JUNE 2024 (№30)
Volume 10; Issue 2; Page No. 193-216
ISSN: 2346-7916 (Print)
ISSN: 2587-5043 (Online)

INTERNATIONAL JOURNAL OF LAW: "LAW AND WORLD" www.lawandworld.ge

https://doi.org/10.36475/10.2.14

COMMERCE IN THE SHADOWS: EXPLORING DARK WEB BLACK MARKETS

Anri Nishnianidze
Doctoral Candidate of Law, Grigol Robakidze University, Georgia

ARTICLE INFO

Article History:

Received	20.04.2024
Accepted	05.06.2024
Published	30.06.2024

Keywords:

Cybercrime, Dark Web, E-Commerce, Darknet, Cybercriminal

ABSTRACT

In the twenty-first century, several negative moments have accompanied many positive technological progress events. With the development of the digital world, criminals with special knowledge – cybercriminals have become active and have developed many means in the depths of cyberspace, with the help of which they achieve their criminal and illegal goals.

The presented paper aims to analyze in detail and in-depth the system and working principles of digital black markets created by cybercriminals on the dark side of the Internet. The paper also looks at what tools and products are available on the digital black market and why digital black markets are hazardous to operate successfully.

The paper analyzes practical cases, legal studies, and other interdisciplinary studies to present the problems in the legal struggle against digital black markets as of the day it was written. The paper's primary purpose is to show why the unimpeded functioning of digital black markets on the dark web is dangerous – both for the ordinary citizen and the state structures.

In the final part of the article, based on the analysis of the processed literature and practical cases, recommendations will be presented, the use of which is of particular importance to make the legal fight against digital black markets successful and to prevent such a dangerous phenomenon as digital black markets from existing in any part of the digital world.

INTRODUCTION

Technological progress has made everyday life easier for many people in the twenty-first century. Today, it is easier for people to connect because the development of technology has created many tools that have made it possible to perform previously tricky actions efficiently. One of the best results of progress is the development of the digital world. Today, if a person owns even one electronic device, be it a computer system or a mobile phone, and the device is connected to the Internet, individuals can perform almost any activity without leaving their homes. People use such systems for personal purposes, e.g. Reading an e-book, getting an education, or deepening personal relationships, as well as for other professional or commercial purposes – e.g. Remote work in various fields, be it remote court hearings or lecturing at a university. One of the areas that has developed in the digital world is online stores. At any part of the day, a person can remotely view what products the store offers him, select the desired product, pay the amount electronically, and wait for him to receive the desired item.[1] Of course, such possibilities greatly simplify a person's daily life.

The development of technological progress, as mentioned, has made life easier for many people and created many opportunities. But, as in the case of any progress, in the case of technological progress, along with positive events, many adverse events have become its concomitants, in particular, a new type of criminals – cybercriminals[2] – have appeared in the digital world, whose goal has become to use the opportunities arising from the progress of the digital world to achieve their own criminal goals, e.g. Cyber extortionists,[3] cyber fraudsters,[4] and other kinds of cybercriminals. The mentioned cybercrimes look similar to crimes in the real world; however, in reality, they are entirely different from each other, both in terms of methods and ways of execution.[5]

Most people use computer devices such as digital banks, social platforms, and many other websites and applications for daily activities. However, most of the users do not know that the part of the digital world that they use every day is the smallest and does not even reflect the actual scale of the digital world.[6] When using the Google search engine (or any other traditional search engine), much of the data in cyberspace is not accessible because traditional search engines perform strict filtering so that various types of irrelevant data are not available to everyone.[7] The second part of the digital world, which the everyday ordinary user does not use and does not know, is the deep web,[8] and the part of the deep web where cybercriminals mainly operate is the dark web.[9]

In connecting to the dark web, anonymity, privacy, and other ways are especially protected, so it is challenging to identify the person who uses it. It is because of the mentioned opportunities that the dark web is the best place for cybercriminals and the so-called shelter.[10] It should be noted here that access to the dark web is not only used by cybercriminals. It is used by researchers,[11] and whistleblowers working in various government agencies so that if the agency violates the laws, they can inform the world about the case.[12] Of course, such actions are essential. However, the fact is that the majority of Dark Web users want

[1] Jain, V., Malviya, B., Arya, S., (2021). An overview of electronic commerce (e-Commerce). *Journal of Contemporary Issues in Business and Government,* 27(3). p. 665.

[2] Sabillon, R., Cavaller, V., Cano, J., Serra-Ruiz, J., (2016). Cybercriminals, cyberattacks and cybercrime. *In 2016 IEEE International Conference on Cybercrime and Computer Forensic*. pp. 1-2.

[3] Salvi, M.H.U., Kerkar, M.R.V., (2016). Ransomware: A cyber extortion. *Asian Journal For Convergence In Technology,* 2. p. 1.

[4] Banerjee, A., Barman, D., Faloutsos, M., Bhuyan, L.N., (2008). Cyber fraud is one typo away. *In IEEE INFOCOM 2008*. p. 66.

[5] Wall, D., (2007). Cybercrime: The transformation of crime in the information age. *Polity.* (Vol. 4). p. 31.

[6] Ciancaglini, V., Balduzzi, M., McArdle, R., Rösler, M., (2015). the Deep Web. *Trend Micro.* pp. 35-38.

[7] Supra.

[8] He, B., Patel, M., Zhang, Z., Chang, K.C.C., (2007). Accessing the deep web. *Communications of the ACM,* 50(5). p. 95.

[9] Omar, Z.M., Ibrahim, J., (2020). An overview of Darknet, rise and challenges and its assumptions. *Int. J. Comput. Sci. Inf. Technol,* 8. pp. 110-111.

[10] Ciancaglini, V., Balduzzi, M., Goncharov, M., McArdle, R., (2013). Deepweb and cybercrime. *Trend Micro report,* 9. pp. 5-6.

[11] Dalvi, A., Ankamwar, L., Sargar, O., Kazi, F., Bhirud, S.G., (2021). From Hidden Wiki 2020 to Hidden Wiki 2021: What Dark Web Researchers Comprehend with Tor Directory Services? *In 2021 5th International Conference on Information Systems and Computer Networks*. p. 1.

[12] Pender, K., Cherkasova, S., Yamaoka-Enkerlin, A., (2019). Compliance and whistleblowing: How technology will replace, empower and change whistleblowers. *In FinTech, Edward Elgar Publishing.* pp. 379-380.

to carry out their criminal activities anonymously and achieve specific criminal results.

In the early stages of the development of the digital world, cybercriminals, in the process of carrying out their criminal activities, were mostly in possession of the personal data of ordinary users, whether it was data about bank accounts, personal life data, or other kinds of information.[13] As a result of such criminal activities, which had a daily character, it is logical that cybercriminals accumulated a lot of data that they could no longer use personally, so it was on the agenda for criminals to create a system where they could sell such data or exchange it for other data they wanted. They imitated the so-called real-world black market system, where it is possible to buy any desired means illegally,[14] and cybercriminals in the dark web created a digital black market, the pace and scale of which has exceeded all expectations.[15] As of today, in the digital black market, it is possible to buy any digital or real-life products: a person can buy firearms,[16] drugs,[17] and prohibited pornographic material.[18] The list is not exhaustive – the digital black market offers users much more opportunities than one can imagine.

In this paper, the author will delve deep into the world of the dark web and the digital black market. The analysis will highlight the intricacies of how these markets work and their impact on society. The author will also discuss the dangers that come with the successful functioning of these black markets and why it is crucial to wage an unrelenting struggle against them. The existence of black markets in the digital world poses a significant threat to the safety and security of individuals, businesses, and even governments. Therefore, it is of utmost importance to take appropriate measures to eliminate them once and for all.

In the final part of this article, recommendations to implement to make the fight against cybercriminals successful will be provided. These recommendations will be practical, actionable and aimed at ensuring that the digital world is a safe and secure place for everyone.

The twenty-first century has given humanity many gifts – one of the greatest gifts is the development of the digital world because people's lives have become much easier, and citizens can perform previously unimaginable actions or be associated with particular difficulties. If earlier it was challenging to connect with someone on the other side of the planet, today it is enough for two people to have access to any social network, and they will be in touch with each other in a few seconds. However, as mentioned, there are not only positive moments that accompany progress. In the early stages of the development of the digital world, more people have decided to use cyberspace for criminal purposes rather than to take care of its security. It can be said that cybercriminals have recognized the potential of cyberspace, while security experts have ignored it at the initial stage. This is one of the reasons why digital black markets exist and why it is easier for cybercriminals to engage in criminal activities on the dark web. Nevertheless, giving up is not an option. More people must understand what the dark web is to understand what the digital black market is so that more people are digitally armed so that the fight against cybercriminals becomes stronger and digital black markets disappear from the space of the digital world forever.[19]

1. DARK WEB AND BLACK MARKET

According to specialists in the field, the modern Internet can be likened to an iceberg, with the visible tip representing the part of the Internet that everyday users have access to and use on a regular basis.[20] How-

[13] Babanina, V., Tkachenko, I., Matiushenko, O., Krutevych, M., (2021). Cybercrime: History of formation, current state and ways of counteraction. *Amazonia Investiga,* 10(38). p.114.

[14] Boulding, K.E., (1947). A Note on the Theory of the Black Market. Canadian Journal of Economics and Political Science. *Revue canadienne de economiques et science politique,* 13(1). p. 115.

[15] Spagnoletti, P., Ceci, F., Bygstad, B., (2021). Online black-markets: An investigation of a digital infrastructure in the dark. *Information Systems Frontiers.* pp. 1811-1812.

[16] Liggett, R., Lee, J.R., Roddy, A.L., Wallin, M.A., (2020). The dark web as a platform for crime: An exploration of illicit drug, firearm, CSAM, and cybercrime markets. *The Palgrave handbook of international cybercrime and cyberdeviance.* p. 94.

[17] Supra, p. 97.

[18] Supra, p. 104.

