferring online, for instance, money laundering. This procedure happens for two major reasons: to clean illegal fiat currency (turning illegal money into currency that can be used publicly without fear of authorities), and to mix up unlawfully gained cryptocurrencies. This choice of money is based on the offering of higher anonymity when using a specific type, like private coins, to have the ability to justify a sudden increase of balance, and for the low cost and speed when moving funds. For private coins, its benefits can include the ability to hide users' addresses, their balance, and origin of their assets. As for the justification of how an individual could suddenly gain a large amount of money, in a short amount of time, cryptocurrencies' growth rates are difficult to predict, and can grow up to 10,000% in moments, thus being able to justify sudden

[17] "Cryptocurrencies, Corruption and Organised Crime." U4 Anti-Corruption Resource Centre, 2022, www.u4.no/publications/cryptocurrencies-corruption-and-organised-crime/fullversion#the-role-of-cryptocurrencies-in-facilitating-corruption.

[18] UNITED NATIONS CONVENTION against CORRUPTION. 2004, www.unodc.org/documents/treaties/UNCAC/Publications/Convention/08-50026_E.pdf.

wealth easily. Despite all of this, it is still possible to track down the source of the money, hence the use of crypto-mixers. These mixers are technologies that put users' currencies into a blend, which stirs their coins up with other currencies from other sources, before giving back the same value of cryptocurrencies put in. This essentially makes it impossible to track the sources of the assets.[19]

Figure 2: Image is From the UNODC Depicting the Process of Crypto-mixers.[20]



Case Study: BitCoin Fog's Money Laundering Business

In 2021, a man by the name of Roman Sterlingov was convicted in the United States for running a BitCoin money laundering business on the dark web. This operated from 2011 until his conviction, in which he moved over 1.2 million BitCoins during that time; a value of approximately four hundred million dollars. His service, named BitCoin Fog, allowed criminals to launder their illicit funds, letting them get away with illegal narcotics, identity theft, cybercrime, and explicit material. As of now, BitCoin Fog's operation is considered to be the longest running cryptocurrency mixer, and stays as the highest record.[21] This example provides

[19] "Money Laundering through Cryptocurrencies." United Nations : UN Toolkit on Synthetic Drugs, 2023, syntheticdrugs.unodc.org/syntheticdrugs/en/cybercrime/launderingproceeds/moneylaundering.html.
[20] "Money Laundering through Cryptocurrencies." United Nations : UN Toolkit on Synthetic Drugs, 2023, syntheticdrugs.unodc.org/syntheticdrugs/en/cybercrime/launderingproceeds/moneylaundering.html.
[21] "Office of Public Affairs | Bitcoin Fog Operator Convicted of Money Laundering Conspiracy | United States Department of Justice." Www.justice.gov, 12 Mar. 2024, www.justice.gov/opa/pr/bitcoin-fog-operator-convicted-money-laundering-conspiracy.

insights into the dangers of crypto-mixers and how sought out they are by criminals. Moreover, it also creates issues for authorities to be able to properly track down the sources of money.

Illicit Activities: Ransomware

The issue of ransomware is a worldwide complication that is not uncommon, however it has gone up a notch with the rise of cryptocurrencies. In 2024, approximately 65% of financial institutions worldwide were struck with this catastrophe alone.[22] These figures do not include the impact on everyday citizens, government institutions, businesses, places of education, and hospitals that too struggle with this issue, proving it to be an extremely concerning issue. The process of ransomware is simple: cybercriminals will launch a cyberattack somewhere, block technological access for owners, or steal personal information from them, and then demand a sum that needs to be paid to have everything restored. Essentially, hackers are holding peoples' digital data up for ransom. With acknowledgement of the dangers of ransomware and how it could destroy organizations and livelihoods, there are still questions, and debates on whether ransoms should be paid or not.

When faced with detrimental threats by cybercriminals, individuals may feel like it is necessary to pay the demanding fee for their own safety; however, 80% of ransomware victims that do pay, are often faced with another future attack. It is then crucial to enforce better precautions into systems to avoid future mishaps, such as stronger forms of encryption.[23] This is exactly why it is often debated to not pay ransoms, because studies show that agreeing to criminal demands only influence them to keep going. Furthermore, funding these criminals only provides them with better tools to further expand their virtual power. In 2021, forty countries signed a US led initiative (Counter Ransomware Initiative) to not pay ransoms to cybercriminals, as they recognize the power that paying ransoms give to criminals. The agreement to this consisted of formulating a blacklist where signed nations would put together information of digital wallets that are being used to transfer ransomware payments. There then would be plans to use artificial intelligence to analyze blockchains to subdue the specific funds being transferred,

[22] "Global Financial Ransomware Attack Rate 2024." Statista, www.statista.com/statistics/1460896/rate-ransomware-attacks-global/#:~:text=From%202021%20to%202024%2C%20the.

[23] "Should We Pay the Ransom - the Most Common Ransomware Question." Ransomware.org, 12 Oct. 2021, ransomware.org/why-should-we-pay-the-ransom/.

to capture the perpetrators. Forward to 2023, there are now fifty signers, one being INTERPOL, for the fight against ransomware.[24] Overall, it is up to delegates to weigh the risks of paying ransoms or not, while keeping in mind on how to regulate the cryptocurrencies being used to make these payments.

Evasion of Sanctions

Nations with oppressive regimes, or nations that choose to take actions that disrupt international peace and security are often left to face the consequences of sanctions. This choice of action is to try to make political change by economically affecting its citizens of the targeted country in hopes that it would reach its governments.[25] Some countries may choose to follow suit and change their course of action, while some will find ways to withstand it, for example, with cryptocurrencies. Similarly to how criminals use cryptocurrency as a way to hide their transactions across the globe, likewise, nations can use this technology to do so as well. By using this currency, nations can keep their economies going by conducting trade with it, and, or by using the coin as a potential investment for profit to reduce the strain of the sanctions. Additionally, nations could pretend to throw up the white flag, but still continue disagreeable operations by using cryptocurrencies.[26] All in all, delegates should focus on finding new methods that will not only be able to reprimand individuals from using this currency illegally, but whole countries.

Case Study: North Korea Sanction Evasion

North Korea is a notorious illegal user of this digital coin, stealing approximately three billion dollars worth in Bitcoin from the past six years. In 2022 alone, North Korean hackers were able to steal $1.7 billion in crypto; an inarguable stat to prove the abilities of

---

[24] House, The White. “International Counter Ransomware Initiative 2023 Joint Statement.” The White House, 2 Nov. 2023, www.whitehouse.gov/briefing-room/statements-releases/2023/11/01/international-counter-ransomware-initiative-2023-joint-statement/.

[25] Bossuyt, Marc. THE ADVERSE CONSEQUENCES of ECONOMIC SANCTIONS on the ENJOYMENT of HUMAN RIGHTS. www.ohchr.org/sites/default/files/Documents/Events/WCM/MarcBossuyt_WorkshopUnilateralCoerciveSeminar.pdf.

[26] Office, U. S. Government Accountability. “The Effectiveness of Economic Sanctions at Risk from Digital Asset Growth | U.S. GAO.” Www.gao.gov, 27 Sept. 2023, www.gao.gov/blog/effectiveness-economic-sanctions-risk-digital-asset-growth#:~:text=For%20example%2C%20in%20October%202022.

cryptocurrencies. As for the use of this money collected, the nation's use of it is not only to evade sanctions, but to collect proceeds to fund its military, and illegal nuclear weapons program. The majority of the cryptocurrencies used are from crypto's Decentralized Finance space which allows for users to move funds around while bypassing regulated financial intervenors. To further increase the nation's ability to continue doing so, and to gain maximum profits, North Korea has been using Chinese money laundering, and Russian ransomware.[27] Overall, this case is crucial in the sense that it proves the capabilities of cryptocurrencies, and how nations can take advantage of it for their own economical benefits.

The Advantages: Potential Tool for Anti-Corruption

When considering the purpose for the existence of cryptocurrencies, and if they are still prevalent to use today, it is undeniable that it definitely is. The capabilities of blockchain can help provide people with identities, land rights, and avoidance of unjustified interference with banks or the government. According to the 2023 Corruption Perceptions Index, two thirds of the 180 countries scaled, got a score less than 50, in comparison to a hundred score (hundred is a clean score; meaning no corruption).[28] This is an extreme issue around the world as it risks individuals' human rights, thus calling for the need of cryptocurrencies. It is to be noted that the International Monetary Fund has a working paper that claims that blockchain would actually increase corruption; however, it was additionally stated in that same paper that the paper is an issue that is still being researched, and that it is posted publicly to fuel debate.[29]

Land rights are often lost in rural, poor communities due to entities of higher power being capable of undermining them by getting away with avoiding the providence of their respective land. For example, governments could simply grant land for development, and sustainability, but not enough that respects the rights of rural communities. This is where blockchain could be

[27] "ICYMI: At Hearing, Warren Warns about Crypto's Use by North Korea to Fund Nuclear Weapons Program and Evade to Sanctions | U.S. Senator Elizabeth Warren of Massachusetts." Senate.gov, 21 July 2023, www.warren.senate.gov/newsroom/press-releases/icymi-at-hearing-warren-warns-about-cryptos-use-by-north-korea-to-fund-nuclear-weapons-program-and-evade-to-sanctions#:~:text=warned%20about%20the%20national%20security

[28] "Infographic: Where Corruption Is Rampant." Statista Infographics, www.statista.com/chart/16834/countries-and-territories-ranked-on-perceived-public-sector-corruption/.

