**Library Progress International** *Print version ISSN 0970 1052*
*Vol.44 No. 3, Jul-Dec 2024: P.18057-18070* *Online version ISSN 2320 317X*

*Original Article* *Available online at www.bpasjournals.com*

# The Effect Of Dark Web On National And International Security

**Prof. Dr Ahmed Orabi**

Dubai police science Academy

**How to cite this article**: Ahmed Orabi (2024). The Effect Of Dark Web On National And International Security. *Library Progress International,* 44(3), 18057-18070.

**ABSTRACT**

The immense technological advancement in communication tools in our modern era has become a reality aimed at human prosperity, linked to the information revolution that has facilitated life for humanity in various aspects, including economic, social, security, industrial, cultural, and educational areas. However, individuals with dangerous criminal tendencies have hastened to employ this modern technology to serve their criminal purposes. Highly skilled individuals in electronic technology and scientific knowledge have become involved in the world of crime, adversely affecting societies. This type of crime is not limited to local contexts but transcends borders and continents through the internet and various communication means, posing a security challenge at a global level. In light of this electronic danger, it has become necessary for international communities to establish security, technical, and legislative controls to combat cybercrime in its various forms to ensure the safe use of information technology.

**Keywords:** Dark Web, Cybercrimes, national security, databases, combating, international cooperation

## Introduction

"Exploring the Shadows: Cybercrimes in the Dark Web" investigates the clandestine aspects of the Internet where illicit activities thrive, and anonymity prevails. The Dark Web offers insight into the intricate network of cybercrimes flourishing in the obscure recesses of the internet. The dark web is a clandestine network accessible solely through specialized software. It serves as a sanctuary for numerous unlawful operations, such as identity theft, cyber espionage, and the trafficking of narcotics and arms. This research conducts comprehensive analysis, revealing how cybercriminals operate and detailing the tools and strategies they employ to evade law enforcement and exploit unsuspecting victims.

It underscores the vulnerabilities inherent in our increasingly interconnected society and elucidates the evolving landscape of cyber threats through case studies and expert analysis. This abstract underscore the necessity for stakeholders to collaborate and enforce robust cybersecurity protocols to mitigate the risks posed by cybercrimes on the dark web. "Exploring the Shadows" ultimately serves as a compelling call to action that advocates for more vigilance and awareness.

The dark web is a vast, unexplored segment of the internet shrouded in enigma and secrecy. This concealed network, inaccessible via traditional search engines, harbors a clandestine underbelly teeming with illicit activities and cyber enterprises. "Exploring the Shadows: Cybercrimes in the Dark Web" investigates this enigmatic realm to illuminate the intricacies of cybercrimes that flourish within it. The dark web, facilitated by anonymizing

software such as Tor, offers users unparalleled privacy and anonymity, rendering it an ideal sanctuary for malicious individuals seeking to evade detection and prosecution. [1]

A thriving black market for illegal goods and services, including weapons, narcotics, stolen data, and hacking tools, emerges within this digital wasteland. Moreover, the anonymity provided by cryptocurrency facilitates illicit transactions, rendering the dark web an attractive milieu for cybercriminal activities. This inquiry seeks to unveil the techniques employed by cybercriminals operating within the dark web. We want to study the strategies and techniques employed by these malefactors to perpetrate crimes such as fraud, identity theft, and cyber espionage through the examination of case studies and real-world examples. The dark web serves as a refuge for numerous cyber risks, including ransomware assaults, phishing operations, and clandestine forums that enable the exchange of criminal expertise. "Exploring the Shadows" elucidates the far-reaching consequences of cybercrimes in the digital age. Besides the immediate financial losses incurred by the victims, these illicit operations pose significant threats to individual privacy, economic stability, and national security. The interconnectedness of the internet amplifies the effects of cybercrimes, transcending national borders and legal constraints. This investigation underscores the necessity of implementing proactive measures to counteract cybercrimes on the dark web, considering the evolving nature of cyber threats. A comprehensive approach to mitigate these dangers must encompass enhanced cybersecurity protocols, collaboration between law enforcement and IT companies, and public awareness initiatives. Our objective is to furnish individuals and Organizations equipped with the necessary information and tools to navigate the digital realm securely and safely by illuminating the dark web.