[19] Sviatun, O., Goncharuk, O., Roman, C., Kuzmenko, O., Kozych, I.V., (2021). Combating cybercrime: economic and legal aspects. *WSEAS Transactions on Business and Economics,* 18. pp. 751-752.

[20] Kavallieros, D., Myttas, D., Kermitsis, E., Lissaris, E., Giataganas, G., Darra, E., (2021). Understanding the dark web.

ever, this visible part only accounts for a small fraction of the total information available on the Internet. This is because traditional search engines like Google, Yahoo, and Bing are designed to filter out a large portion of the information available to ordinary users.[21]

In reality, the vast majority of the Internet lies beneath the surface, in what is commonly referred to as the "deep web". This includes everything from private databases and password-protected websites to academic research and government records. However, there is also a subset of the deep web known as the "dark web", which is intentionally hidden and requires special software to access.[22] Within the dark web, there exists a subset known as the "Black Market". This is a hidden network of websites where users can buy and sell illegal goods and services, such as drugs, weapons, and stolen personal information. These sites are often accessed using specialized software that allows users to browse anonymously and avoid detection.

It is important to note that while the terms "deep web", "dark web", and "Black Market" are often used interchangeably, they actually refer to distinct parts of the Internet with different levels of accessibility and content. Understanding these terms is crucial for anyone who wants to navigate the Internet safely and responsibly, as it can help users avoid potentially dangerous or illegal activities.

1.1. Dark Web

The deep web is a vast and complex network that comprises all the information on the internet that is not indexed by conventional search engines. This includes various types of online content that are not easily accessible to the average user. However, the dark web, a segment of the deep web, is notorious for being a hub for cybercriminals.[23] The dark web is home to a range of confidential data, password-protected websites, and databases that are hidden from the public eye. Unfortunately, the dark web has become increasingly popular among cybercriminals, making it a significant cybersecurity threat. Therefore, taking necessary precautions while accessing the deep and dark web is essential to avoid any potential risks. It is where malicious users can conduct illegal activities such as trading stolen data, selling illegal goods, and planning cyberattacks. On the dark web, it is possible to find data that cybercriminals have illegally obtained and distributed e.g.

a) In 2019, cyber attackers spread the personal data of users of one of the banking systems of the Cayman Islands.[24]

b) In 2020, the personal data of the population of Georgia, which cybercriminals obtained by attacking the database of personal data protected in the Central Election Commission, was distributed.[25]

c) In 2021, cybercriminals spread the personal data of Washington Metropolitan Police officers.[26]

One cannot rely on traditional web browsers like Google Chrome, Firefox, or Microsoft Edge to access the dark web. Instead, they must use specialized software that provides high anonymity and security. One such software is Tor (The Onion Router), an open-source and free-to-use software that allows users to connect to the dark web securely and anonymously. Essentially, Tor routes internet traffic through several different servers worldwide, making it difficult for anyone to trace a person's online activity or physical location. Moreover, Tor provides access to hidden websites that cannot be found through traditional search engines like Google or Bing. However, it's important to note that the dark web can be dangerous, and users must exercise caution while browsing it. Several illegal activities take place on the dark web, including drug trafficking, human trafficking, and cybercrime. Therefore, users must be careful while accessing the dark web and avoid clicking on suspicious links or downloading files from unknown sources. Additionally, it's recommended to use a VPN (Virtual Private Network) along with Tor to further enhance your anonymity and protect your privacy. By using

Dark web investigation. p. 6.

[21] Supra, p. 8.

[22] Finklea, K.M., (2015). Dark web. *Congressional Research Service*. p. 2.

[23] Supra, pp. 1-3.

[24] BBC News. 'Cayman National Suffers Manx Bank 'Data Hack' [Online] Available at: <https://www.bbc.com/news/world-europe-isle-of-man-50475734> [Last Accessed: June 11, 2024].

[25] Cimpanu C., Personal Details for the Entire Country of Georgia Published Online [Online] Available at: <https://www.zdnet.com/article/personal-details-for-the-entire-country-of-georgia-published-online> [Last Accessed: June 11, 2024].

[26] Rose R., LeBlanc P. and Fung B., DC Police Personnel Files Obtained by Hackers in Recent Ransomware Attack, Acting Police Chief Says [Online] Available at: <https://www.cnn.com/2021/04/29/politics/dc-police-ransomware-attack-personnel-files/index.html> [Last Accessed: June 11, 2024].

Tor and following safe browsing practices, one can access the dark web and explore its content without compromising their security or privacy.[27]

The software mentioned in the text is designed to give users anonymity when they connect to the dark web. This is because anonymity is fundamental to the dark web's existence. However, even users who are well-versed in security protocols are aware that relying solely on this software may not be enough to guarantee their anonymity. As a result, many users employ additional security measures to further reduce the risk of their anonymity being compromised and their identity being exposed.[28]

Despite the risks involved, the dark web remains a popular destination for cybercriminals due to its anonymity and lack of oversight. This has led to the development of a thriving digital black market, where users can buy and sell illegal goods and services without fear of being caught by law enforcement agencies.[29]

1.2. The Digital Black Market

When discussing the topic of black markets, many people tend to conjure up images of shady street corners or dimly lit alleyways where individuals can purchase illegal or hard-to-find goods. However, the reality of black markets in the modern world is vastly different, particularly when it comes to the digital realm. Digital black markets offer a far greater range of products and services to consumers than their real-world counterparts ever could, and as such, it has become crucial to examine the extent and significance of these markets. To fully understand the implications of digital black markets, it is important to analyze their scope, how they operate, and their potential consequences on society. By doing so, citizens can better equip themselves to combat the negative effects that these markets can have and ensure that our society remains safe and secure in the digital age. Furthermore, it is important to investigate the motivations of those who engage in the digital black market and the methods they use to navigate these online spaces. This can help us to better understand the factors that contribute to the growth of these markets and how people can work to prevent them from becoming a more significant threat in the future.

In the early 2000s, the concept of a digital black market began to emerge, driven by increased internet use for commerce. However, it wasn't until 2011 that the black market truly reached new heights with the launch of Silk Road. This online marketplace allowed users to anonymously buy and sell illegal goods and services, including drugs, weapons, and stolen personal information.

Silk Road quickly gained notoriety and became a hub for criminal activity. It operated on the dark web, a part of the internet that is not easily accessible to the general public and is often used for illicit purposes. Despite attempts by law enforcement to shut it down, Silk Road continued to thrive, earning an estimated 183 million USD during its period of operation.[30]

In 2013, the Federal Bureau of Investigation (FBI) finally managed to shut down Silk Road and arrest its founder, Ross Ulbricht.[31] This was a significant victory for law enforcement, but it didn't take long for other cybercriminals to see the financial potential of running a digital black market.

Soon after Silk Road's demise, Silk Road 2.0 emerged, promising to be even bigger and better than its predecessor. However, its functionality was short-lived, as it was also shut down by law enforcement soon after its launch.[32] Nevertheless, the success of the Silk Road had already set a precedent, and other black markets such as Hansa[33] and Alpha Bay[34] surfaced to take its place.

[27] Macrina, A., Phetteplace, E., (2015). The Tor browser and intellectual freedom in the digital age. *Reference and User Services Quarterly,* 54(4). pp. 18-19.

[28] Jadoon, A.K., Iqbal, W., Amjad, M.F., Afzal, H., Bangash, Y.A., (2019). Forensic analysis of Tor browser: a case study for privacy and anonymity on the web. *Forensic science international,* 299. p. 3.

[29] Zhang, H., Zou, F., (2020). A survey of the dark web and dark market research. *In 2020 IEEE 6th international conference on computer and communications*. p. 1695.

[30] Mullin, J., (2015). Silk Road prosecutors complete the bizarre DPR murder-for-hire story. *Ars Technica.* pp. 1-3.

[31] Minnaar, A., (2017). Online'underground'marketplaces for illicit drugs: the prototype case of the dark web website'Silk Road. *Acta Criminologica: African Journal of Criminology & Victimology, 30(1).* p. 30.

[32] Dolliver, D.S., (2015). Evaluating drug trafficking on the Tor Network: Silk Road 2, the sequel. *International Journal of Drug Policy, 26(11).* p. 1115.

[33] Tavabi, N., Bartley, N., Abeliuk, A., Soni, S., Ferrara, E., Lerman, K., (2019). Characterizing activity on the deep and dark web. *In Companion proceedings of the 2019 world wide web conference*. p. 209.

[34] Baravalle, A., Sin Wee Lee, (2018). Dark web markets: Turning the lights on AlphaBqay. *In Web Information Sys-*

The rise of digital black markets has posed a significant challenge to law enforcement agencies worldwide in recent years. One of the key factors driving the growth of these markets is the emergence of cryptocurrency as a payment method. Cryptocurrency, by its very nature, is designed to be anonymous and decentralized, making it an ideal payment method for people who want to remain hidden while engaging in illegal activities.

When a person purchases a product from a digital black market using cryptocurrency, they can do so without leaving a trace. Authorities can easily trace traditional payment methods like credit cards or bank transfers, but cryptocurrency transactions are much harder to track. This makes it difficult for law enforcement agencies to identify the seller and the buyer,[35] allowing these markets to operate with impunity for extended periods.

While it is technically possible to trace cryptocurrency transactions, doing so is time-consuming and labour-intensive, requiring specialized knowledge and resources. As a result, individual buyers who use cryptocurrency to purchase illegal goods or services often go unpunished, and digital black markets can continue to operate for years before they are finally shut down by law enforcement agencies.[36]

The use of cryptocurrency in digital black markets has raised many concerns among governments and policymakers, who worry that it will make it much harder to combat illegal activities such as drug trafficking, money laundering, and terrorism financing. Some countries have taken steps to regulate cryptocurrency more closely, while others have banned it outright.

Despite these efforts, digital black markets continue to thrive, and the use of cryptocurrency as a payment method is likely to remain a significant challenge for law enforcement agencies in the years to come. As new forms of cryptocurrency emerge and technology evolves, tracking transactions will be even harder, making it easier for criminals to engage in illegal activities.