[29] "Crypto, Corruption, and Capital Controls: Cross-Country Correlations." IMF, www.imf.org/en/Publications/WP/Issues/2022/03/25/Crypto-Corruption-and-Capital-Controls-Cross-Country-Correlations-515676.

considered as a tool to use, as its ledger system provides proof of transactions and evidence of who a piece of land belongs to, without the variables of it being wrongly adjusted by banks/government. In 2016, a blockchain technology company, BitFury made a contract with the National Agency of Public Registry to create a blockchain to provide proofs of transactions and ownerships. This case happened in Georgia, in which the nation holds immutable land ownership rights.[30]

With concerns of government officials and financial institutions of taking advantage of individuals for their own interests, the decentralized blockchain can provide a space of unmissed identification, and clarity for belongings of assets. The technology provides information of users and their transactions that are promised to not be able to be tampered with. This is because cryptography ensures that once a transaction goes through, a block forms and gets added to the chain, making it so that transaction history can no longer be edited or deleted. Additionally, with blockchain having an encryption feature, it will always be secure.[31] There is a reason why money laundering crypto-criminals use mixers, and that is because they do not have the ability to falsify and fake their transactions. Overall, cryptocurrencies can be a method to provide people with a place where their finances will never be wrongfully dismissed or taken advantage of, providing them with a place where their identity is of the same value as everyone else.

The Advantages: Profit/Donations

There is a clear reason why people are so desperate to use cryptocurrencies despite the risks of it today, and that is for profit. Whether it be from trading, mining, yield-farming, staking, or selling: choosing to use cryptocurrencies is a resourceful investment that revenues a great fortune. Take all cryptocurrencies' value in 2021 for example, it hit $3 trillion dollars, approximately 0.717% of the total amount of money in the world. This amount of money categorized only took a little over a decade to compile, since cryptocurrencies came fully to existence, but the trends prove it to have great potential to rise even more as time goes on.[32]

---

[30] "Are Blockchain Technologies Efficient in Combatting Corruption." Www.u4.No, 2019, www.u4.no/publications/are-blockchain-technologies-efficient-in-combatting-corruption.pdf.

[31] "Are Blockchain Technologies Efficient in Combatting Corruption." Www.u4.No, 2019, www.u4.no/publications/are-blockchain-technologies-efficient-in-combatting-corruption.pdf.

[32] Tzanetos, Georgina. "Cryptocurrency Statistics 2022: Investing in Crypto." Bankrate, 8 July 2022, www.bankrate.com/investing/cryptocurrency-statistics/.

While many individuals take this as a chance to increase their own personal balances, other individuals or nations view this as a way to gain more funds to sustain themselves. For instance, people in poorer areas may use it to afford basic necessities to survive, while nations may use it to possibly lower debts, or extensive but necessary payments. Overall, cryptocurrencies hold the potential to provide a new method of gaining a large sum of money.

Case Study: Use of Cryptocurrencies During the Russian-Ukraine War

Following the Russian-Ukraine Invasion, many nations have sent Ukraine funds to fuel their war efforts in order to survive the attack. A month into the invasion, Ukraine legalized cryptocurrencies so that accounts can be made to receive donations, and for trading to generate profits. Considering the fact that Russia is additionally using cryptocurrencies to increase their funds for the war, this war, stated by the World Economic Forum, is the first major cyber-war between two countries. $212 million worth of donations in crypto were sent to Ukraine, with around $80 million being directly given to the Ukrainian government. Additionally, since cryptocurrencies are decentralized, this makes trading of them very proficient, generating enough money to protect devastated areas. All in all, cryptocurrencies play a major role in supporting Ukraine, whether it be through donations, or profits from trading.[33] Although, it is seen that crypto-currencies definitely can help an opposing side, it likewise can help those in need.

The Advantages: Assisting Developing Nations

It is a renowned fact that developing countries have many financial barriers that block them from progressing forward, thus the need for ways to bypass these obstacles, and cryptocurrencies may be one of the answers. By utilizing cryptocurrencies, it can fill the gaps of missing banking, be used to combat corruption, and to increase receivings of remittances. This is no surprise as the creation of BitCoin came to serve purposes similar to these.

There are currently only a few countries around the world that do not have a central bank: take Monaco, Palau, and Tuvalu[34] as three examples, however, there are many countries around

[33] "Why the Role of Crypto Is Huge in the Ukraine War." World Economic Forum, www.weforum.org/agenda/2023/03/the-role-cryptocurrency-crypto-huge-in-ukraine-war-russia/.

[34] "Countries without Central Banks 2020." Worldpopulationreview.com, worldpopulationreview.com/country-rankings/countries-without-central-banks.

the world that do have banks at all. In order to solve this issue, cryptocurrencies have been suggested to provide individuals with a fast and easy way to make transfers. This would help to solve the issue for many individuals who cannot receive banking due to not being able to meet their bank's minimum requirement balances.[35]

Having remittances sent over to developing nations is pivotal for individuals as it encourages education, provision of healthcare, funds for food, and for any other possible necessities one may need. In 2022, remittances sent to these nations rounded to approximately $636 billion, creating questions on how impoverished places would look without them. Seeing the necessity of these funds, the World Bank makes it one of their goals to increase these transfers of money to ensure that poverty can diminish.[36] Cryptocurrencies provide easy and quick movements of money internationally with low transfer fees. Furthermore, this technology can be reached to anyone, including those with no financial institutions/banking, making it extremely resourceful and inclusive for all. It has been reported that a fourth of Americans who send money digitally to another country have tried using crypto, and many see it as their most common payment method for this as well.[37] Additionally, nations that have the most crypto users are from South America, Africa, and Asia as those nations are heavily populated with individuals that are financially stricken, thus proof or recognition for the potentials and uses of cryptocurrencies.[38]

---

[35] "Unbanked: What It Means, Statistics, Solutions." Investopedia, 2024, www.investopedia.com/terms/u/unbanked.asp#:~:text=The%20main%20reason%20for%20being.

[36] "Remittances Are a Critical Economic Stabilizer." World Bank Blogs, blogs.worldbank.org/en/voices/remittances-are-critical-economic-stabilizer.

[37] CRYPTO and REMITTANCES 2. assets.ctfassets.net/c5bd0wqjc7v0/PX9g1EAnHHAKlCg1zHCwX/f9dde71351c320a15fc4eecff83e14e8/Crypto___Remittances.pdf.

[38] "Cryptocurrency Adoption by Country 2020." Statista, 2023, www.statista.com/statistics/1202468/global-cryptocurrency-ownership/.

Questions to Consider

1) Considering the risks of cryptocurrencies, instead of creating regulations, should they just be flat out banned? If not, what regulations can be created?

2) Should cryptocurrencies be considered as a legal tender?

3) Should cryptocurrencies remain decentralized?

4) How does your nation use cryptocurrencies? Is it favored or frowned upon?

5) Do cryptocurrencies affect the economy in a positive or negative way?

6) What measures can be taken to balance the provision of privacy by cryptocurrencies and criminal activities?

7) To ensure that all the risks of cryptocurrencies are taken into account for investors, should there be digital literacy programs?

8) What technology advancements, or science can be used to detect criminals through pseudonymity?

9) How can international cooperation help regulate cryptocurrencies?

10) Do cryptocurrencies have potential powers to help combat inflation? If so, can it potentially help reduce crime, as some people who commit them are due to being financially unstable?

Topic 2 Overview - The Dark Web

The infamous dark web: known for its digital blackmarket and illicit activities. A place on the internet which is heavily monitored and raided by governments to undermine criminals and their wrongdoings. Though notorious for these factors, it is not actually what most individuals think it is, and it definitely is not a place made just for criminals. The dark web is a place to provide individuals the privacy that they deserve as human beings, and a place for journalists and activists to be able to speak out on critical issues. Daily, there are approximately five million people active on this web,[39] in which only 6.7% actually use it for malicious intentions, evidently debunking the stereotypical image of this part of the internet.[40] Despite the low figures, that small percent still contributes to the billions of dollars processed through illegal markets, which provide goods and services that terrorize the world.

It is true, the dark web holds all sorts of criminals and vendors who traffic drugs, arms, humans, and sales of all sorts of peoples' personal information (SINs, credit cards, etc,...). In 2021, the total value received from these dark markets amounted to about $3.1 billion USD, and $1.5 billion in 2022. Of the profits gained in 2022, it contributed to 0.24% of the world's cryptocurrency transactions. Dark web criminals are smart, and they understand that their anonymous status when using a dark web browser does not protect them if they choose to take actions that could potentially lead them to being caught, which is why purchases on this web are additionally made with cryptocurrencies. In spite of all the horrific activities happening within this web, it is actually legal in most countries, and is only really blocked in nations that apply a lot of censorship. In this committee, delegates will comprehend the crimes conducted throughout this net, debating on new laws and regulations to take down these illicit activities. While doing

[39] "Cybercrime." United Nations : UNODC ROMENA, www.unodc.org/romena/en/cybercrime.html.
cycles, This text provides general information Statista assumes no liability for the information given being complete or correct Due to varying update, and Statistics Can Display More up-to-Date Data Than Referenced in the Text. "Topic: The Dark Web." Statista, www.statista.com/topics/11491/dark-web/#topicOverview.