Securing communication, information, electronic media, and information networks is no longer limited to a particular state; it has become a security message that all countries must cooperate to maintain, forming an indivisible security unit. This is crucial in the face of the intricate and evolving nature of cybercrime, which crosses borders and adapts technically, racing against the protective measures that countries seek to implement.

It is no longer a secret that the activities of cybercrime, used by organized criminal entities as a method for committing modern crimes, such as money laundering, drug trafficking, human trafficking, and organ trade, impact security in its broadest sense. The internet has not only become part of our lives but has also become our entire life, with every activity we engage in taking place online, from communicating with others via Facebook and WhatsApp to working and building projects.

The internet is a global communication system for transferring and exchanging data through various types of media among smaller networks interconnected by computers worldwide, operating under specific protocols known as Internet Protocol (TCP/IP). The term "internet" refers to the totality of information exchanged over the network and also to the infrastructure that transmits that information across continents.

**1-The three parts of the internet:**

**(First): The Surface Web** The surface web, also known as the visible web or indexed web, refers to the part of the internet that can be accessed and indexed by standard search engines like Google, Bing, and Yahoo. The internet comprises a set of computer networks of various types and sizes that connect to provide many services and information among individuals and groups relying on global messaging systems known as TCP/IP. This part of the web includes websites and content available to the public that can be easily found through typical search queries.

It encompasses a wide range of resources such as commercial websites, blogs, news sites, and social media platforms. Additionally, the surface web includes public databases and educational resources from institutions such as universities, as well as information from government websites and official public documents. Notably,

[1] Hilbert M (2020) Digital technology and social change: the digital transformation of society from a historical perspective. Dialog Clin Neurosci 22(2):189–194. https://doi.org/10.31887/dcns.2020.22.2/mhilbert

the size of the internet used in a typical manner does not exceed 10% of the total internet capacity, with the remaining percentages distributed between the deep web and the dark web.[2]

**(Second): The Deep Web** In contrast, the deep web contains parts of the web not indexed by search engines, including private databases and password-protected sites. Websites in this part of the deep internet cannot be archived or accessed by ordinary browsers, requiring special software for access. Moreover, deep web usage is difficult to trace as it relies on obscuring the user's serial number along with all of their data, making it challenging for security agencies to track criminals using such hidden sites.

The deep web's origins trace back to the end of the last century when an Irish youth named Ian Clarke presented a new project at the University of Edinburgh to study artificial intelligence and computer science. This project aimed at using the internet without tracking through the download of Clarke's program, intended for free distribution so that anyone could chat online, read, create a website, and share files while almost completely obscuring the user's identity. Although his project did not gain sufficient support from professors who found it somewhat strange, Clarke persevered and succeeded in launching his program called Freenet in 2000. Despite receiving negative publicity for its ability to host illegal materials, Clarke remained loyal to his project, which amassed over two million users in less than ten years.[3]

In reality, the deep web has garnered a bad reputation among the public, viewed as a source of much evil and criminal activity. However, this belief stems from a misunderstanding as people confuse the deep web with the dark web—which we will discuss later. The deep web contains many legitimate sites that some people turn to for increased protection not available on the surface web. Thus, it is natural for large companies, security agencies, the military, and intelligence agencies to utilize it for confidentiality and data protection. Additionally, the deep web serves as a refuge for many journalists, political dissidents, human rights advocates, and persecuted minorities, providing secure, encrypted, and fully protected communication for those unable to voice their opinions due to government oppression. Furthermore, the deep web hosts millions of vital documents and files that cannot be accessed through the surface web, allowing researchers to access extensive archives of necessary research materials along with critical information for NASA, weather data, economic organizations, and databases for major sites like WikiLeaks, among others.

However, you certainly won't get everything for free; you must pay the price, but this price is not in cash or bank transactions that can be easily traced, but in digital currencies called Bitcoin, which is a virtual encrypted currency ensuring protection and confidentiality for its users. For this reason, one might fall victim to scams when using this currency; if you buy something from the deep web and pay the seller, then he flees without providing what you wanted, you certainly won't be able to reach him since that currency conceals your identity and his. Like everything, the deep web is a double-edged sword; its provision of secrecy, protection, and almost complete freedom naturally leads to the emergence of the worst human conflicts and inclinations, which is known as the dark web or the back alleys of the deep web.