The rise of cryptocurrency has made it easier for people to engage in black market trading by providing an anonymous payment method that is difficult to trace. While it is possible to track cryptocurrency transactions, doing so is time-consuming and resource-intensive, often yielding little results. As a result, digital black markets continue to operate, posing a significant challenge to law enforcement agencies worldwide.

It's important to note that the digital black market is not limited to just those abovementioned platforms. Countless other black markets exist on the dark web.[37] To help readers understand the breadth of this underground economy, it's important to look beyond just listing the marketplaces themselves. It's also important to examine the available products and services on these platforms. From stolen personal information, counterfeit goods, and illicit drugs to hacking services, malware, and firearms, the digital black market offers consumers a wide range of illegal products and services. By understanding this market's scope, individuals can protect themselves and their personal information online.

2. PRODUCTS ON THE DIGITAL BLACK MARKET

The preceding sections of the article have extensively discussed the topic of the digital black market and its exponential growth. It has been emphasized multiple times that the digital black market has become a massive enterprise, and its operations have reached unprecedented dimensions. To fully comprehend the extent of the dangers posed by the digital black market and understand why it is challenging to combat it, it is essential to have a clear understanding of the various products and services readily available on digital black market platforms. The digital black market is a clandestine platform that facilitates the trading of illicit goods and services, which include but are not limited to drugs, weapons, counterfeit products, stolen data, and hacking tools. The platform also offers various services like money laundering, identity theft, and hacking. The anonymity provided by the platform enables the buyers and sellers to operate with impunity, making it difficult for law enforcement

tems Engineering–WISE 2018, Springer. p. 503.

[35] Mukhopadhyay, U., Skjellum, A., Hambolu, O., Oakley, J., Yu, L., Brooks, R., (2016). A brief survey of cryptocurrency systems. *In 2016 14th annual conference on privacy, security and trust.* p. 745.

[36] Dyson, S., Buchanan, W.J., Bell, L., (2019). The challenges of investigating cryptocurrencies and blockchain related crime. *arXiv, 1907.12221.* pp. 1-2.

[37] Kermitsis, E., Kavallieros, D., Myttas, D., Lissaris, E., Giataganas, G., (2021). Dark web markets. *Dark Web Investigation.* pp. 88-89.

agencies to track down the perpetrators. It is crucial to have a comprehensive knowledge of the workings of the digital black market and the range of illicit goods and services traded on these platforms. The digital black market is a hub for cybercriminals, who use it to sell and purchase illegal items, significantly contributing to the global cybercrime economy. The products and services traded on these platforms are harmful to individuals and pose significant threats to national security. For instance, cybercriminals can use the data stolen from individuals to launch targeted attacks on government agencies or corporations, leading to significant financial losses and reputational damage. Therefore, it is crucial to have a comprehensive understanding of the workings of the digital black market and the range of illicit goods and services traded on these platforms to combat this growing threat.[38]

2.1. Drugs

The digital black market is primarily fueled by the demand for drugs, making it one of the most common products found there. Every type of drug imaginable, including those that have never been heard of before, can be found in this unregulated market. Some of these drugs are newly invented and created by amateur chemists in their basements.[39] This widespread availability of drugs poses a significant problem for many countries, as cybercriminals operate the buying and selling process without any regulation or control.[40]

In the process of using social networks, almost every user has received a message from a stranger offering him many types of drugs, be it cocaine, heroin, MDMA or any other. For this, the user only needs to transfer the amount of money to the designated account of a "friendly stranger", indicate in which city he lives, and wait for instructions on where he can take the drug (often a similar place is a cemetery, forest and other uninhabited areas).[41]

Illegal drug trafficking on the internet is a serious problem that has been plaguing the world for quite some time now. The dark web is the go-to place for digital black market narcotics syndicates as it provides them with complete anonymity, making it almost impossible for law enforcement agencies to identify and prosecute them. These cybercriminals use various methods to conceal their identity and location so that they cannot be traced back to their illegal activities. The reason why it is so difficult to prevent the activities of these cybercriminals is due to the nature of the dark web. Accessing the dark web without special software that masks your IP address and encrypts your communication is almost impossible. This makes it very difficult for law enforcement agencies to monitor or intercept communications between the buyers and sellers of illegal drugs.[42]

Moreover, if a law enforcement representative were to purchase drugs during a special police operation, they would not be able to identify the seller during the purchase process. This is because the seller would be using sophisticated methods to conceal their identity, such as using cryptocurrency to receive payment and shipping the drugs through anonymous postal services. These methods make it almost impossible for law enforcement agencies to track down the seller.

In the world of the dark web, the absence of a centralized system or empire of digital black markets poses a significant challenge to the state's power structures. With many markets operating independently, the government's task of controlling illicit activities becomes increasingly difficult. Even if the government successfully shuts down one digital black market, it does not guarantee that the drug trade in the dark web will cease entirely. For instance, even after the infamous "Silk Road" was taken down, the drug trade continued to thrive on the dark web through other independent markets. This decentralized nature of the dark web's digital black markets makes it challenging for authorities to curb illegal activities effectively.[43]

[38] Lacson, W., Jones, B., (2016). The 21st century darknet market: lessons from the fall of Silk Road. *International Journal of Cyber Criminology, 10(1).* p. 40.

[39] Rhumorbarbe, D., Staehli, L., Broséus, J., Rossy, Q., Esseiva, P., (2016). Buying drugs on a Darknet market: A better deal? Studying the online illicit drug market through the analysis of digital, physical and chemical data. *Forensic science international,* 267. pp. 173-175.

[40] Buxton, J., Bingham, T., (2015). The rise and challenge of dark net drug markets. *Policy brief, 7(2).* p. 3.

[41] Demant, J., Bakken, S.A., Oksanen, A., Gunnlaugsson, H., (2019). Drug dealing on Facebook, Snapchat and Instagram: A qualitative analysis of novel drug markets in the Nordic countries. *Drug and alcohol review, 38(4).* p. 380.

[42] Jardine, E., (2015). The Dark Web dilemma: Tor, anonymity and online policing. *Global Commission on Internet Governance Paper Series, (21).* pp. 2-3.

[43] Spalevic, Z., Ilic, M., (2017). The use of dark web for the purpose of illegal activity spreading. *Ekonomika, 63(1).* p.

The drug trade in the digital black market, like the other types of trade presented in this chapter, due to the possibilities of the digital world, is an event of an international nature because a person from any country can purchase the desired drug, both in his native country and in any other foreign country.[44]

2.2. Illegal Arms

Firearms have been around for centuries, and with them, the illegal trade of these lethal weapons. This illegal market has been present since the early days of firearms, but it has become more sophisticated and widespread over time. The twentieth century was a turning point for the illegal trade in firearms, as it reached exceptional heights. This was partly due to the proliferation of guns and ammunition after World War II, which led to the establishment of large-scale smuggling networks across the globe. Moreover, the beginning of the twenty-first century saw a continuation of this trend, with the emergence of new technologies and the increasing availability of weapons in conflict zones.[45] Despite the efforts of governments and international organizations to curb this trade, it remains a persistent and dangerous problem that threatens public safety and security.

As the digital world continues to evolve, cybercrime syndicates have found new opportunities to expand their illicit activities. One of these opportunities is the digital black market, where not only drugs but also firearms can be sold. This has made their business process much easier, as they no longer have to meet with the buyer in the real world, thus reducing the risks associated with such transactions. Today, it is possible to purchase firearms in both individual and bulk quantities, posing unimaginable dangers for civilians.[46] The digital black market offers a wide range of firearms, from simple pistols to weapons of mass destruction, along with information about them or their parts.

This alarming trend has raised concerns among governments and ordinary citizens, as the availability of such dangerous weapons in the digital black market seriously threatens public safety and security and calls for urgent action to curb this growing problem.[47]

2.3. Personal and Confidential Information

In today's world, people rely heavily on electronic devices for both personal and professional use. They use these devices to store and access various personal information, ranging from photographs and videos to banking information and social media accounts. Additionally, many individuals store sensitive work-related data on their devices, such as confidential documents and intellectual property, intending to access these materials from the comfort of their homes.

However, despite the convenience and efficiency of these devices, it is crucial to recognize that there is no such thing as absolute security in the digital world.[48] Hackers and cybercriminals are always on the lookout for vulnerabilities in electronic devices and software, and they continue to develop new and sophisticated methods to gain unauthorized access to personal and confidential information.

Furthermore, even if an individual takes all the necessary precautions to secure their device, there is always a risk of physical theft or damage to the device, which can result in the loss of valuable data. Moreover, many people also tend to overlook the risk of unintentionally sharing sensitive information through their digital activities, such as downloading apps or opening email attachments from untrusted sources.

Therefore, it is essential to acknowledge these risks and take appropriate measures to protect personal and confidential information. This includes implementing strong passwords, using two-factor authentication, regularly updating software and security settings, and being vigilant about phishing scams and other forms of cyber-attacks.

76.

[44] Holland, B.J., (2020). Transnational cybercrime: The dark web. *Encyclopedia of Criminal Activities and the Deep Web*. p. 109.

[45] Stohl, R., Grillot, S., (2009). *The international arms trade. Polity, (Vol.7).* pp. 15-16.

[46] Jiang, C., Foye, J., Broadhurst, R., Ball, M., (2021). Illicit firearms and other weapons on darknet markets. *Trends and Issues in Crime and Criminal Justice, (622).* pp. 3-4.

[47] Chen, H., Chen, H., (2012). Weapons of Mass Destruction (WMD) on Dark Web. *Dark Web: Exploring and Data Mining the Dark Side of the Web.* pp. 341-342.

[48] Trabelsi, S., (2019). Monitoring leaked confidential data. *In 2019 10th IFIP International Conference on New Technologies, Mobility and Security.* p. 1.

While electronic devices have undoubtedly revolutionized the way people live and work, it is critical to recognize that they also pose significant security risks. By being proactive and taking the necessary steps to protect personal and confidential information, individuals can enjoy the benefits of technology while minimizing the associated risks.