[40] Jardine, Eric, et al. "The Potential Harms of the Tor Anonymity Network Cluster Disproportionately in Free Countries." Proceedings of the National Academy of Sciences, vol. 117, no. 50, Nov. 2020, pp. 31716–21. https://doi.org/10.1073/pnas.2011893117.

so, delegates will also consider their position on whether their respective country has the dark web legalized (or should they, or not), and argue about whether it should still exist today. Furthermore, on a global scale, approximately 70% of people do not understand the dark web. This thus should make delegates question whether there should be a stronger spread of awareness for this topic, or if it should not be deemed necessary at all (since it is relatively safe, unless individuals purposely seek out the danger).[41] As a whole, all considerations must be made in regards to this topic to ensure that these crimes do not increase, human rights are continuously protected, and that the dark web's true purpose only remains.

NOTE: This committee, although recognizing the issue, will not cover illegal pornography or sexually explicit material, as the dark web does lean to distributing it with a focus being on minors. With recognition of the fact that the majority of TMUN delegates are minors, and how it may be a sensitive issue to discuss, as it could potentially lead to more triggers than other subjects, it should not be mentioned when debating. This is to also be considered for organ trafficking as it could also be far out of the comforts of some delegates.

[41] "Topic: The dark web." Statista, 29 Feb. 2024, www.statista.com/topics/11491/dark-web/#topFacts.

How the Dark Web Works and the History of TOR

To understand the dark web, it is necessary to first recognize the different parts of the web. People often assume that the sections of the internet go like this: first the surface web, next the deep web, and then last the dark web; however, this is not exactly true. Although it is true that the surface web does come first, as it is the part of the internet that everybody can access (public articles, social media, free websites, anything searchable), the other two parts often get misunderstood. The deep web is accessed by almost all internet users everyday, this occurs simply by going into any part of the internet that needs authorization. This can include examining bank accounts, logging into social media accounts, and using subscriptions: basically anything that involves a login, or proof of identity. The dark web is actually a small section in the deep web, and is not a separate entity on its own. In the case of authorization, using a dark web browser, such as TOR (The Onion Router) is how it can be accessed. Currently, the surface web

makes up about 5% of the internet,[42] and the deep web makes up about 95%, in which 5% of that is of the dark web.[43]

When individuals want to get onto the dark web, it is actually extremely easy for them to do so. The process is simple: a dark web browser needs to be downloaded (such as TOR), then to be connected to it, and then from there, the user would essentially be on the dark web. Once on the web, in the case of using TOR, they will know that they are on it when the domain suffix is no longer ".com" and is now ".onion".[44] Criminals use this web for the purpose of anonymity, as the browser has onion routing, which means that the user's data will then be encrypted through many layers, with their ip address constantly changing with nodes, as nodes decrypt the layers, to reveal a message, but only reveal enough to remain anonymous.[45] To understand why these sorts of browsers still exist today, and why they are typically legal in most countries, the history of TOR is a great example for an answer.

TOR originated from the United States where a Naval Research Laboratory developed it in around the mid 90s' to protect American intelligence online. It was only established for the public when realizing the abilities of this tool to protect people's rights of privacy and safety online in 2003. In 2006, it got picked up by a non-profit research organization called The TOR Project to manage it, with their goal "to advance human rights and freedoms by creating and deploying free and open source anonymity and privacy technologies." Currently, TOR remains funded by the US government; however, it is to be noted that direct funding does not mean that the state has a say in how this organization should operate, or have any influence over it, as TOR remains a non-profit organization on its own, with its own goals and beliefs.[46] With that, it is to be understood that these browsers still exist today because of the potential protection it could

---

[42] K, Jennifer. "The Surface Web, Deep Web, and Dark Web Explained - Active Intel Investigations." Active Intel Investigations, 10 Dec. 2022, www.activeintel.com/the-surface-web-deep-web-and-dark-web-explained/.

[43] Molinaro, Domenic. "Dark Web Facts Revealed: Myths and Stats about the Secret Web." Dark Web Facts Revealed: Myths and Stats about the Secret Web, Avast, Dec. 2023, www.avast.com/c-dark-web-facts#:~:text=No%2C%20the%20deep%20web%20is.

[44] "The Dark Web: A Definitive Guide | McAfee." McAfee, 5 Dec. 2022, www.mcafee.com/learn/the-dark-web-a-definitive-guide/.

[45] Ghimiray, Deepan. "The Dark Web Browser: What Is Tor, Is It Safe, and How to Use It." The Dark Web Browser: What Is Tor, Is It Safe, and How to Use It, 4 Aug. 2022, www.avast.com/c-tor-dark-web-browser.

[46] Greengard, Samuel. "Tor | Browser, Dark Web, & Function | Britannica." Www.britannica.com, 21 Feb. 2023, www.britannica.com/technology/Tor-encryption-network.

offer, and that the intentions of these browsers were never malicious. What needs to be banned and put under control are the criminals choosing to act with unlawful decisions on this web.

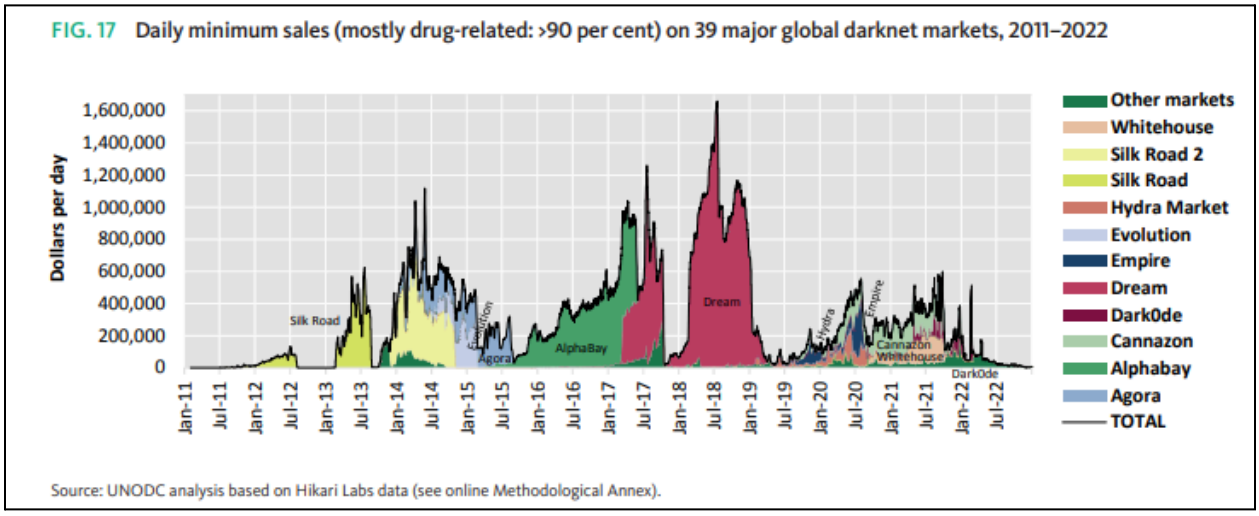
The Drug Trade

From cannabis, stimulants, opioids, prescription drugs, healthcare drugs, and others: the dark web is riddled with it all. Reported by the UNODC, it is estimated that of all illicit activities on the dark web, more than 90% of it is just from purchasing drugs, and this is based on the information from blockchain analytics from 2011-2022.[47] There are many markets on the darknet, as such, there are vendors who sell their goods on them. These vendors gain a reputation on this net through a review system to prove that they are not scammers and are genuine dealers. In order to gain market attention and actually be able to sell these drugs effectively, these sellers will first go on social media, and openly advertise their goods on the surface web. Next, those interested will go on the darknet to purchase the goods with cryptocurrencies, then the drugs will

[47] USE of the DARK WEB and SOCIAL MEDIA for DRUG SUPPLY. 2023, www.unodc.org/res/WDR-2023/WDR23_B3_CH7_darkweb.pdf.

be delivered through drops or post. Messenger services and forums online are additionally used to discuss sales.[48]

Figure 3: Timeline of Major Darknet Markets and Their Values[49]



Case Study: Operation SpecTor

Following Operation SpecTor, law enforcements were able to seize 850 kilograms of drugs, with 64 kilograms of it being fentanyl. This operation was coordinated internationally over three continents with the goal of controlling the fentanyl and opioid trade on the dark web. Seizures have been successful for several years through Europe, South America, and the United States thanks to the strong partnerships with law enforcements and the Joint Criminal Opioid Darknet Enforcement. The success shows as it reaches over a hundred federal operations and persecutions. This case is significant as it demonstrates the capabilities of international cooperation and/or partnerships to take down illegal businesses.[50]

---

[48] UNODC Tools and Programs to Address Illicit Online Drug Sales on the Open and Dark Web. www.state.gov/wp-content/uploads/2021/11/UNODC-Tools-and-Programs-to-Address-Illicit-Online-Drug-Sales-on-the-Open-and-Dark-Web.pdf.

[49] UNODC Tools and Programs to Address Illicit Online Drug Sales on the Open and Dark Web. www.state.gov/wp-content/uploads/2021/11/UNODC-Tools-and-Programs-to-Address-Illicit-Online-Drug-Sales-on-the-Open-and-Dark-Web.pdf.