It is worth noting that the deep web is not part of the dark web; the deep web includes any part of the network that is not indexed by search engines, including websites that protect their content behind paywalls or password-protected sites, as well as your email contents. On the other hand, the dark web uses more complex encryption programs to provide greater security.

**(Third): The Dark Web** The dark web is a subset of the deep web that requires specific software to access and often hosts illegal activities; it is the deepest and most dangerous part of the deep internet. The dark web gained significant attention in 2001 when many security institutions reported the existence of dangerous dark networks

[2] Abbasi, Chen H (2007) Affect intensity analysis of dark web forums, presented at the IEEE intelligent of security information, May 2007

[3] Akhoondi M, Yu C, Madhyastha HV (2012) LASTor: a low-latency AS-aware tor client, presented at the IEEE symposium of security privacy, May 2012

operating secretly and engaging in illegal activities. This browser is considered the gateway to entering this hidden world, consisting of layers of communications that relay one another until they reach the final destination, with complex encryption at each stage, making it theoretically impossible to decrypt these networks.[4]

If you wonder about the hidden or strange activities in the dark web, the answer is that you will find everything forbidden imaginable and unimaginable—from counterfeit bills and stolen credit cards to banned books, stolen artworks, all types of drugs, unlicensed weapons, stolen goods, prohibited chemicals, bomb-making instructions, and electronic attacks, as well as forged official documents, hiring hitmen, human trafficking, and conducting medical experiments on victims. The most notorious criminal operations that occur on the dark web are known as "Red Rooms," where live broadcasts of killings, rapes, or tortures occur in exchange for exorbitant sums of money, often amounting to thousands of dollars paid by viewers. The minimum price to watch a show is one Bitcoin, equivalent to approximately $1,000 for an hour, with prices increasing depending on the event. Some individuals pay vast sums for VIP membership, allowing them to dictate how to torture the unfortunate victim and manage the event according to their sadistic tendencies.

In reality, the owners of these red rooms are intelligent; they target homeless individuals living on the streets or undocumented migrants, abducting the victims and scheduling the broadcasts while presenting different pricing for regular and VIP viewers. Prices can reach up to 250 Bitcoins ($250,000), with the final agreement established through the account displayed on the website.

Governments have made efforts to track these criminals through the dark web, as seen in 2013 when "Ross Ulbricht," the founder of a website called "Silk Road," was arrested. This site, created in 2011, was for illegal trade, allowing the purchase of drugs and weapons using the digital currency Bitcoin with complete anonymity regarding the identities of the parties involved.

Among the horrific cases apprehended by security forces is that of "Peter Scully," one of the most notorious criminals on the dark web. Born in Australia in 1963, he is mentally unstable and a well-known child predator who engaged in fraud and deception. He formed a gang specializing in child abduction for sexual abuse, broadcasting torture videos from dark web red rooms. However, he was arrested in 2015 and charged with 75 offenses of child abduction, torture, and rape alongside 40 accomplices.

Despite the dark web being associated in many minds with the world of crime, it also has a brighter side, hosting numerous scientific, cultural, and news platforms. For example, "Torbox" allows users to create an email account without needing personal information, relying solely on an email for privacy. Similarly, "Securedrop" enables users to send any information and data without anyone spying on or breaching it, allowing individuals with confidential files to send them securely.[5]

The researcher believes that the primary difference between the deep web and the dark web lies in the access method and available content. While the deep web contains legal and legitimate information and sites that are not easily accessible, the dark web comprises prohibited content and illegal activities.[6]

[4] Alipoaie A, Shortis P (2015) From dealer to doorstep—how drugs are sold on the dark net, GDPO situation analysis, Swansea University, Global Drugs Policy Observatory, Swansea, U.K., Technical Report

[5] Biddle P, England P, Peinado M, Willman B (2003) The Darknet and the future of content protection. In: Feigenbaum J (eds) Digital rights management. DRM 2002. Lecture notes in computer science, vol 2696. Springer, Berlin, Heidelberg

[6] Butler S (2018) Dark web history. https://www.technadu.com/dark-web-history/52017/