The paper discusses a specific type of cybercriminals who operate in the digital black market. Unlike traditional criminals who engage in physical activities to obtain drugs and weapons, these cybercriminals do not have to leave their comfort zone to achieve their goals. However, it must be emphasized that an ordinary person cannot carry out these actions, as it requires special knowledge and equipment to gain access to personal or confidential information from another person's computer or device.[49]

The subsection of the paper will delve deeper into the techniques these cybercriminals use to infiltrate digital systems. They might use phishing scams or malware attacks to access sensitive information, which they can auction off on digital black markets. These markets offer a platform for cybercriminals to sell their ill-gotten gains to the highest bidder.[50]

The digital black market has become a lucrative business for cybercriminals specializing in stealing and selling personal information, credit card details, and other confidential data. They can sell this information to other criminals who use it to commit fraud, identity theft, or other illegal activities.

Trade-in personal information is one of the most significant threats law enforcement agencies face today. The danger lies not in the information itself but in the potential consequences of its misuse. Personal information can be extremely harmful to one's dignity and reputation, especially when it falls into the wrong hands. The extent of the damage, however, depends on who the person is and what information is obtained.[51]

For instance, if cybercriminals gain access to sensitive information about the head of a country's intelligence service, they could potentially blackmail him into doing something against his principles or the interests of his country. The implications of such an action could be catastrophic since the intelligence chief is responsible for safeguarding the country's national security. If he were to succumb to the cybercriminals' demands, the consequences could be severe for him and the entire nation.

Cybercriminals' possession of state confidential material can have serious consequences. Such material may contain information crucial for the state's functioning, which can significantly damage the country's security and interests if it falls into the wrong hands. In addition to state secrets, such material may contain personal data of individuals employed in various state structures. The release of such data can put their lives in danger, making them vulnerable to blackmail and other forms of exploitation.[52]

Government agencies and employees need to be aware of the risks associated with cyberattacks, including phishing and social engineering scams, which are often used by cybercriminals to gain access to sensitive information. Regular training and awareness programs can help to educate employees about these risks and help them to identify and report any suspicious activity.

It is important to note that cybercriminals are not necessarily interested in the content of the documents they steal. Instead, their primary objective is to obtain such material and then advertise the fact that they have it. They often wait for a buyer to come forward who is willing to pay a high price for the information.[53] This makes it crucial for the government to take necessary measures to protect its confidential material and ensure that it is not compromised by cybercriminals. This includes implementing robust security measures, such as encryption and access controls, to prevent unauthorized access to sensitive data.

[49] Belmabrouk, K., (2023). Cyber Criminals and Data Privacy Measures. *In Contemporary Challenges for Cyber Security and Data Privacy, IGI Global.* p. 199.

[50] Pantelis, G., Petrou, P., Karagiorgou, S., Alexandrou, D., (2021). On strengthening smes and mes threat intelligence and awareness by identifying data breaches, stolen credentials and illegal activities on the dark web. *In Proceedings of the 16th International Conference on Availability, Reliability and Security.* p. 3.

[51] Al Amro, S., (2020). How safe is governmental infrastructure: A cyber extortion and increasing ransomware attacks perspective. *International Journal of Computer Science and Information Security (IJCSIS), 18(6).* p. 81.

[52] Sharma, N., Oriaku, E.A., Oriaku, N., (2020). Cost and effects of data breaches, precautions, and disclosure laws. *International Journal of Emerging Trends in Social Sciences, 8(1).* p. 39.

[53] Howell, C.J., Fisher, T., Muniz, C.N., Maimon, D., Rotzinger, Y., (2023). A Depiction and Classification of the Stolen Data Market Ecosystem and Comprising Darknet Markets: A Multidisciplinary Approach. *Journal of Contemporary Criminal Justice, 39(2).* p. 299.

2.4. Counterfeit Products

It's important to know that digital black market sites exist where counterfeit products can be purchased. These sites offer a vast range of fake items, including electronic devices, watches, lighters, and other goods with real-world value. Unfortunately, individuals who purchase such items from the digital black market may mistake them for authentic items in the real world. In many cases, the forgeries are so well-made that even a seasoned user might find it challenging to differentiate between the fake and the genuine piece.[54] It is crucial to exercise caution and verify the authenticity of any item you intend to purchase, especially if it is from an online source.

Counterfeit products available on digital black market pages have the potential to cause significant harm, not just to individuals but to entire states. While some fake products may only be harmful to individuals, other counterfeit items like fake currencies,[55] passports, and other documents can be bought and sold on the pages of the digital black market.[56] Cybercriminals with unique knowledge can use these fake documents to penetrate various state systems, making it difficult for specific state agencies to determine which documents are real and which are fake. In fact, after verifying the fake passport data in the electronic database, the agencies may receive information that the submitted passport data is stored in the database and, therefore, is real.[57] This poses a significant threat to national security and requires the attention and action of law enforcement agencies to curb the activities of cyber criminals and crack down on the digital black market.

It can be quite challenging to determine the potential consequences of engaging in activities that involve fake passports, forged documents, and counterfeit money banknotes. The outcome of such actions is highly dependent on the specific case at hand. For instance, the severity of the consequences can vary greatly based on who is using the fake passport and for what purpose. If a person is using a fake passport to enter a desired country, it could lead to issues such as immigration problems or even legal troubles. Similarly, the consequences of using forged documents to access a protected building can range from minor security breaches to serious security threats.

When it comes to counterfeit money banknotes, the outcome can depend on several factors. The amount of money being counterfeited plays a significant role in determining the potential consequences. Counterfeiting a small amount of money may not have a significant impact on the economy of a state. However, if a large number of fake banknotes are being used, it can cause irreparable damage to the economy. This is because counterfeit money can lead to inflation, which can result in the devaluation of the currency and a decline in the purchasing power of the citizens. It can also lead to a loss of confidence in the financial system, which can have a ripple effect on the economy as a whole.

2.5. Other Types of Services on the Digital Black Market

Upon careful analysis of the products presented in this particular chapter of the article, the sheer extent of the digital black market becomes abundantly clear to the researcher. However, it is vital to note that this particular market is not limited to only the products mentioned here. There are many other types of services and products available in the digital black market, including but not limited to:

A. Cybercrime has become a common phenomenon in today's fast-paced digital world. It is no longer uncommon for users to hire the services of cybercriminals to achieve their desired objectives. For instance, a user may hire a cybercriminal to break into another person's computer device to obtain confidential information or acquire a large company's sensitive data. This can be done through various means, such as hacking, phishing, social engineering, or other cyber-attack forms. Cybercrime is a serious offence and can lead to grave consequences. Therefore, users need to be cautious and take necessary measures to protect themselves and their organizations from cyber threats.[58]

[54] Chaudhry, P.E., (2017). The looming shadow of illicit trade on the Internet. *Business Horizons,* 60(1). p. 81.

[55] Spalevic, Z., Ilic, M., (2017). The use of dark web for the purpose of illegal activity spreading. *Ekonomika,* 63(1). p. 78.

[56] Vargas, V.M., (2019). The new economic good: Your own personal data. An integrative analysis of the Dark Web. *In Proceedings of the International Conference on Business Excellence,* Vol. 13, No. 1. p. 1221.

[57] Zhang, Y., Xiao, Y., Ghaboosi, K., Zhang, J., Deng, H., (2012). A survey of cyber crimes. *Security and Communication Networks, 5(4).* p. 423.

[58] Manky, D., (2013). Cybercrime as a service: a very modern

B. The user is presented with various options for obtaining hacking software, which can be used to achieve specific objectives. However, it is important to understand that these programs are not authorized by law and using them can lead to severe legal consequences. Additionally, the use of such software can pose a significant risk to the security of the user's computer system and personal data.[59]

C. The deep web markets are notorious for being a hub of illegal activities. In these markets, users can access a wide range of illicit goods and services, including drugs, fake IDs, hacking tools, and more. Shockingly, some of these markets even offer the service of hiring an assassin to carry out a murder. This dangerous and illegal activity is highly condemned by society and law enforcement agencies worldwide. It is important to stay away from such activities as they can lead to severe consequences and put one's life at risk.[60]

D. In the deep web, individuals with malicious intent can purchase access from cybercriminals to gain unauthorized access to cameras to monitor people illegally. This activity seriously violates privacy and security measures to protect individuals and their personal information. The perpetrators of such crimes use advanced hacking techniques to bypass security systems and gain access to cameras, which can be located in private homes, businesses, or other public places. The consequences of such actions can be severe, including identity theft, blackmail, and other forms of cybercrime. Individuals and organizations need to take proactive steps to protect their privacy and security online, including using strong passwords, regularly updating security software, and being vigilant about suspicious activity.[61]

E. It is possible to find a wide range of illegal services and products on the deep web, including the ability to hire individuals with specialized knowledge to assist with money laundering. These individuals typically operate under the radar, using cryptocurrencies to avoid detection and maintain anonymity. With their expertise in the field, they can help clients navigate the complex world of financial crime, offering advice on how to launder money safely and effectively. This is just one of many illegal services that can be found on the deep web, making it a dangerous and illicit place to explore.[62]

The digital black market has been growing at an unprecedented rate in recent years, with its vast scale and far-reaching operations expanding every year. The idea of a cyber black market may have started small, but with the growing consumer demand for illegal goods and services, it has become a lucrative venture for cybercriminals to exploit. Today, the digital black market has become a hub for the buying and selling of all kinds of illicit products, including drugs, weapons, counterfeit money, and stolen personal information. The increasing accessibility of the internet and the rise of cryptocurrency have made it easier for cybercriminals to operate anonymously and evade law enforcement agencies. As a result, the digital black market is now a major threat to online security and a challenge for law enforcement agencies worldwide.