[50] Office of Public Affairs. "Largest International Operation against Darknet Trafficking of Fentanyl and Opioids Results in Record Arrests and Seizures." Www.justice.gov, 2 May 2023, www.justice.gov/opa/pr/largest-international-operation-against-darknet-trafficking-fentanyl-and-opioids-results.

Prescribed and Healthcare Drugs

As access to healthcare is an issue to people in many nations, this leads to many individuals to make desperate decisions that results in them receiving treatment from illegal pharmacies, and providers. In 2015, there were approximately 27,500-40,000 illegal pharmacies running online. This then runs into concerns of the replacements of legitimate businesses and questions of how exactly these unofficial sources are getting their products. The majority of the types of drugs sold on the darknet are to reduce pain: both physically and mentally. Examples of psychiatric drugs sold can be hypnotics, anxiolytics, CNS stimulants, and antidepressants.[51] In 2020, a man named Cullen Roberts was found selling oxymorphone pills for the price of $90 a piece on the dark web. He was only caught when he was going through the process of selling the goods internationally, which then brought attention to the necessity of stronger shipping security for drugs: illegal or not.[52] Many of these drugs sold are advertised online to promise pleasure, relief, and euphoria to buyers, and as there is a lack of healthcare providers and mental health services available, people are turning to the darknet.

Case Study: Fake Vaccines Sold Online

As the COVID-19 pandemic hit and people were rampant on receiving their share of the vaccine, fake vaccines were created and were sold on the dark web to make profit. This was first recognized by the Interpol, with the Europol officially confirming it. Many vendors offered all sorts of COVID-19 related products: masks, testers, fabricated proofs of vaccinations, and vaccines. A major component that made these vendors very favorable was the fact that most of them offered worldwide shipping, and when struck by a global pandemic, this is extremely sought out for. From data collected from around 2020-2021, there were listings of 10,330 products related to the virus, with 248 of them marked as approved vaccines. This brings much concern as offers like these serve as a major threat to public health, whether they be legitimate or

[51] Cunliffe, Jack, et al. "Nonmedical prescription psychiatric drug use and the darknet: A cryptomarket analysis." International Journal of Drug Policy, vol. 73, Feb. 2019, pp. 263–72. https://doi.org/10.1016/j.drugpo.2019.01.016.
[52] "Darknet Drug Vendor Pleads Guilty to Distributing Illicit Prescription Drugs." Justice.gov, 4 Aug. 2021, www.justice.gov/usao-edva/pr/darknet-drug-vendor-pleads-guilty-distributing-illicit-prescription-drugs.

not.[53] With this case, the dark web is now seen as a clear threat to innocent individuals who may just be desperate for medical care.

The Arms Trade

Firearms being in the hands of the wrong people is a universally agreed terror. It is one thing for someone to attain them legally, and another if an individual has to seek them out on the dark web. Take the 2016 Munich Shooting for example: this was a case in Germany where an eighteen year old male shot nine dead, and got twenty-one people injured. He then proceeded to commit suicide before authorities could question his motives, however, it was suspected to be a terroristic attack.[54] This was all committed by a gun bought from the dark web. The incident then left the world wondering if the dark web could be a place that enables terrorist attacks.[55] Current findings found that the dark web is a distributor of both illegal and legal firearms, and have sales of quality ones for the same or lower price in comparison to buying them in person. As such, this furthers the growth of sales for arms, and could cause problems of maintaining control of exactly who has possession of one. Statistics show that firearm listings on the dark web have a popularity of 42%. Pistols are most commonly sold with 84% of arms sales being them, 10% to rifles, and 6% to sub-machine guns. Based on only 12 cryptomarkets, it is estimated that these sales make $80,000 per month. With all these findings, it is evitable that law enforcements must find a way to reveal the identities of sellers and buyers before these untraced arms get out of hand.[56]

According to studies by the Australian National University, there have been findings of vendors' pride in “ghost” guns. These are essentially arms that have been concealed by removal of their serial numbers or have not been registered. Along with these untraceable arms, there have also been 3D printed guns being sold online. People have been creating the main piece of guns through 3D printing, and vendors are selling different components and kits made out of

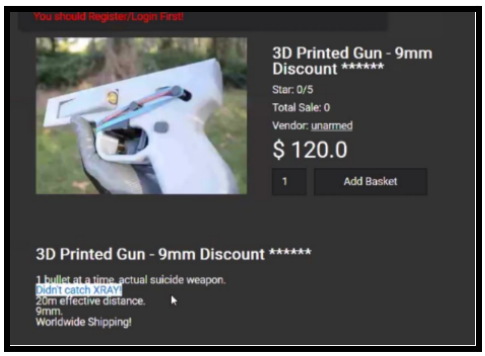
---

[53] Bracci, Alberto, et al. “Vaccines and more: The response of Dark Web marketplaces to the ongoing COVID-19 pandemic.” PLoS ONE, vol. 17, no. 11, Nov. 2022, p. e0275288. https://doi.org/10.1371/journal.pone.0275288.

[54] Callimachi, Rukmini, et al. “Gunman in Munich Kills 9, Then Himself, the Police Say.” The New York Times, 22 July 2016, www.nytimes.com/2016/07/23/world/europe/munich-mall.html.

[55] RAND Europe. “International Arms Trade on the Dark Web.” Rand, www.rand.org/randeurope/research/projects/2017/international-arms-trade-on-the-hidden-web.html.

[56] RAND Europe. “International Arms Trade on the Dark Web.” Rand, www.rand.org/randeurope/research/projects/2017/international-arms-trade-on-the-hidden-web.html.



harder plastics that vendors have been using. In 2019, the Australian Institute of Criminology found approximately 2124 weapons being sold between July and December. Collectively, there are major concerns around the world for the number of arms being provided to the wrong person online, with complications to trace these arms and identification of holders.[57]

Figure 4:
A 3D printed gun being sold on the dark web.
Image provided by the UNODC.[58]

Fraud and Scams

While the providence of illegal goods and services are typically fake, the same can happen within the dark web alongside real proceedings. As the anonymity of the dark web makes users have issues with identifying other users, people are taking advantage of this to commit fraud. For example, criminals have been stealing data from businesses and selling that on the market. By selling this data, other criminals can purchase it and then commit fraud using the information purchased. Overall, the process of fraud on the dark web is growing rampantly. The dark web is also the perfect underground area for people to pretend to be other people, without the victim realizing before it is too late. This can easily be done with for example, company

[57] "Glock Ghost Guns up for Grabs on the Dark Web." ANU, 22 Mar. 2021, www.anu.edu.au/news/all-news/glock-ghost-guns-up-for-grabs-on-the-dark-web.
[58] "Webinar on Investigations of Firearms Trafficking in Dark Web." United Nations : Office on Drugs and Crime, 2021, www.unodc.org/unodc/en/firearms-protocol/news/2020/Jan/webinar-on-investigations-of-firearms-trafficking-in-dark-web.html.

workers by stealing data through their organization, and then to use that information about them to proceed with malicious intentions.[59] In short, fraudsters are taking advantage of the dark web, and if their rate of growth does not deter down anytime soon, this can critically affect the reputations and finances of many future victims.

In addition to frauds, there are exceeding numbers of scammers surfing through the darknet today. In order for these sellers to gain people's information to provide frauds with material, it may be through scams. Vendors may attempt to inflict malware, send phishing emails, or make their "customers" leak their personal information in order to acquire it.[60] These threats suggest educating individuals on online safety, and of all the types of scams that criminals attempt to commit. Furthermore, there are scams on the dark web that consist of vendors advertising a product, getting someone to purchase it, but then not actually following through and providing the item/service. In this case vendors would lose face because of the review system; however, it still is being conducted frequently. In this case, regulations of the scams can be difficult to consider as they may not be necessary to handle as attempts to purchase illegal goods/services are going to end the buyer with repercussions regardless. Looking at a different case like purchasing goods that are not illegal like, scammers selling counterfeit goods to consumers (consumers thinking it is real), it would then bring incentives to end these scams completely.[61]

Distribution of People's Private Information

When exploring the specifics of what kind of personal information is being sold on the dark web, individuals might find credit cards, social security numbers, passwords, addresses, and details about their relatives. Essentially they can find all the materials needed to commit the perfect identity fraud, and in order to combat this, it is crucial to understand how these criminals are obtaining this information. Starting with credit cards, they can be stolen through data breaches, phishing attacks, and skimmers (devices placed in card readers to steal information). Once the card information is stolen, criminals would sell these cards in bulk to people who use it

[59] "How the Dark Web Is Making Fraud Easier." Www.aicpa-Cima.com, www.aicpa-cima.com/professional-insights/article/how-the-dark-web-is-making-fraud-easier.

[60] "How to Spot and Avoid Scams | Equifax UK." Equifax.co.uk, 2018, www.equifax.co.uk/resources/identity-protection/scam-avoidance-a-few-ways-to-help-stay-secure.html.

[61] Soldner, Felix, et al. "Counterfeits on dark markets: a measurement between Jan-2014 and Sep-2015." Crime Science, vol. 12, no. 1, Oct. 2023, https://doi.org/10.1186/s40163-023-00195-2.

to purchase goods/products to sell to others. In order to withstand these fraudulent transactions, it is crucial to implement stronger encryption and data storages, implementation of MFA, regulations of security, and educating/training people on how to handle/avoid these issues.[62] Data breaches are the main source of accessing confidential information, with social security numbers included. The impact of this being accessed is critical: people's personal, medical, and financial aspects of their life can be detrimentally affected.