**2-The characteristics and typs of Dark Web's**

**2-1- The characteristics of Dark Web**

It is essential to understand the characteristics of the dark web and how it differs from the surface web, which is indexed by search engines, before exploring the realm of cybercrimes. All websites that are not indexed by search engines constitute the deep web, of which the dark web is a subset. Access to the dark web necessitates certain software, such as Tor (The Onion Router), unlike the surface web, which is accessible to anybody with an internet connection. Tor conceals users' IP addresses and ensures anonymity by encrypting each layer of internet data. The dark web functions as a refuge for numerous illicit activities due to its anonymity. Due to the anonymity afforded by cryptocurrencies such as Bitcoin, a market for illicit items and services has emerged. Dark web markets facilitate the buying and selling of many commodities, including firearms, narcotics, counterfeit currency, stolen information, and hacking tools. Moreover, forums and groups on the dark web function as a nexus for cybercriminals to exchange hacking techniques, collaborate on unlawful activities, and share expertise.

The dark web is a concealed segment of the World Wide Web that can only be accessed with a specialized browser called Tor. Dark web pages are not indexed by search engines, necessitating knowledge of the precise URL of the desired website.

This segment of the internet is commonly classified as "hazardous." The prevalent perception is that the dark web is a hub for various illicit activities, including drug trafficking and contract killing. The dark web harbors not only unlawful businesses but also various other risks.

The dark web can serve as a secure platform for journalists and whistleblowers to interact without restriction. Individuals from nations with stringent internet prohibitions may utilize the dark web for unrestrained communication. Visitors to the dark web should exercise extreme caution when downloading files, as they may infect your devices with viruses, malware, trojans, ransomware or other malicious files. At a minimum, users should ensure that their cybersecurity defenses are activated and up to date

**2-2-Distinguishes the black web from the deep web.**

Deep web denotes segments of the internet that are not indexed by search engines and necessitate authentication, such as passwords, for access. Conversely, the Dark Web is deliberately concealed and necessitates specialized software for access.

The internet comprises three primary components: the surface web, the deep web, and the black web. While some individuals conflate the phrases "deep web" and "dark web," this is inaccurate. Both are concealed from the general public online; yet, significant distinctions exist in their accessibility and utilization.

The surface web, sometimes referred to as the clear web, constitutes the portion of the internet that is predominantly accessed by users throughout their online activities. This content is freely accessible due to indexing by search engines such as Google. They index web content, categorise it, and facilitate searchability. [7]

Deep web: This segment of the internet is inaccessible by conventional search engines. The deep web is accessed when login credentials are required to enter accounts and circumvent paywalls. Whenever you access your email account, make online transactions, retrieve medical records, search corporate databases, or enter other sensitive internet areas, you are navigating the deep web.

[7] Pete Ildiko, Hughes Jack, Chua Yi T., Bada Maria, 2020, A Social Network Analysis and Comparison of Six Dark Web Forums, w: IEEE European Symposium on Security and Privacy Workshops, IEEE, s. 484–493 (https://doi.org/10.1109/EuroSPW51379.2020.00 071).

The dark web, or darknet, constitutes a segment of the deep web that is deliberately concealed and can only be accessed with specialized software such as the Tor browser. Political dissidents, whistleblowers, cybercriminals, and others seeking internet anonymity can utilize the dark web to render their activities largely untraceable.

**2-3-Types Of Cybercrimes in The Dark Web**

The dark web hosts a variety of cybercrimes, each characterized by distinct strategies, objectives, and consequences. The subsequent categories represent the most prevalent forms of cybercrime on the dark web:

• Drug trafficking: Illicit substances, including cocaine, marijuana, and synthetic chemicals, are easily obtainable on dark web marketplaces. Similar to authentic e-commerce platforms, these marketplaces enable sellers to list their products and permit customers to assess and criticize them. [8]

• Arms Trafficking: Illicit firearms and weaponry are frequently traded on the dark web. Consumers can readily purchase firearms, ammo, explosives, and other illicit commodities, often utilizing bitcoins to maintain anonymity. Cybersecurity and Cyber Laws: Issues and Challenges

• Compromised Data: Cybercriminals frequently sell credit card numbers, social security numbers, login credentials, and other personally identifiable information on the dark web.

Malware attacks, phishing tactics, and data breaches are prevalent methods for obtaining this information.

• Identity Theft: A prevalent cybercrime on the dark web is identity theft. Cybercriminals illicitly acquire personal information, such as driver's license numbers and social security numbers, to commit fraud or impersonate individuals. [9]

• Cyber Espionage: On the dark web, both nation-state actors and cybercriminal organizations engage in cyber espionage, acquiring confidential information from individuals, corporations, and government entities. This knowledge has political, economic, and strategic applications.