3. DIGITAL BLACK MARKET TRADING AND CONSUMERS

3.1. Trading in the Digital Black Market

In the previous chapter of the paper, a comprehensive analysis was presented on the various products and types of services that exist in the digital black market. However, this analysis raises a completely logical question as to how cybercriminals can continue to carry out their criminal activities and why it is so challenging to eliminate their operations.[63] As mentioned, technology is advancing at an unprecedented pace, and many opportunities are becoming available not only to ordinary citizens but also to cybercriminals. This means that these criminals are constantly

business. *Computer Fraud & Security,* 2013(6). p. 9.

[59] Basheer, R., Alkhatib, B., (2021). Threats from the dark: A review over dark web investigation research for cyber threat intelligence. *Journal of Computer Networks and Communications,* 2021. p. 3.

[60] Akintaro, M., Pare, T., Dissanayaka, A.M., (2019). Darknet and black market activities against the cybersecurity: a survey. *In The Midwest Instruction and Computing Symposium, North Dakota State University, Fargo,* ND. p. 5.

[61] Jones, A.S., Gagneja, K., (2016). Preventing covert webcam hacking in the civilian and governmental sectors. *In 2016 International Conference on Computational Science and Computational Intelligence.* p. 993.

[62] De Sanctis, F.M., (2023). Cyber Risks, Dark Web, and Money Laundering. *Regulating Cyber Technologies: Privacy Vs Security*. p. 283.

[63] Ablon, L., Libicki, M., (2015). Hacker's Bazaar: The markets for cybercrime tools and stolen data. *Def. Counsel,* 82. p. 143.

adapting and improving their tactics to evade detection and continue their illegal activities. Additionally, the anonymity provided by the internet and the ease of communication and exchange of information has made it difficult for law enforcement agencies to track and apprehend cybercriminals. As a result, it becomes increasingly important to develop more advanced and effective strategies to combat cybercrime.

In the world of cybercrime, achieving complete anonymity is one of the primary objectives for criminals to continue their illegal activities. Cybercriminals use various software and tools to hide their identities, making it challenging for law enforcement agencies to track them down. But it's not just about identifying the culprit; determining their physical location and the location of the digital black market servers is equally challenging.[64] The digital black market is often spread across multiple countries, with servers located in one country, cybercriminals in another, and users in a different country altogether. This complex web of operations makes it nearly impossible to track down the criminals involved.

As opposed to traditional online shopping, where customers are required to provide their personal information,[65] in the digital black market, both the seller and the buyer use only pseudonyms, and no personal information is collected.[66] This anonymity provides a safe haven for cybercriminals to operate without being detected. However, the question arises as to how financial transactions are made in such an environment. While personal information is not collected, financial transactions still take place. Cybercriminals use various means to transfer funds, such as digital currencies, which are difficult to trace. Using digital currencies allows cybercriminals to operate without leaving a paper trail, making it challenging for law enforcement agencies to track financial transactions. Furthermore, cybercriminals often use money laundering techniques to make it even more difficult to trace transactions. This complex system of operations is designed to make it extremely difficult to detect and prosecute cybercriminals.

In the modern era, one of the most rapidly developing technologies is that of cryptocurrencies. Cryptocurrencies are digital currencies that can be used by anyone.[67] Unlike traditional bank payments, where a person typically uses a plastic card registered in their name, cryptocurrencies offer a level of anonymity and security that many find appealing.

When using a cryptocurrency, a person does not need to identify themselves, unlike traditional banking methods where personal data is recorded. During a cryptocurrency transfer, both the sender and the recipient can remain completely anonymous.[68] While this anonymity is attractive for many, it also raises questions about how buyers can be protected from fraud and scams.

On the digital black market, groups of individuals operate with their own "wallets" in pursuit of their goals.[69] To purchase a product, a user does not directly send payment to the seller. Instead, the payment is made to a third-party account. This third party acts as an intermediary between the buyer and seller, ensuring that the transaction is safe and secure. Once the customer receives the product and confirms that it is what they ordered, the third party credits the seller's account.[70] This system provides a layer of protection for users, eliminating the fear of transferring money and not receiving the desired product.

While this system may create some difficulties for cybercriminals, it ultimately benefits users by increasing the number of people willing to participate in the digital black market. Although the payment process has become more complex, introducing this intermediary system has helped reduce fraudulent activities and increase the trust between buyers and sellers.

It is worth noting that introducing this intermediary system has made the payment process more se-

[64] Biddle, P., England, P., Peinado, M., Willman, B., (2002). The Darknet and the future of content distribution. *In ACM Workshop on digital rights management,* Vol. 6. p. 54.

[65] Nanehkaran, Y.A., (2013). An introduction to electronic commerce. *International journal of scientific & technology research,* 2(4). p. 190.

[66] Hämäläinen, L., (2019). User names of illegal drug vendors on a darknet cryptomarket. *Onoma,* 50. pp. 62-63.

[67] Mukhopadhyay, U., Skjellum, A., Hambolu, O., Oakley, J., Yu, L., Brooks, R., (2016). A brief survey of cryptocurrency systems. *In 2016 14th annual conference on privacy, security and trust.* p. 745.

[68] Tewari, S.H., (2020). Abuses of cryptocurrency in dark web and ways to regulate them. *SSRN 3794374*. p. 3.

[69] White, R., Kakkar, P.V., Chou, V., (2019). Prosecuting darknet marketplaces: Challenges and approaches. *Dep't of Just. J. Fed. L. & Prac.,* 67. pp. 65-66.

[70] Evangelista, A., Allodi, L., Cremonini, M., (2018). Darknet Markets: Competitive Strategies in the Underground of Illicit Goods. *The Eindhoven University of Technology.* pp. 13-14.

cure and reliable, but it has also led to an increase in the number of users on the digital black market. This is because people who were previously hesitant to engage in online transactions due to the fear of being scammed can now rely on a third party to ensure the safety of their transactions.

In conclusion, while the payment process on the digital black market has become more complicated, introducing this intermediary system has helped protect users' interests and increase their confidence in online transactions. Despite the challenges that come with operating in the digital black market, the use of intermediaries has made it a safer and more reliable space for buyers and sellers alike.

3.2. Digital Black Market Users

In today's digital age, it is becoming increasingly important to identify who is connected to the digital black market. However, when it comes to digital black market users, no clear-cut profile can be used to identify them. This is because the existing theories in the science of criminology around the profile of criminals are not sufficient to respond to the challenges posed by the development of the digital world.[71] It is widely accepted among criminological scientists that a new type of criminal has emerged in cyberspace, which does not fit the current criminal profiles in the science of criminology.

Unlike the members of criminal syndicates in the real world, a member of a criminal syndicate in the digital world could be anyone. Cybercriminals may not fit a particular age group, nationality, gender, or origin. They could be simple, ordinary citizens who interact with society daily. This makes it impossible to determine who can be a cybercriminal.[72]

It is important to understand that the digital world has opened up a new avenue for criminal activities, and it is difficult to predict who would be attracted to this illegal activity. The anonymity offered by the internet can make it easier for people to engage in criminal activities without being caught. Some people may even be unaware they are involved in illegal activities when browsing the digital black market.

Therefore, law enforcement agencies must stay up-to-date with the latest trends in cybercrime and work towards developing a comprehensive understanding of the digital black market. This can help them identify and prevent criminal activities in the digital world and protect innocent citizens from the harms of cybercrime.

The digital black market is a notorious platform where individuals can purchase products or services that are not legally available. Those who enter this market usually have a variety of motivations, with the most common being criminal goals. These goals may include the acquisition of illegal substances, weapons, and other prohibited items that are not readily available through traditional channels.[73]

The one type of consumer motivation refers to individuals driven by specific goals that may not align with societal norms and values. Such buyers aim to purchase products that can potentially harm society or state structures. For instance, extremists who gather around a particular ideology may seek to acquire firearms or other types of weapons to cause large-scale damage. These consumers are often motivated by a sense of purpose that is rooted in their belief system and may be willing to go to extreme lengths to achieve their objectives.[74]

It is worth noting that law enforcement officials often have connections to the digital black market. These connections are established to help track down cybercriminals and buyers within the digital black market. By keeping tabs on these illegal activities, law enforcement officials can take timely legal action to prevent the criminal activities of these individuals. This is particularly important in cases where security norms are violated, and it becomes possible to identify the perpetrators. By quickly identifying and apprehending these individuals, law enforcement officials can help safeguard the public against the harmful effects of cybercrime and keep our digital world safe and secure.[75]

[71] Jaishankar, K., (2018). Cyber criminology as an academic discipline: history, contribution and impact. *International Journal of Cyber Criminology,* 12(1). p. 1.

[72] Kwan, L., Ray, P., Stephens, G., (2008). Towards a methodology for profiling cyber criminals. *In Proceedings of the 41st Annual Hawaii International Conference on System Sciences.* p. 264.

[73] Wang, M., Wang, X., Shi, J., Tan, Q., Gao, Y., Chen, M., Jiang, X., (2018). What is in the Darknet? Measurement and analysis of darknet person attributes. *In 2018 IEEE Third International Conference on Data Science in Cyberspace*. pp. 948-949.

[74] Weimann, G., (2016). Going dark: Terrorism on the dark web. *Studies in Conflict & Terrorism,* 39(3). p. 195.

[75] Heidenreich, S., Westbrooks, D.A., (2017). Darknet mar-

To gain a deeper understanding of the practices and operations of the digital black market, researchers need to establish a connection with this elusive marketplace. This entails accessing and analyzing the vast amounts of data generated by this underground economy, including the types of goods and services sold, the prices charged, the payment methods used, and the communication channels employed by its participants. Through careful analysis of this data, researchers can identify patterns and trends that can help shed light on the inner workings of the digital black market. This information can then be shared with the general public to increase awareness of the dangers of the digital black market and develop effective strategies to combat its illicit activities. By gaining a better understanding of the digital black market, researchers can help law enforcement agencies and policymakers prevent cybercrime, protect consumers, and safeguard the integrity of digital systems.[76]

Overall, the digital black market is a complex and multifaceted space that attracts users with diverse interests and motives. While some users seek to exploit it for illegal activities, others use it to promote justice and prevent crime. Understanding the different types of users and their objectives is essential in devising effective strategies to combat the digital black market and ensure the safety and security of individuals and communities worldwide.