Furthermore, it can be difficult for the victims to recognize that their information is being spread online when it is hidden by unindexed webs. With this issue being apparent, dark web monitors have been used to surf the web for fraudulent activities. When it becomes clear that an individual's social security number has been leaked on the web, they must take action, which is the following: freezing credit, checking bank statements, setting up fraud alerts, changing passwords, setting up two factor authentications, and contacting law enforcements. Since this is possible to occur to anybody, including those who are not familiar with technology: methods on how people can protect themselves from these attacks should be spread. This can also be considered with passwords, addresses, and other sensitive details that need to be protected, which can only be done if the right protocols are taught and implemented.[63]

Case Study: USDod Data Breach Class Action Lawsuit

A class action lawsuit was filed in the United States in 2024, when a hacker group USDod launched a major data breach, resulting in 2.9 billion people's information stolen from National Public Data. This group made claims for that alleged number, and further stated that they were selling this information on the dark web for $3.5 million. There were findings of a file containing 277.1 gigabytes of data of stolen information such as names, addresses, relatives, and

[62] Akasaka, Yuzuka. "Dark Web Credit Card Fraud: Detecting and Preventing Credit Card Fraud - Flare." Flare | Cyber Threat Intel | Digital Risk Protection, 15 May 2023, flare.io/learn/resources/blog/dark-web-credit-cards/.
[63] "My Social Security Number on Dark Web | Help!" Malwarebytes, 11 Apr. 2024, www.malwarebytes.com/cybersecurity/basics/ssn-on-dark-web?srsltid=AfmBOoqAQX0xftFTKbZ3dzkdQrhC_q7coUi7akWiHKVYbRvf8ul2C4Wo.

social security numbers.[64] This is proven to be problematic as this is one of the many cases of people having their information forcefully taken and sold.

Hitmen and Hackers for Hire

While a majority of transactions are processed for tangible items, it is also possible to pay for services such as hacking and murder. Starting with hackers for hire: as many recognize the detrimental capabilities of cyberattacks conducted by hackers, this leads to not just authorities seeking out these criminals, but also those with malicious intentions. Hackers can offer services such as MaaS (malware as a service), RaaS (ransomware as a service), PhaaS (phishing as a service), and DDoS (distributed denial of service). When making payments for these services, privacy coins are used, the most popular ones being Monero, ZCash and AXEL to clear traces of the illegal agreements. Similarly to drug trafficking, these hackers advertise themselves on the open web through social media before taking it to the dark web to make actual proceeds.[65] With these opportunities being available on the dark web, it is causing evidential issues with ensuring the protection of individuals on the internet, and declining the cyberattack rates.

Hitmen can likewise be hired in this manner of advertisement on social media, and then being paid through cryptocurrencies. A site on the dark web called Slayers Hitmen offers murder for $5000, while death by torture going for $50,000. Although this can be obviously seen as an issue as first-degree murder is being conducted with difficulties finding the perpetrators, studies have shown that these services are often scams. Many operators of these murder for hire sites often send proof of their legitimacy to skeptic buyers by creating videos that depict a death, but without necessarily killing anyone.[66] In this sense it brings questions to whether this is still considered something that needs to be seriously watched, and if it can be used as a tool for authorities to find potential murderers, and/or malicious buyers.

Figure 5:

[64] DeLetter, Emily. “2.9 Billion Records, Including Social Security Numbers, Stolen in Data Hack: What to Know.” USA TODAY, USA TODAY, 15 Aug. 2024, www.usatoday.com/story/tech/2024/08/15/social-security-hack-national-public-data-breach/74807903007/.
[65] Self, William. “Hackers for hire: The dark web, pen tests, and beyond.” Crowe, 7 Dec. 2023, www.crowe.com/cybersecurity-watch/hackers-for-hire.
[66] Popper, Nathaniel. “Can You Really Hire a Hit Man on the Dark Web?” The New York Times, 4 Mar. 2020, www.nytimes.com/2020/03/04/technology/can-you-hire-a-hit-man-online.html.

Screenshot from Slayers Hitmen[67]

Attack on Intellectual Property and Business Data

Issues arising from counterfeits and piracy interfere with intellectual property rights as they infringe on trademarks and contribute to copyright concerns. Essentially, dark web criminals are using intellectual properties without the permission from its owner, and this can often be seen with organized crime groups. This is an extreme concern as vendors are not just selling counterfeit items that can be considered materialistics, such as clothing, but also pharmaceutical products, and food. There can also be counterfeit products such as fertilizers, which instead of enriching the land, can instead be toxic and create detrimental problems for the environment. Furthermore, it will inevitably affect the economy as well as counterfeits can make consumers choose the cheaper options opposed to real, but more expensive options, which can lead to reductions of revenue in businesses and contribute to loss of jobs. These fake goods are often sold alongside real ones which makes it difficult to actually pinpoint their authenticity, especially when it is sold on the dark web. Estimated in 2017, 1.5-2.5% of listings are counterfeits. When Alphabay, a major marketplace was still around, approximately 10,000 of the items sold were not legitimate, which included fake IDs, and banknotes. Although a lot of ingenuine goods are sold on the darknet, most are advertised and sold on the surface web.[68] Regardless of where the products are sold, this problem is becoming very concerning as it threatens people's health, livelihoods, the economy, and the environment.

---

[67] Popper, Nathaniel. "Can You Really Hire a Hit Man on the Dark Web?" The New York Times, 4 Mar. 2020, www.nytimes.com/2020/03/04/technology/can-you-hire-a-hit-man-online.html.

[68] INTELLECTUAL PROPERTY CRIME on the DARKNET. www.europol.europa.eu/cms/sites/default/files/documents/darknet.pdf.

Following the concerns for the economy because of illicit activities from the darknet, businesses are at risk with their data being sold rapidly throughout the web. To start, inside business information can be stolen and sold in illicit marketplaces alongside employee information. In terms of negative effects for victimized companies, they can face damages to their reputation, and marketing, which is critical for their means of profit to help keep the economy moving. Furthermore, issues involving human rights are additionally brought into this when confidential information from employees of businesses are being sold with malicious intentions on the web. Moreover, there are hacking services, and hacking tools being sold on the darknet which can be effective for data breaches for these attacks. As long as a business sells goods, the business can have data stolen about their future goods and have counterfeits made of them, furthering the damages.[69] All in all, these are all stressful illegal issues that companies have to deal with, and it is up to international partnerships and law entities to undermine these attacks to protect these businesses and the people working in them.

Major Case Studies: Silk Road, Alphabay, Hansa

The Silk Road is considerably the most infamous darknet market: being the first modern market on the web to accept cryptocurrencies, it is one that every dark web criminal has heard of. Silk Road started in 2011, by its founder Robert William Ulbricht, who went by the name "Dread Pirate Roberts". He started this market because of his opposing political belief regarding drugs and other substances, which he believed that the government should not have a say on what

[69] Collins, Kathy. "What Risks Does the DarkWeb Pose to Businesses?" Secureideas.com, Secure Ideas, LLC, 10 Feb. 2023, www.secureideas.com/knowledge/what-risks-does-the-darkweb-pose-to-businesses.

people choose to put in their own bodies. Ulbricht first started selling light substances on his own, but eventually got vendors to sell their goods on his market. As time progressed, the market went from selling weaker drugs to counterfeit documents, hackers, hitmen, and heavier drugs. All transactions went through with Bitcoin. In 2013, when the FBI realized the existence of the Silk Road, the agency worked hard to bypass the anonymity of TOR and the use of cryptocurrencies, and was able to seize 144 000 Bitcoins (valued at $34 million at the time). Ulbricht's identity was also eventually discovered and his computer was seized by the FBI, in which he was found guilty and sentenced for life.[70] Despite the massive amount of money this market had made, the figures could have actually been much higher than that if not for James Zhong's stealing from the Silk Road. In 2021, Zhong was found to have over 50 000 Bitcoins (worth $3.34 billion back then), which he committed wire fraud for.[71] Overall, it is undeniable the impact that the Silk Road had on the world, with it gaining an insane amount of profits in just two years. Since its fall, the now inactive market has been the blueprint for future markets, inspiring people to start a massive monopoly similar to Ulbricht's.

The next massive darknet market that took over the world is Alphabay. Created by a Canadian citizen, Alexander Cazes, Alphabay was introduced into the darknet in December 2014 to provide illegal goods and services like Silk Road did. This market actually grew 5-10 times larger than Silk Road at its peaks, and had thousands of vendors selling each day to around 200,000 buyers internationally. The marketplace was a huge deal, and a massive problem for nations across the world to handle. In July of 2017, the United States (FBI), European countries, the Drug Enforcement Agency, Europol, and the Dutch National Police worked together to take down this operation.[72] Authorities with awareness that buyers and sellers of these markets would simply move on to another when one falls, had Hansa market under control while Alphabay was being monitored and raided. Hansa's infiltration was conducted by the Dutch National Police, where they monitored it for months to seize information on vendors and buyers before fully taking down the market. Hansa is a case where authorities decided to infiltrate and control before

---

[70] Frankenfield, Jake. "Silk Road Definition." Investopedia, 26 July 2021, www.investopedia.com/terms/s/silk-road.asp.