• Ransomware: In recent years, criminals have employed malicious software to encrypt victims' data and solicit ransom payments for the decryption keys. This has resulted in a heightened incidence of ransomware attacks. Ransomware operators utilize the dark web as a medium for communication and a payment processor for its victims.[10]

**2-4-Methods And Tactics of the Dark Web**

Cybercriminals operating on the dark web employ various approaches and methodologies to execute their illicit activities while evading discovery by law enforcement agencies. PGP (Pretty Good Privacy) and end-to-end encryption are prevalent encryption technologies employed to safeguard communications and transactions. These technologies hinder authorities' ability to gather and decipher data. The anonymity provided by the dark web complicates the identification and apprehension of cybercriminals for law enforcement agencies.[11]

---

[8] Johnson, L. R. (2019). "The Anatomy of Cybercrime: Understanding Dark Web Operations." International Journal of Cybersecurity Research, 5(1), 78-91.

[9] Alnabulsi Hussein, Islam Rafiqul, 2018, Identification of Illegal Forum Activities inside the Dark Net, w: Proceedings — International Conference on Machine Learning and Data Engineering, IEEE, s. 30–34.

[10] . Smith, J. (2020). "Dark Web Chronicles: Unveiling the Underworld of Cybercrime." Journal of Cybersecurity Studies, 8(2), 45-62.

[11] Radha Ranjan, Dr. Pallavi Singh, (2023). Cyber crime against women: A view, JyotirvedaPrasthanam

Tor, cryptocurrencies, and temporary email accounts are commonly employed to conceal the identities of individuals engaged in illicit activities.

Hackers routinely employ obfuscation techniques to conceal their traces and avoid detection. This may involve utilizing proxy servers, VPNs (Virtual Private Networks), and more

Cybersecurity and Cyber Laws: Issues and Challenges

anonymizing services to obscure their IP addresses and localities.

Cybercriminals can execute illicit transactions in a convenient and comparatively secure environment through dark web markets, which function similarly to regular e-commerce platforms. On these platforms, businesses offer a wide range of items and services, while consumers evaluate and critique them, fostering unlawful behaviour.Cybercriminals often utilise phishing methods to get personal information, such as bank account details and login credentials.

Cybercriminals impersonate legitimate businesses and organisations through fraudulent websites and emails to deceive victims into disclosing personal information. Furthermore, cybercriminals frequently employ malicious software, including ransomware and spyware, to infiltrate networks, expropriate data, and extort ransom payments from victims. [12]

Malware can propagate through various channels, including phishing emails, harmful websites, and more vectors. Consequently, both people and businesses are at significant risk.[13]

**3-The impact of the Dark Web on national security**

The security landscape of a country is evolving. Threats are mitigated while new problems emerge unexpectedly, rendering this an ongoing process of transformation. The Dark Web represents a novel phenomenon characterized by various threats and threat actors that national security experts must reconsents study. The Dark Web has outlined the primary activities on the Dark Web that could pose security risks to national security. This section delineates the impact of illicit Dark Web activity on national security components, emphasizing the primary issues and hazards involved. The intricate nature of national security necessitates interdependence among its pieces, such that a single detrimental action can impact multiple components. The issue of drug abuse is one of the multifaceted issues, cite just one example. Economic issues are highly intricate due to some types of crimes intersecting multiple domains of national security. Drug trafficking and trade impact on the economy, public safety, and healthcare system. In addition to the previously mentioned tax-related offences, the cryptocurrency marketplaces bolster the grey and black economies. [14]The trading of counterfeit goods adversely affects companies by diminishing their revenues and tarnishing their brand reputation and consumer trust. The trade in counterfeit monetary services, such as gift cards, credit cards, and other offerings using fraudulent or stolen bank accounts, undermines the financial system. Such crimes not only inflict harm but also undermine public confidence in these systems. State secrets, espionage. To safeguard the sovereignty of nations and defend their constitutional order, it

Journal, 12 (1), 97-100.

[12] Patel, N. J., & Chen, L. (2014). "From Hacking Havoc to Cyber Warfare: Battling Threats in the Digital Age." International Journal of Cybersecurity Policy, 2(1), 56-73.