As people move forward with technological advancements, they witness the emergence of new opportunities every day. However, alongside the benefits, there is a growing concern about the increasing number of cybercriminals taking advantage of technological progress results. They continue to develop the digital black market system, which poses a significant challenge for law enforcement agencies worldwide. This system enables cybercriminals to conduct illicit activities such as selling stolen data, malware, hacking services, and other illegal products on the dark web. The anonymity and encryption offered by the dark web make it difficult for law enforcement to track the perpetrators and bring them to justice. As a result, the fight against cybercrime has become more complex and requires a collaborative effort from governments, law enforcement agencies, and private organizations to mitigate the risks of cyber threats.[77]

4. THE PROBLEM OF COMBATING THE DIGITAL BLACK MARKET

At the turn of the twenty-first century, numerous experts predicted that the digital world, driven by the proliferation of the internet, would grow to a level that would dominate every aspect of people's lives.[78] However, sceptics dismissed these predictions, believing that the digital world would never attain the level of development it has today. As it has now appeared, the proponents of the first opinion were right. Nonetheless, criminals were not oblivious to the potential of the digital world and its opportunities. They shifted their focus to the digital world, where they could operate without needing firearms and other tools, instead relying solely on their specialized knowledge and appropriate technical equipment. The fact that cybercriminals have mastered the digital world better than security professionals reflects their expertise in exploiting digital vulnerabilities and weaknesses often unnoticed by security professionals. As a result, cybercrime has become a significant challenge for law enforcement and security agencies, who must stay ahead of the criminals to maintain a secure digital world.[79]

One of the greatest challenges law enforcement agencies face in their fight against digital black markets is that the very nature of these markets is international. The black market is not limited to a specific geographic location; rather, it operates across borders and jurisdictions, making it incredibly difficult for authorities to track and prosecute offenders.[80]

In addition, the complexity of these markets

kets: A modern day enigma for law enforcement and the intelligence community. *American Intelligence Journal,* 34(1). p. 38.

[76] Benjamin, V., Valacich, J.S., Chen, H., (2019). DICE-E: A Framework for Conducting Darknet Identification, Collection, Evaluation with Ethics. *MIS Quarterly,* 43(1). pp. 1-2.

[77] Ajayi, E.F.G., (2016). Challenges to enforcement of cyber-crimes laws and policy. *Journal of Internet and Information Systems,* 6(1). p. 4.

[78] Krämer, N.C., Neubaum, G., Eimler, S.C., (2017). A brief history of (social) cyberspace. *Cyberemotions: Collective emotions in cyberspace.* pp. 11-12.

[79] Ramdinmawii, E., Ghisingh, S., Sharma, U.M., (2014). A study on the cyber-crime and cyber criminals: A global problem. *International Journal of Web Technology,* 3. p. 53.

[80] Goodman, M., (2010). International dimensions of cybercrime. *In Cybercrimes: A multidisciplinary analysis, Springer.* pp. 311-312.

makes it difficult for law enforcement agencies to effectively investigate and prosecute those involved in illicit activities. This is because the server of the digital black market can be located in one country, while the customer and seller can be located in different countries, and the products can be stored in other countries altogether.

Moreover, the lack of international legal frameworks, codes, and bases to govern the fight against digital black markets further complicates the efforts of law enforcement agencies. This means that there are no established international laws to facilitate cooperation among national investigative units in their efforts to combat these markets.

The absence of an international legal framework creates legal barriers that make it difficult for countries to work together and exchange information, which is critical in the fight against digital black markets. Hence, the absence of international cooperation and legal frameworks makes it challenging for law enforcement agencies to effectively combat digital black markets.[81]

In the digital world, black markets are a growing concern, and one of the significant challenges is anonymity.[82] While it is true that no one can be entirely anonymous in the digital world, law enforcement agencies can identify a person's identity if necessary. However, this raises a severe ethical dilemma for any democratic state. The state must identify the person responsible for illegal activities without compromising fundamental human rights and freedoms.[83]

The fight against digital black markets is crucial to protect society from the harms of illegal activities. However, if the state violates its citizens' fundamental rights and freedoms in the process, the fight will lose its significance. Protecting one legal good should not come at the expense of other legal rights. The systematic violation of human rights and freedoms will undermine the very existence of democracy. In such a society, the democratic state will eventually crumble, turning into a totalitarian regime where the rulers justify their complete control and surveillance by claiming to protect human rights.[84]

Therefore, balancing the need to identify and prosecute those responsible for illegal activities is essential while protecting fundamental human rights and freedoms. The state must use legal and ethical means to identify and prosecute those involved in illegal activities. A democratic state should never compromise its citizens' basic rights and freedoms in the name of fighting against digital black markets or any other illegal activities.

One of the pressing issues that is currently being discussed is the widespread use of cryptocurrency. Cybercriminals have increasingly used this digital currency, as it offers an anonymous and untraceable method of transferring funds. The article highlights that due to the decentralized nature of cryptocurrencies, it is often difficult to track the financial transactions conducted using them. Moreover, the lack of regulatory oversight and a central authority makes it easier for cybercriminals to evade detection and prosecution. As a result, these criminals can profit from their illegal activities without fear of being caught.[85] This has become a major concern for law enforcement agencies worldwide, struggling to keep up with the constantly evolving methods of cybercrime and the use of cryptocurrencies.

The issue of cybercrime is growing more and more pressing as the world continues to digitize. While it may be tempting to believe that existing legal frameworks will be sufficient to deal with future threats from cyberspace, the reality is that fighting crimes in the digital world requires a different set of strategies and mechanisms.[86] While some illegal activities, such as drug trafficking or document forgery, can be punished under existing criminal law regulations, the unique challenges posed by the digital world require updated legal bases that are tailored to the specific needs of this new domain.

One of the most significant challenges is the is-

[81] Chang, W., Chung, W., Chen, H., Chou, S., (2003). An international perspective on fighting cybercrime. *In Intelligence and Security Informatics: First NSF/NIJ Symposium, ISI 2003, Springer.* p. 379.

[82] Saleem, J., Islam, R., Kabir, M.A., (2022). The anonymity of the dark web: A survey. *IEEE Access,* 10. p. 628.

[83] Herschel, R.T., 2021. Privacy, ethics, and the Dark Web. *In Research anthology on privatizing and securing data, IGI Global*. p. 2066.

[84] Mc Manamon, C., Mtenzi, F., (2010). Defending privacy: The development and deployment of a darknet. *In 2010 International Conference for Internet Technology and Secured Transactions.* p. 5.

[85] Reddy, E., Minnaar, A., (2018). Cryptocurrency: A tool and target for cybercrime. *Acta Criminologica: African Journal of Criminology & Victimology*, 31(3). pp. 74-75.

[86] Sviatun, O., Goncharuk, O., Roman, C., Kuzmenko, O., Kozych, I.V., (2021). Combating cybercrime: economic and legal aspects. *WSEAS Transactions on Business and Economics,* 18. p. 759.

sue of jurisdiction. For example, if someone from one country sells a drug in another country, and the drug itself is located in a third country, which existing legal basis should be used to effectively fight against this crime? The answer is far from clear and highlights the need for a new way of thinking when it comes to cybercrime.

The digital world is a new phenomenon, and the digital black market is a new side effect of this new phenomenon. As such, a new kind of approach is required to address the unique challenges that it presents. Without a new way of thinking, the digital black market will continue to expand, and it will be increasingly difficult to control the flow of illegal products and activities. This unacceptable outcome requires urgent attention from lawmakers and law enforcement agencies worldwide.

CONCLUSION

The twenty-first century is often called the era of technological progress, evolution, and revolution. The article highlights that this century has brought about unprecedented opportunities that were once unimaginable. One area that has been significantly developed is the digital world, commonly known as cyberspace. This space's development has simplified how people connect and their daily lives. It has brought numerous benefits, such as enhancing communication, facilitating online transactions, and making knowledge accessible to people across the globe.

However, as the paper highlights, technological progress has also presented certain challenges. Cybercriminals have found it easier to commit crimes thanks to technological advancements. They can now exploit computer network and system vulnerabilities to gain unauthorized access to sensitive information, steal identities, and infiltrate financial systems. This has led to an increase in cybercrime cases, which pose a threat to individuals, organizations, and governments. Therefore, while technology has brought numerous benefits, it is crucial to ensure that it is used responsibly and ethically to prevent misuse and safeguard our digital lives.

The article analyses the deep web, the dark web, and the digital black market. It explains what these terms mean and sheds light on the dangers associated with the unimpeded functioning of digital black markets. The article highlights why their existence poses a significant threat to individuals and states alike.

To support its claims, the article draws upon a detailed study of the researched materials, which reveal the comprehensive nature of the digital black market. It highlights the fact that users of the dark web have access to a wide range of illegal goods and services, from drugs and firearms to the possibility of purchasing parts for weapons of mass destruction.

The paper strives to provide a comprehensive understanding of the digital black market and the risks associated with its existence. By doing so, it aims to educate readers on the dangers of the dark web and the importance of taking steps to curb the unimpeded functioning of digital black markets. Digital black markets on the dark web pose a significant threat to ordinary citizens who use cyberspace for various purposes. Therefore, it is crucial to take necessary measures to eliminate the functioning of these illegal marketplaces.

Upon analyzing the problems presented in the article, the author has developed some essential recommendations that must be implemented in reality. These measures aim to stop the functioning of digital black markets and ensure a safer online environment for everyone.