[71] U.S. Attorney Announces Historic $3.36 Billion Cryptocurrency Seizure and Conviction in Connection with Silk Road Dark Web Fraud. 7 Nov. 2022, www.justice.gov/usao-sdny/pr/us-attorney-announces-historic-336-billion-cryptocurrency-seizure-and-conviction.

[72] "True Crime Story - AlphaBay." United Nations : Office on Drugs and Crime, www.unodc.org/unodc/en/untoc20/truecrimestories/alphabay.html.

seizing, unlike Alphabay and Silk Road: demonstrating ways law officials can take advantage of these digital black markets.[73]

Use to Capture Criminals and to Find Future Threats

There are thousands of individuals seeking out illegal vendors and dealers for their unlawful purposes, and doing so successfully, despite the implications that come with it, this also means that there are many openings for law enforcements to capture these criminals. Just as criminals are able to meet and create deals with illegal vendors, authorities can also do this to view the risks and dangers that must be considered before raiding a darknet market. Though the anonymous nature of the web is still intact, authorities can at least access and follow the trails left by these criminals, since, afterall, digital footprint still exists. Organized by RAND, the corporation provides recommendations to identify these traces and risks: providing training for officers and investigators, better sharing of information, development of better forensic tools, better packaging inspections, and research on crime connections.[74] By following these suggestions, darknet markets can be tracked, data leaks can be recognized early on, and leads can be evaluated. Furthermore, many criminals on the darknet use a forum online to discuss their next moves and motives, so by collecting information through these and by using OSINT sources, these crimes can be recognized and considered for further legal action. Essentially, in order to realize future threats and to capture these criminals, every piece of information on them is critical, no matter how big or small.[75]

Case Study: International Cooperation to Capture Criminals

From July 2-5 in 2018, the Europol and the Eurojust, involved 60 experts from 19 countries to conduct a coordinated action week to track all the illegal goods and services on the dark web. There was identification of 247 high value targets, and there was providence of intelligence to the respective countries concerned with these subjects. By using these findings,

---

[73] Mack, Ryan. Combating the Illicit Goods Trade on the Dark Web. 2018, scholarworks.calstate.edu/downloads/1v53jz121.

[74] National Institute of Justice. “Taking on the Dark Web: Law Enforcement Experts ID Investigative Needs.” National Institute of Justice, National Institute of Justice, 15 June 2020, nij.ojp.gov/topics/articles/taking-dark-web-law-enforcement-experts-id-investigative-needs.

[75] Davies, Gemma. “Shining a Light on Policing of the Dark Web: An Analysis of UK Investigatory Powers.” The Journal of Criminal Law, vol. 84, no. 5, Sept. 2020, pp. 407–26. https://doi.org/10.1177/0022018320952557.

further investigations were able to be created, in which many of them led to successful captures. For example, in November, 2018, the Austrian Federal Criminal Police Office were able to follow leads to capture men that were suspected of selling drugs such as heroin, cannabis, and methamphetamine to people internationally. This investigation led to the findings of around $17 million in cryptocurrencies of profits to the main perpetrator of the sales. Overall, this case demonstrates the process of finding criminals, the importance of keeping records of every bit of information, and how dark web criminals are definitely able to get caught.[76]

Protection of Human Rights: Freedom of Speech

Article 19 of the Universal Declaration of Human Rights states that "everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers."[77] Despite the many illicit activities that the darknet is involved in, software like TOR, are crucial in protecting this human right. With many people living under oppressive regimes who want to speak out but cannot, such as whistleblowers, activists, and journalists, the darknet can be a pivotal tool. Typically in these severe states, governments will try to censor the content that their citizens can view and send out. This can be proved problematic as if people cannot retrieve crucial information about the world that is not meant to be confidential, they thus cannot make actual judgements and opinions, hence infringing upon their rights. Moreover, apart from trying to manipulate citizen opinions, governments could try to silence their people by reprimanding those who speak out on the atrocities happening within a nation, or by making it difficult to do so. This is why the dark web can be imperative as it provides people the ability to bypass censorship, and to speak out without fear of being caught.[78] As such, many of these repressive nations have darknet softwares blocked; however, with the use of bridges, it can usually be passed.[79] Major organizations such as the BBC and Facebook have

---

[76] "Global Law Enforcement Action against Vendors and Buyers on the Dark Web." Europol, www.europol.europa.eu/media-press/newsroom/news/global-law-enforcement-action-against-vendors-and-buyers-dark-web.

[77] "Universal Declaration of Human Rights." United Nations, 1948, www.un.org/en/about-us/universal-declaration-of-human-rights#:~:text=Article%2019.

[78] "[I-Lluminate] Exploring the Dark Web: TOR for Activism." Carleton.ca, 5 Feb. 2019, carleton.ca/align/2019/illuminate-exploring-the-dark-web-tor-for-activism/.

[79] "What Is a Bridge? | Tor Project | Support." Torproject.org, 2024, support.torproject.org/censorship/censorship-7/#:~:text=Bridges%20are%20useful%20for%20Tor.

created darknet websites for those in such regimes to use as a tool for their rights. In this sense, this web is proven to have a critical purpose for its existence today.

Case Study: Censorship in Iran

Due to oppressive circumstances in Iran, with a lot of its citizen's access to the internet being blocked and monitored, many individuals have turned to the dark web. Iran is one of the nations that currently have Tor blocked, forcing citizens to use bridges. After the death of Mahsa Amini, a woman who was held in custody for not wearing her hijab right, protests have been running rampantly. This made the government assert further control, seizing absolutely everyone that speaks against the nation. Since then many Iranians have been using Tor to spread awareness of the situation by posting information and videos. In recognition of this, The Tor Project created a guide in Farsi and English to teach Iranian citizens on how to access the browser in Iran.[80] All in all, Tor is being used as a pivotal tool to protect the humanity and lives of many people, not just Iran, but for all who have a need to speak out.

Protection of Human Rights: Right to Privacy and Access to Information

Following the growth of the digital world, privacy rights have been considered further as the fear of interference with human rights rises with it. Since 2013, the United Nations General Assembly and the Human Rights council has created many resolutions with the goal of undermining these concerns. According to an adoption from September 2019, A/HRC/RES/42/15, it states that "states should ensure that any interference with the right to privacy is consistent with the principles of legality, necessity and proportionality. It affirms that the same rights that people have offline must also be protected online, including the right to privacy; and it acknowledges that the use, deployment and further development of new and emerging technologies, such as artificial intelligence, can impact the enjoyment of the right to privacy and other human rights."[81] In most cases this would be referrals to the surface and deep web, and not necessarily the darknet. The browsers to access the dark web can be seen and used as a tool for protection of privacy because of its providence of anonymity; however, the fact

[80] Butcher, Mike. "As Iran Throttles Its Internet, Activists Fight to Get Online." TechCrunch, 5 Oct. 2022, techcrunch.com/2022/10/05/iran-internet-protests-censorship/.

[81] "International Standards OHCHR and Privacy in the Digital Age." OHCHR, www.ohchr.org/en/privacy-in-the-digital-age/international-standards#:~:text=Article%2012%20of%20the%20Universal,his%20or%20her%20honor%20and.

remains that there are many malicious criminals on this web that will find ways to interfere regardless. That being said, it is imperative to find a way to balance the good nature of the dark web, with the many dangers that are lurking in it.

In 2022, The Human Rights Council presented resolution 48/4, A/HRC/51/17, which made a focus on trends around that time frame in concern for privacy rights in regards to digital interferences. The resolution addresses the issues of hacking, restrictions on encryption, surveillance on public spaces, online monitoring, and human rights impacts and requirements.[82] All of these subjects are affiliated with the many different crimes conducted on the darknet, and despite this resolution covering the majority of it, there is always room for improvement and further protection. As the digital age continues to grow with new tools and technologies to be used for the better of the world, cybercriminals also gain more power and tactics to terrorize the world. In order to keep this age as something that protects and helps the world develop, it is inevitable that human rights, such as the right of privacy, must be protected first. Whether it be information on people's family members, addresses, social security numbers, passwords, or banking information, all of these things must be protected from data breaches or any other sorts of releases of confidential information.

Questions to Consider

1) Despite the illicit activities on the darknet, can nations find a way to take advantage of how the web works for better purposes?

2) Should dark web browsers still exist? Should they be legal/illegal? Are they okay to be used?

[82] Human Rights Council. documents.un.org/doc/undoc/gen/g22/442/29/pdf/g2244229.pdf.

3) What laws and regulations should be imposed for the digital world? Should there be ones specifically made for darknet criminals?

4) What should privacy mean for darknet users? How can the privacy of darknet users be furthered without the identification of malicious users becoming more difficult to find?

5) Should there be limited access for the darknet? For example: only for journalists, whistleblowers, and activists?

6) How can nations monitor illicit activities while maintaining the protection of privacy rights?

7) What does your given nation have in their laws, and acts in regards to cybercrime/cybersecurity, or the darknet?

8) What tools/technologies can be used to capture criminals?

9) How can goods/services be tracked from the dark web?

10) How can dark web transactions be monitored/tracked when they are done through cryptocurrencies?

Resources to Understand General Concepts of Cybersecurity/Cybercrime:

For understanding encryption:

- What is encryption? How it works + types of encryption – Norton

Reading and video on public/private keys:

- Public key vs private key: What's the difference? - MoonPay - MoonPay

- Public Key Cryptography - Computerphile - YouTube

Videos to expand knowledge on cybersecurity:

- What Is Cyber Security | How It Works? | Cyber Security In 7 Minutes | Cyber Security | Simplilearn - YouTube
- Cybersecurity for Beginners: Basic Skills

TED Talks:

- Cybercrime is the Next Pandemic: How to Prepare for it | Imani McHenry | TEDxSIUC - YouTube
- Profiling Hackers - The Psychology of Cybercrime | Mark T. Hoffmann | TEDxHHL

Further Research: Cryptocurrencies

Understanding crypto wallets:

- How Public and Private Key Work In Your Crypto Wallets

Understanding cryptocurrencies:

- Cryptocurrency Explained With Pros and Cons for Investment

- How Cryptocurrency ACTUALLY works. - YouTube

How blockchain works:

- How does a blockchain work - Simply Explained - YouTube
- Blockchain Facts: What Is It, How It Works, and How It Can Be Used

To further grasp the pseudonymous nature of cryptocurrencies:

- Is Cryptocurrency Anonymous? - YouTube
- Anonymity vs. Pseudonymity | Blockchain and Cryptocurrency Course: What You Need to Know | 2019

Further Research: The Dark Web

Overview/introductory video on the dark web:

- What's the Dark Web Really Like?

Site to understand the nodes used with Tor, and how Tor works:

- The Tor Network: A Guide to the Dark Web Browser

- The Ultimate Guide to Using Tor Browser Securely - YouTube

Video to strengthen understanding the perspective of a cyber criminal:

- Dark Web Questions Answered By A Former Cyber Criminal - YouTube

Videos to further explore the case studies:

- The Dark Web | Black Market Trade | Cyber Crime | Crime | Alpha Bay - YouTube
- The Most Illegal Business In The World: Silk Road

Works Cited

"[I-Lluminate] Exploring the Dark Web: TOR for Activism." *Carleton.ca*, 5 Feb. 2019, carleton.ca/align/2019/illuminate-exploring-the-dark-web-tor-for-activism/.

Akasaka, Yuzuka. "Dark Web Credit Card Fraud: Detecting and Preventing Credit Card Fraud - Flare." *Flare | Cyber Threat Intel | Digital Risk Protection*, 15 May 2023, flare.io/learn/resources/blog/dark-web-credit-cards/.

"Are Blockchain Technologies Efficient in Combatting Corruption." *Www.u4.No*, 2019, www.u4.no/publications/are-blockchain-technologies-efficient-in-combatting-corruption.pdf.

Bossuyt, Marc. *THE ADVERSE CONSEQUENCES of ECONOMIC SANCTIONS on the ENJOYMENT of HUMAN RIGHTS*. www.ohchr.org/sites/default/files/Documents/Events/WCM/MarcBossuyt_WorkshopUnilateralCoerciveSeminar.pdf.

Bracci, Alberto, et al. "Vaccines and More: The Response of Dark Web Marketplaces to the Ongoing COVID-19 Pandemic." *PLOS ONE*, edited by Federico Botta, vol. 17, no. 11, Nov. 2022, p. e0275288, https://doi.org/10.1371/journal.pone.0275288.

Butcher, Mike. "As Iran Throttles Its Internet, Activists Fight to Get Online." *TechCrunch*, 5 Oct. 2022, techcrunch.com/2022/10/05/iran-internet-protests-censorship/.

Callimachi, Rukmini, et al. "Gunman in Munich Kills 9, Then Himself, the Police Say." *The New York Times*, 22 July 2016, www.nytimes.com/2016/07/23/world/europe/munich-mall.html. Accessed 31 Aug. 2024.

Collins, Kathy. "What Risks Does the DarkWeb Pose to Businesses?" *Secureideas.com*, Secure Ideas, LLC, 10 Feb. 2023, www.secureideas.com/knowledge/what-risks-does-the-darkweb-pose-to-businesses. Accessed 31 Aug. 2024.

"Countries without Central Banks 2020." *Worldpopulationreview.com*, worldpopulationreview.com/country-rankings/countries-without-central-banks.

CRYPTO and REMITTANCES 2. assets.ctfassets.net/c5bd0wqjc7v0/PX9g1EAnHHAKlCg1zHCwX/f9dde71351c320a15fc4eecff83e14e8/Crypto___Remittances.pdf.

"Crypto, Corruption, and Capital Controls: Cross-Country Correlations." *IMF*, www.imf.org/en/Publications/WP/Issues/2022/03/25/Crypto-Corruption-and-Capital-Controls-Cross-Country-Correlations-515676.

"Cryptocurrencies, Corruption and Organised Crime." *U4 Anti-Corruption Resource Centre*, 2022, www.u4.no/publications/cryptocurrencies-corruption-and-organised-crime/fullversion#the-role-of-cryptocurrencies-in-facilitating-corruption. Accessed 31 Aug. 2024.

"Cryptocurrency Adoption by Country 2020." *Statista*, 2023, www.statista.com/statistics/1202468/global-cryptocurrency-ownership/.

Cunliffe, Jack, et al. "Nonmedical Prescription Psychiatric Drug Use and the Darknet: A Cryptomarket Analysis." *International Journal of Drug Policy*, vol. 73, Feb. 2019, https://doi.org/10.1016/j.drugpo.2019.01.016.

"Cybercrime." *United Nations : UNODC ROMENA*, www.unodc.org/romena/en/cybercrime.html.

cycles, This text provides general information Statista assumes no liability for the information given being complete or correct Due to varying update, and Statistics Can Display More up-to-Date Data Than Referenced in the Text. "Topic: The Dark Web." *Statista*, www.statista.com/topics/11491/dark-web/#topicOverview.

"Darknet Drug Vendor Pleads Guilty to Distributing Illicit Prescription Drugs." *Justice.gov*, 4 Aug. 2021, www.justice.gov/usao-edva/pr/darknet-drug-vendor-pleads-guilty-distributing-illicit-prescription-drugs. Accessed 31 Aug. 2024.

Davies, Gemma. "Shining a Light on Policing of the Dark Web: An Analysis of UK Investigatory Powers." *The Journal of Criminal Law*, vol. 84, no. 5, Sept. 2020, pp. 407–26, https://doi.org/10.1177/0022018320952557. Sage Journals.

DeLetter, Emily. "2.9 Billion Records, Including Social Security Numbers, Stolen in Data Hack: What to Know." *USA TODAY*, USA TODAY, 15 Aug. 2024, www.usatoday.com/story/tech/2024/08/15/social-security-hack-national-public-data-breach/74807903007/.

Federal Trade Commission. "What to Know about Cryptocurrency and Scams." *Consumer Advice*, 21 Apr. 2021, consumer.ftc.gov/articles/what-know-about-cryptocurrency-and-scams.

Frankenfield, Jake. "Silk Road Definition." *Investopedia*, 26 July 2021, www.investopedia.com/terms/s/silk-road.asp.

Ghimiray, Deepan. "The Dark Web Browser: What Is Tor, Is It Safe, and How to Use It." *The Dark Web Browser: What Is Tor, Is It Safe, and How to Use It*, 4 Aug. 2022, www.avast.com/c-tor-dark-web-browser.

"Global Cybercrime Treaty: A Delicate Balance between Security and Human Rights | | UN News." *News.un.org*, 25 Feb. 2024, news.un.org/en/interview/2024/02/1146772#:~:text=Recognizing%20the%20growing%20dangers%20of.

"Global Financial Ransomware Attack Rate 2024." *Statista*, www.statista.com/statistics/1460896/rate-ransomware-attacks-global/#:~:text=From%202021%20to%202024%2C%20the.

"Global Law Enforcement Action against Vendors and Buyers on the Dark Web." *Europol*, www.europol.europa.eu/media-press/newsroom/news/global-law-enforcement-action-against-vendors-and-buyers-dark-web.

"Glock Ghost Guns up for Grabs on the Dark Web." *ANU*, 22 Mar. 2021, www.anu.edu.au/news/all-news/glock-ghost-guns-up-for-grabs-on-the-dark-web.

Greengard, Samuel. "Tor | Browser, Dark Web, & Function | Britannica." *Www.britannica.com*, 21 Feb. 2023, www.britannica.com/technology/Tor-encryption-network.

House, The White. "International Counter Ransomware Initiative 2023 Joint Statement." *The White House*, 2 Nov. 2023, www.whitehouse.gov/briefing-room/statements-releases/2023/11/01/international-counter-ransomware-initiative-2023-joint-statement/.

"How the Dark Web Is Making Fraud Easier." *Www.aicpa-Cima.com*, www.aicpa-cima.com/professional-insights/article/how-the-dark-web-is-making-fraud-easier.

"How to Spot and Avoid Scams | Equifax UK." *Equifax.co.uk*, 2018, www.equifax.co.uk/resources/identity-protection/scam-avoidance-a-few-ways-to-help-stay-secure.html. Accessed 31 Aug. 2024.

Human Rights Council. documents.un.org/doc/undoc/gen/g22/442/29/pdf/g2244229.pdf.