It is imperative to analyze the recommendations given below and implement them, in reality, to ensure that ordinary citizens can use cyberspace freely without any fear of being targeted by illegal activities, in particular:

A. International cooperation. Digital black markets are a growing concern, and their existence is not limited to a particular country or region. These markets pose a significant threat to the global economy, as they operate clandestinely and are often involved in illegal activities. Therefore, it is crucial to establish international organizations and communities whose primary objective is to combat digital black markets. One of the key strategies that can help in the fight against digital black markets is the quick and efficient exchange of information. This will increase the chances of detecting digital black market servers on time and arresting those responsible for running them. By doing so, cooperation can effectively end the digital black market. Without such international communities, tracking the movement of digital black market servers will be difficult. The people running these servers can quickly relocate them to another location and erase all traces of their existence. Consequently, the fight against digital black markets must start from scratch. Therefore, it is essential to establish robust international partnerships where the sharing of intelligence and resources is a priority. This will enable the authorities to stay ahead of the game and take down digital black markets before they can cause significant damage. By working together, international cooperation can create a safer and more secure digital landscape free from the threat of digital black markets.

B. Updating legal bases. It is crucial to follow the law when fighting crime, even in the face of criminal activity. This means that law enforcement officers must adhere to the latest legal acts, which provide them with the necessary tools to combat criminal activity. Adopting these legal acts is essential because it streamlines identifying, investigating, and prosecuting criminal activity. In today's digital age, international legal acts are particularly important. This is because digital black markets often operate across international borders, making it challenging for law enforcement agencies to take quick and effective action. Having international legal acts in place enables law enforcement agencies to work together to fight crime and bring criminals to justice, regardless of location. However, time is of the essence in combating cybercrime. Every second that law enforcement agencies spend on legal matters is a second that cybercriminals can use to cover their tracks. For this reason, it is essential to have streamlined legal procedures to ensure that law enforcement agencies can take swift and decisive action against criminals. By doing so, relevant state structures can make the Internet safer for everyone.

C. Cyber security experts. States must establish dedicated departments specializing in this area to effectively combat the growing threat of digital black markets. These departments should focus solely on studying and combating the threat posed by digital black markets rather than dealing with cybercrime in general. One of the key tasks of these specialized units should be to conduct a detailed analysis of the organization and functioning of digital black markets. This is a complex and time-consuming task that requires a great deal of expertise and experience. By having dedicated experts in the field of cybersecurity working within these units, states can take a significant step forward in the fight against the digital black market. Overall, establishing specialized departments to combat digital black markets is a crucial step governments should take to protect their citizens from the various threats these illicit online marketplaces pose.

D. Interdisciplinary studies. To effectively combat cybercriminals in the digital black market, law enforcement agencies must comprehensively understand the various factors involved. It is not enough to view the issue from a single professional perspective. Instead, a multidisciplinary approach is needed, incorporating insights from law, cyber security, programming, and psychology. To truly comprehend the complexities of the digital black market, it is essential to examine the problems from various angles. This includes analyzing the psychological profile of cybercriminals, identifying security norms and best practices, and establishing a solid legal foundation for addressing these issues. Law enforcement agencies can gain a more objective and nuanced understanding of the digital black market by taking a holistic approach. This will enable them to better identify and respond to cybercriminal activities, ultimately helping to protect individuals and organizations from the damaging effects of cybercrime.

E. Strategies and mechanisms. To effectively combat the growing threat of digital black markets, developing comprehensive strategies and mechanisms is imperative. These should be designed to equip relevant department representatives with the necessary tools and knowledge to tackle individual cases head-on. It is also important to ensure that these strategies and mechanisms are constantly updated to stay ahead of the latest challenges and threats. To achieve this, it is necessary to incorporate cutting-edge technologies such as artificial intelligence, machine learning, and data analytics. By leveraging these advanced technologies, patterns and trends can be analyzed, and it will be possible to predict potential threats before they occur. Furthermore, educating the public about the dangers of digital black markets and promoting awareness of the risks associated with engaging in illegal activities online is important. This can be achieved through targeted campaigns that aim to inform and educate people about the consequences of their actions. Combating digital black markets requires a multi-pronged approach incorporating the latest technologies, ongoing education and awareness campaigns, and a commitment to constantly updating strategies and mechanisms to stay ahead of the ever-evolving threat landscape.

The dark web, a part of the Internet that is not indexed by search engines and requires specific software to access, is expanding at an alarming rate. This growth is largely fueled by the constant development and innovation of new digital tools by cybercriminals. These tools are designed to facilitate illegal activities such as hacking, identity theft, drug trafficking, and other illicit activities. Unfortunately, this trend shows no signs of slowing down, posing a significant threat to online security and privacy. Therefore, individuals and organizations must take necessary precautions to protect their sensitive information from falling into the wrong hands.

In today's digital age, it is crucial to have international cooperation, updated legal frameworks, practical strategies and mechanisms, and people with appropriate expertise and education to prevent the rapid growth of cybercrime and eliminate black markets from the digital space. With the increasing reliance on technology, it has become easier for cybercriminals to carry out their illegal activities, and law enforcement agencies need to be equipped with the necessary tools to combat these crimes effectively.

International cooperation is essential in this regard, as cybercrime is a global issue requiring coordinated effort from all nations. Updated legal frameworks should be implemented to ensure that cybercriminals are brought to justice and that victims are adequately protected. Moreover, practical strategies and mechanisms, such as robust cybersecurity measures and data protection laws, should be implemented to prevent cyber-attacks and safeguard sensitive information.

However, having updated legal frameworks, practical strategies, and mechanisms alone may not be enough to combat cybercrime. People with appropriate expertise and education are the key to preventing and fighting cybercrime effectively. It is essential to have a skilled workforce that can understand the nature of cybercrime and develop innovative solutions to counter it. This requires proper training, education, and awareness programs to equip individuals with the necessary knowledge and skills.

Cybercrime is a significant threat to the digital world, and unless appropriate changes are made and proper training and education are in place, cybercriminals will ultimately win, and law enforcement will lose control of the digital world forever. A concerted effort from all stakeholders is required to address this issue and ensure a safe and secure digital environment for all.

BIBLIOGRAPHY

1. Ablon, L., Libicki, M., (2015). Hacker's bazaar: The markets for cybercrime tools and stolen data. *Def. Counsel,* 82.
2. Ajayi, E.F.G., (2016). Challenges to enforcement of cyber-crimes laws and policy. *Journal of Internet and Information Systems*, 6(1).
3. Akintaro, M., Pare, T., Dissanayaka, A.M., (2019). Darknet and black market activities against the cybersecurity: a survey. *In The Midwest Instruction and Computing Symposium. (MICS),* North Dakota State University, Fargo, ND.
4. Al Amro, S., (2020). How safe is governmental infrastructure: A cyber extortion and increasing ransomware attacks perspective. *International Journal of Computer Science and Information Security,* 18(6).
5. Babanina, V., Tkachenko, I., Matiushenko, O., Krutevych, M., (2021). Cybercrime: History of formation, current state and ways of counteraction. *Amazonia Investiga,* 10(38).
6. Banerjee, A., Barman, D., Faloutsos, M., Bhuyan, L.N., (2008). Cyber-fraud is one typo away. *In IEEE INFOCOM.*
7. Baravalle, A., Sin Wee Lee, (2018). Dark web markets: Turning the lights on AlphaBay. *In Web Information Systems Engineering–WISE 2018.* Springer.
8. Basheer, R., Alkhatib, B., (2021). Threats from the dark: A review over dark web investigation research for cyber threat intelligence. *Journal of Computer Networks and Communications.*

9. BBC News."Cayman National Suffers Manx Bank 'Data Hack'" BBC (November 19, 2019) <https://www.bbc.com/news/world-europe-isle-of-man-50475734> [Last accessed: June 11, 2024].
10. Belmabrouk, K., (2023). Cyber Criminals and Data Privacy Measures. *In Contemporary Challenges for Cyber Security and Data Privacy.* IGI Global.
11. Benjamin, V., Valacich, J.S., Chen, H., (2019). DICE-E: A Framework for Conducting Darknet Identification, Collection, Evaluation with Ethics. *MIS Quarterly,* 43(1).
12. Biddle, P., England, P., Peinado, M., Willman, B., (2002). The Darknet and the future of content distribution. *In ACM Workshop on digital rights management,* Vol. 6.
13. Boulding, K.E., (1947). A Note on the Theory of the Black Market. Canadian Journal of Economics and Political Science. *Revue canadienne de economiques et science politique,* 13(1).
14. Buxton, J., Bingham, T., (2015). The rise and challenge of dark net drug markets. *Policy brief,* 7(2).
15. Chang, W., Chung, W., Chen, H., Chou, S., (2003). An international perspective on fighting cybercrime. *In Intelligence and Security Informatics: First NSF/NIJ Symposium,* Springer.
16. Chaudhry, P.E., (2017). The looming shadow of illicit trade on the Internet. *Business Horizons,* 60(1).
17. Chen, H., Chen, H., (2012). Weapons of Mass Destruction (WMD) on Dark Web. *Dark Web: Exploring and Data Mining the Dark Side of the Web.*
18. Ciancaglini, V., Balduzzi, M., Goncharov, M., McArdle, R., (2013). Deepweb and cybercrime. *Trend micro report,* 9.
19. Ciancaglini, V., Balduzzi, M., McArdle, R., Rösler, M., (2015). the Deep Web. *Trend Micro.*
20. Cimpanu C, Personal Details for the Entire Country of Georgia Published Online [Online] Available at: <https://www.zdnet.com/article/personal-details-for-the-entire-country-of-georgia-published-online> [Last Accessed: June 11, 2024].
21. Dalvi, A., Ankamwar, L., Sargar, O., Kazi, F., Bhirud, S.G., (2021). From Hidden Wiki 2020 to Hidden Wiki 2021: What Dark Web Researchers Comprehend with Tor Directory Services?. *In 2021 5th International Conference on Information Systems and Computer Networks.*
22. De Sanctis, F.M., (2023). Cyber Risks, Dark Web, and Money Laundering. Regulating Cyber Technologies: *Privacy Vs Security.*
23. Demant, J., Bakken, S.A., Oksanen, A., Gunnlaugsson, H., (2019). Drug dealing on Facebook, Snapchat and Instagram: A qualitative analysis of novel drug markets in the Nordic countries. *Drug and alcohol review,* 38(4).
24. Dolliver, D.S., (2015). Evaluating drug trafficking on the Tor Network: Silk Road 2, the sequel. *International Journal of Drug Policy,* 26(11).
25. Dyson, S., Buchanan, W.J., Bell, L., (2019). The challenges of investigating cryptocurrencies and blockchain related crime. *arXiv.* 1907.12221.
26. Evangelista, A., Allodi, L., Cremonini, M., (2018). Darknet Markets: Competitive Strategies in the Underground of Illicit Goods. *Eindhoven University of Technology,* 13.
27. Finklea, K.M., (2015). Dark web. *Congressional Research Service.*
28. Goodman, M., (2010). International dimensions of cybercrime. *In Cybercrimes: A multidisciplinary analysis, Springer.*
29. Hämäläinen, L., (2019). User names of illegal drug vendors on a darknet cryptomarket. *Onoma,* 50.
30. He, B., Patel, M., Zhang, Z., Chang, K.C.C., (2007). Accessing the deep web. *Communications of the ACM,* 50(5).
31. Heidenreich, S., Westbrooks, D.A., (2017). Darknet markets: A modern day enigma for law enforcement and the intelligence community. *American Intelligence Journal,* 34(1).
32. Herschel, R.T., (2021). Privacy, ethics, and the Dark Web. *In Research anthology on privatizing and securing data.* IGI Global.
33. Holland, B.J., (2020). Transnational cybercrime: The dark web. *Encyclopedia of Criminal Activities and the Deep Web.*
34. Howell, C.J., Fisher, T., Muniz, C.N., Maimon, D., Rotzinger, Y., (2023). A Depiction and Classification of the Stolen Data Market Ecosystem and Comprising Darknet Markets: A Multidisciplinary Approach. *Journal of Contemporary Criminal Justice,* 39(2).
35. Jadoon, A.K., Iqbal, W., Amjad, M.F., Afzal, H., Bangash, Y.A., (2019). Forensic analysis of Tor browser: a case study for privacy and anonymity on the web. *Forensic science international,* 299.
36. Jain, V., Malviya, B., Arya, S., (2021). An overview of electronic commerce (e-Commerce). *Journal of Contemporary Issues in Business and Government,* 27(3).
37. Jaishankar, K., (2018). Cyber criminology as an academic discipline: history, contribution and impact. *International Journal of Cyber Criminology,* 12(1).
38. Jardine, E., (2015). The Dark Web dilemma: Tor, anonymity and online policing. *Global Commission on Inter-*