"ICYMI: At Hearing, Warren Warns about Crypto's Use by North Korea to Fund Nuclear Weapons Program and Evade to Sanctions | U.S. Senator Elizabeth Warren of Massachusetts." *Senate.gov*, 21 July 2023, www.warren.senate.gov/newsroom/press-releases/icymi-at-hearing-warren-warns-about-cryptos-use-by-north-korea-to-fund-nuclear-weapons-program-and-evade-to-sanctions#:~:text=warned%20about%20the%20national%20security. Accessed 31 Aug. 2024.

"Infographic: Where Corruption Is Rampant." *Statista Infographics*, www.statista.com/chart/16834/countries-and-territories-ranked-on-perceived-public-sector-corruption/.

INTELLECTUAL PROPERTY CRIME on the DARKNET. www.europol.europa.eu/cms/sites/default/files/documents/darknet.pdf.

"International Standards OHCHR and Privacy in the Digital Age." *OHCHR*, www.ohchr.org/en/privacy-in-the-digital-age/international-standards#:~:text=Article%2012%20of%20the%20Universal,his%20or%20her%20honor%20and.

Investopedia. "The Great Recession." *Investopedia*, 18 Dec. 2023, www.investopedia.com/terms/g/great-recession.asp.

Jardine, Eric, et al. "The Potential Harms of the Tor Anonymity Network Cluster Disproportionately in Free Countries." *Proceedings of the National Academy of Sciences*, vol. 117, no. 50, Nov. 2020, pp. 31716–21, https://doi.org/10.1073/pnas.2011893117.

K, Jennifer. "The Surface Web, Deep Web, and Dark Web Explained - Active Intel Investigations." *Active Intel Investigations*, 10 Dec. 2022, www.activeintel.com/the-surface-web-deep-web-and-dark-web-explained/. Accessed 31 Aug. 2024.

"Learn about UNCAC." *United Nations : Office on Drugs and Crime*, www.unodc.org/corruption/en/uncac/learn-about-uncac.html.

Mack, Ryan. *Combating the Illicit Goods Trade on the Dark Web*. 2018, scholarworks.calstate.edu/downloads/1v53jz121.

Molinaro, Domenic. "Dark Web Facts Revealed: Myths and Stats about the Secret Web." *Dark Web Facts Revealed: Myths and Stats about the Secret Web*, Avast, Dec. 2023, www.avast.com/c-dark-web-facts#:~:text=No%2C%20the%20deep%20web%20is. Accessed 31 Aug. 2024.

"My Social Security Number on Dark Web | Help!" *Malwarebytes*, 11 Apr. 2024, www.malwarebytes.com/cybersecurity/basics/ssn-on-dark-web?srsltid=AfmBOoqAQX0xftFTKbZ3dzkdQrhC_q7coUi7akWiHKVYbRvf8ul2C4Wo. Accessed 31 Aug. 2024.

National Institute of Justice. "Taking on the Dark Web: Law Enforcement Experts ID Investigative Needs." *National Institute of Justice*, National Institute of Justice, 15 June 2020,

nij.ojp.gov/topics/articles/taking-dark-web-law-enforcement-experts-id-investigative-needs.

Office of Public Affairs. “Largest International Operation against Darknet Trafficking of Fentanyl and Opioids Results in Record Arrests and Seizures.” *Www.justice.gov*, 2 May 2023, www.justice.gov/opa/pr/largest-international-operation-against-darknet-trafficking-fentanyl-and-opioids-results.

“Office of Public Affairs | Bitcoin Fog Operator Convicted of Money Laundering Conspiracy | United States Department of Justice.” *Www.justice.gov*, 12 Mar. 2024, www.justice.gov/opa/pr/bitcoin-fog-operator-convicted-money-laundering-conspiracy.

Office, U. S. Government Accountability. “The Effectiveness of Economic Sanctions at Risk from Digital Asset Growth | U.S. GAO.” *Www.gao.gov*, 27 Sept. 2023, www.gao.gov/blog/effectiveness-economic-sanctions-risk-digital-asset-growth#:~:text=For%20example%2C%20in%20October%202022.

Petrosyan, Ani. “Global Cybercrime Estimated Cost 2028.” *Statista*, 15 Nov. 2023, www.statista.com/forecasts/1280009/cost-cybercrime-worldwide.

Popper, Nathaniel. “Can You Really Hire a Hit Man on the Dark Web?” *The New York Times*, 4 Mar. 2020, www.nytimes.com/2020/03/04/technology/can-you-hire-a-hit-man-online.html.

RAND Europe. “International Arms Trade on the Dark Web.” *Rand*, www.rand.org/randeurope/research/projects/2017/international-arms-trade-on-the-hidden-web.html.

Reiff, Nathan. “Were There Cryptocurrencies before Bitcoin?” *Investopedia*, 26 Aug. 2021, www.investopedia.com/tech/were-there-cryptocurrencies-bitcoin/.

“Remittances Are a Critical Economic Stabilizer.” *World Bank Blogs*, blogs.worldbank.org/en/voices/remittances-are-critical-economic-stabilizer.

“Should We Pay the Ransom - the Most Common Ransomware Question.” *Ransomware.org*, 12 Oct. 2021, ransomware.org/why-should-we-pay-the-ransom/.

Soldner, Felix, et al. “Counterfeits on Dark Markets: A Measurement between Jan-2014 and Sep-2015.” *Crime Science*, vol. 12, no. 1, BioMed Central, Oct. 2023, https://doi.org/10.1186/s40163-023-00195-2.

Team, Chainalysis. “2024 Crypto Crime Trends from Chainalysis.” *Chainalysis*, 18 Jan. 2024, www.chainalysis.com/blog/2024-crypto-crime-report-introduction/.

“The Dark Web: A Definitive Guide | McAfee.” *McAfee*, 5 Dec. 2022, www.mcafee.com/learn/the-dark-web-a-definitive-guide/.

“The Data of the Dark Web.” *The Economist*, www.economist.com/graphic-detail/2016/07/14/the-data-of-the-dark-web.

The Investopedia Team. “Cryptocurrency Explained with Pros and Cons for Investment.” *Investopedia*, 15 June 2024, www.investopedia.com/terms/c/cryptocurrency.asp.

“True Crime Story - AlphaBay.” *United Nations : Office on Drugs and Crime*, www.unodc.org/unodc/en/untoc20/truecrimestories/alphabay.html.

Tzanetos, Georgina. “Cryptocurrency Statistics 2022: Investing in Crypto.” *Bankrate*, 8 July 2022, www.bankrate.com/investing/cryptocurrency-statistics/.

U.S. Attorney Announces Historic $3.36 Billion Cryptocurrency Seizure and Conviction in Connection with Silk Road Dark Web Fraud. 7 Nov. 2022, www.justice.gov/usao-sdny/pr/us-attorney-announces-historic-336-billion-cryptocurrency-seizure-and-conviction.

“Unbanked: What It Means, Statistics, Solutions.” *Investopedia*, 2024, www.investopedia.com/terms/u/unbanked.asp#:~:text=The%20main%20reason%20for%20being. Accessed 31 Aug. 2024.

United Nations. “Developing Countries Most Vulnerable to Cyberattacks – UN.” *UN News*, 9 Dec. 2011, news.un.org/en/story/2011/12/397922.

---. “Money Laundering through Cryptocurrencies.” *United Nations : UN Toolkit on Synthetic Drugs*, 2023, syntheticdrugs.unodc.org/syntheticdrugs/en/cybercrime/launderingproceeds/moneylaundering.html.

---. *UNITED NATIONS CONVENTION against CORRUPTION*. 2004, www.unodc.org/documents/treaties/UNCAC/Publications/Convention/08-50026_E.pdf.

---. “Universal Declaration of Human Rights.” *United Nations*, 1948, www.un.org/en/about-us/universal-declaration-of-human-rights#:~:text=Article%2019.

United Nations Office on Drugs and Crime. “United Nations Office on Drugs and Crime.” *Unodc.org*, 2019, www.unodc.org/.

---. *USE of the DARK WEB and SOCIAL MEDIA for DRUG SUPPLY*. 2023, www.unodc.org/res/WDR-2023/WDR23_B3_CH7_darkweb.pdf.

UNODC Tools and Programs to Address Illicit Online Drug Sales on the Open and Dark Web. www.state.gov/wp-content/uploads/2021/11/UNODC-Tools-and-Programs-to-Address-Illicit-Online-Drug-Sales-on-the-Open-and-Dark-Web.pdf.

"Webinar on Investigations of Firearms Trafficking in Dark Web." *United Nations : Office on Drugs and Crime*, 2021, www.unodc.org/unodc/en/firearms-protocol/news/2020/Jan/webinar-on-investigations-of-firearms-trafficking-in-dark-web.html. Accessed 31 Aug. 2024.

"What Is a Bridge? | Tor Project | Support." *Torproject.org*, 2024, support.torproject.org/censorship/censorship-7/#:~:text=Bridges%20are%20useful%20for%20Tor. Accessed 31 Aug. 2024.

"What Is Cryptocurrency? | TD Direct Investing." *Www.td.com*, www.td.com/ca/en/investing/direct-investing/articles/cryptocurrency.

"Why the Role of Crypto Is Huge in the Ukraine War." *World Economic Forum*, www.weforum.org/agenda/2023/03/the-role-cryptocurrency-crypto-huge-in-ukraine-war-russia/.

"Why Was Bitcoin Created?" *Crypto.com*, crypto.com/bitcoin/why-was-bitcoin-created.