net Governance Paper Series, (21).

39. Jiang, C., Foye, J., Broadhurst, R., Ball, M., (2021). Illicit firearms and other weapons on darknet markets. *Trends and Issues in Crime and Criminal Justice,* (622).
40. Jones, A.S., Gagneja, K., (2016). Preventing covert webcam hacking in the civilian and governmental sectors. *In 2016 International Conference on Computational Science and Computational Intelligence.*
41. Kavallieros, D., Myttas, D., Kermitsis, E., Lissaris, E., Giataganas, G., Darra, E., (2021). Understanding the dark web. *Dark web investigation.*
42. Kermitsis, E., Kavallieros, D., Myttas, D., Lissaris, E., Giataganas, G., (2021). Dark web markets. *Dark Web Investigation.*
43. Krämer, N.C., Neubaum, G., Eimler, S.C., (2017). A brief history of (social) cyberspace. *Cyberemotions: Collective emotions in cyberspace.*
44. Kwan, L., Ray, P., Stephens, G., (2008). Towards a methodology for profiling cyber criminals. *In Proceedings of the 41st Annual Hawaii International Conference on System Sciences.*
45. Lacson, W., Jones, B., (2016). The 21st century darknet market: lessons from the fall of Silk Road. *International Journal of Cyber Criminology,* 10(1).
46. Liggett, R., Lee, J.R., Roddy, A.L., Wallin, M.A., (2020). The dark web as a platform for crime: An exploration of illicit drug, firearm, CSAM, and cybercrime markets. *The Palgrave handbook of international cybercrime and cyberdeviance.*
47. Macrina, A., Phetteplace, E., (2015). The Tor browser and intellectual freedom in the digital age. *Reference and User Services Quarterly,* 54(4).
48. Manky, D., (2013). Cybercrime as a service: a very modern business. *Computer Fraud & Security,* 2013(6).
49. Mc Manamon, C., Mtenzi, F., (2010). Defending privacy: The development and deployment of a darknet. *In 2010 International Conference for Internet Technology and Secured Transactions.*
50. Minnaar, A., (2017). Online'underground'marketplaces for illicit drugs: the prototype case of the dark web website'Silk Road. *Acta Criminologica: African Journal of Criminology & Victimology,* 30(1).
51. Mukhopadhyay, U., Skjellum, A., Hambolu, O., Oakley, J., Yu, L., Brooks, R., (2016). A brief survey of cryptocurrency systems. *In 2016 14th annual conference on privacy, security and trust.*
52. Mullin, J., (2015). Silk Road prosecutors complete the bizarre DPR murder-for-hire story. *Ars Technica.*
53. Nanehkaran, Y.A., (2013). An introduction to electronic commerce. *International journal of scientific & technology research,* 2(4).
54. Omar, Z.M., Ibrahim, J., (2020). An overview of Darknet, rise and challenges and its assumptions. *Int. J. Comput. Sci. Inf. Technol,* 8.
55. Pantelis, G., Petrou, P., Karagiorgou, S., Alexandrou, D., (2021). On strengthening smes and mes threat intelligence and awareness by identifying data breaches, stolen credentials and illegal activities on the dark web. *In Proceedings of the 16th International Conference on Availability, Reliability and Security*.
56. Pender, K., Cherkasova, S., Yamaoka-Enkerlin, A., (2019). Compliance and whistleblowing: How technology will replace, empower and change whistleblowers. *In FinTech*. Edward Elgar Publishing.
57. Ramdinmawii, E., Ghisingh, S., Sharma, U.M., (2014). A study on the cyber-crime and cyber criminals: A global problem. *International Journal of Web Technology,* 3.
58. Reddy, E., Minnaar, A., (2018). Cryptocurrency: A tool and target for cybercrime. Acta Criminologica: *African Journal of Criminology & Victimology,* 31(3).
59. Rhumorbarbe, D., Staehli, L., Broséus, J., Rossy, Q., Esseiva, P., (2016). Buying drugs on a Darknet market: A better deal? Studying the online illicit drug market through the analysis of digital, physical and chemical data. *Forensic science international,* 267.
60. Rose R., LeBlanc P., Fung B., DC Police Personnel Files Obtained by Hackers in Recent Ransomware Attack, Acting Police Chief Says [Online] Available at: <https://www.cnn.com/2021/04/29/politics/dc-police-ransomware-attack-personnel-files/index.html> [Last Accessed: June 11, 2024].
61. Sabillon, R., Cavaller, V., Cano, J., Serra-Ruiz, J., (2016). Cybercriminals, cyberattacks and cybercrime. *In 2016 IEEE International Conference on Cybercrime and Computer Forensic*.
62. Saleem, J., Islam, R., Kabir, M.A., (2022). The anonymity of the dark web: A survey. *IEEE Access, 10*.
63. Salvi, M.H.U., Kerkar, M.R.V., (2016). Ransomware: A cyber extortion. *Asian Journal For Convergence In Technology*, 2.
64. Sharma, N., Oriaku, E.A., Oriaku, N., (2020). Cost and effects of data breaches, precautions, and disclosure laws. *International Journal of Emerging Trends in Social Sciences,* 8(1).
65. Spagnoletti, P., Ceci, F., Bygstad, B., (2021). Online black-markets: An investigation of a digital infrastructure in the dark. *Information Systems Frontiers.*

66. Spalevic, Z., Ilic, M., (2017). The use of dark web for the purpose of illegal activity spreading. *Ekonomika,* 63(1).
67. Stohl, R., Grillot, S., (2009). The international arms trade. *Polity.* (Vol.7).
68. Sviatun, O., Goncharuk, O., Roman, C., Kuzmenko, O., Kozych, I.V., (2021). Combating cybercrime: economic and legal aspects. *WSEAS Transactions on Business and Economics,* 18.
69. Tavabi, N., Bartley, N., Abeliuk, A., Soni, S., Ferrara, E., Lerman, K., (2019). Characterizing activity on the deep and dark web. *In Companion proceedings of the 2019 world wide web conference*.
70. Tewari, S.H., (2020). Abuses of cryptocurrency in dark web and ways to regulate them. *SSRN 3794374*.
71. Trabelsi, S., (2019). Monitoring leaked confidential data. *In 2019 10th IFIP International Conference on New Technologies, Mobility and Security*.
72. Vargas, V.M., (2019). The new economic good: Your own personal data. An integrative analysis of the Dark Web. *In Proceedings of the International Conference on Business Excellence.* Vol. 13, No. 1.
73. Wang, M., Wang, X., Shi, J., Tan, Q., Gao, Y., Chen, M., Jiang, X., (2018). Who are in the Darknet? Measurement and analysis of darknet person attributes. *In 2018 IEEE Third International Conference on Data Science in Cyberspace*.
74. Wall, D., (2007). Cybercrime: The transformation of crime in the information age. *Polity,* (Vol. 4).
75. Weimann, G., (2016). Going dark: Terrorism on the dark web. *Studies in Conflict & Terrorism,* 39(3).
76. White, R., Kakkar, P.V., Chou, V., (2019). Prosecuting darknet marketplaces: Challenges and approaches. *Dep't of Just. J. Fed. L. & Prac.,* 67.
77. Zhang, H., Zou, F., (2020). A survey of the dark web and dark market research. *In 2020 IEEE 6th international conference on computer and communications*.
78. Zhang, Y., Xiao, Y., Ghaboosi, K., Zhang, J., Deng, H., (2012). A survey of cyber crimes. *Security and Communication Networks,* 5(4).