[13] Radha Ranjan, Dr. Pallavi Singh, (2023)Cyber Crime Against Women in Cyber Space: A Critical Analysis of Indian Legislations, Kanpur Philosophers Journal
Volume X, Issue I(A),79-85.
Merriam-Webster. (n.d.). Security. In Merriam-Webster.com dictionary. Retrieved December 10, 2020, from https://www.merriam-webster.com/dictionary/security
*(PDF) THE EFFECT OF THE DARK WEB ON THE SECURITY*. Available from: https://www.researchgate.net/publication/354845415_THE_EFFECT_OF_THE_DARK_WEB_ON_THE_SECURITY [accessed Oct 24 2024]. [14]

is imperative to secure military and state secrets against nefarious attempts to obtain, expose, or alter them. It is often the responsibility of the national security services. They must identify and thwart endeavors and actions that jeopardize the political, economic, defense, and other interests of the nations. This assignment is highly complex and demanding, especially in the absence of the Dark Web. This additional domain complicates and exacerbates their duty. The concealed geolocation and anonymity present new hurdles to these businesses. Currently, there is no viable solution for eavesdropping on communications within the Dark Web, and the issues of de-anonymization and the identification of criminals remain significant concerns. The emerging difficulties necessitate novel solutions. Covert communication can, in certain instances, replace human contact; thus, there is no necessity to arrange dead drops or personal letterboxes in the physical realm, as clandestine sources can transmit their messages to the intelligence officer through the Dark Web. It also enables the revelation of state secrets. Regrettably, it is challenging or, in certain instances, unfeasible to identify the sources of disclosed state or corporate secrets[15].

In 2016, the NSA deployed specialized software kits designed for the collection of intelligence on adversaries. Almost one year later, WikiLeaks unveiled the Vault 7 and Vault 8 CIA projects, which are intricate covert information collection systems. The projects, along with their source codes and user instructions, are accessible on the Dark Web. On one side, these leaks inflicted significant damage on the US;[16] on the other hand, they enabled resource-limited countries to enhance their cyber capabilities by utilizing the source codes to manufacture their own cyber weapons. Unfortunately, these source codes and manuals are also accessible to black hat hackers, enabling them to construct malware. These occurrences have significantly altered the security landscape, and the damage and effects inflicted by leakers are incalculable in both the short and long term.[17]

**3-1-Economy**

The issue is highly intricate due to some types of crimes intersecting multiple domains of national security. Drug trafficking and trade impact on the economy, public safety, and the healthcare system. In addition to the previously mentioned tax-related offences, the cryptocurrency marketplaces bolster the grey and black economies. The trade in counterfeit goods adversely affects companies by diminishing their revenues and undermining the reputation of their brands and consumer confidence. The commerce of counterfeit currency-related services, such as gift cards, credit cards, and other offerings involving fraudulent or stolen bank accounts, undermines the financial system. Such crimes not only inflict harm but also undermine public trust in these systems

[15]Europol. 2018. Crime on The Dark Web: Law Enforcement Coordination Is The Only Cure. [online] Available at: https://www.europol.europa.eu/newsroom/news/crime-dark-web-law-enforcement-coordination-only-cure [Accessed 9 January 2021].

(PDF) THE EFFECT OF THE DARK WEB ON THE SECURITY. Available from: https://www.researchgate.net/publication/354845415_THE_EFFECT_OF_THE_DARK_WEB_ON_THE_SECURITY [accessed Oct 24 2024].

[16] MURALI, J. (2019). Human-trafficking on the dark-web. Retrieved 20 December 2020, from https://www.deccanchronicle.com/nation/in-other-news/020919/human-trafficking-on-the-dark-web.htm

*(PDF) THE EFFECT OF THE DARK WEB ON THE SECURITY*. Available from: https://www.researchgate.net/publication/354845415_THE_EFFECT_OF_THE_DARK_WEB_ON_THE_SECURITY [accessed Oct 24 2024].

[17] D.W. Perkins, 2020. Cryptocurrency: The Economics Of Money And Selected Policy Issues. [ebook] Washington: Congressional Re-search Service, Available at: https://crsreports.congress.gov/product/pdf/R/R45427 [Accessed 1 January 2021]

(PDF) THE EFFECT OF THE DARK WEB ON THE SECURITY. Available from: https://www.researchgate.net/publication/354845415_THE_EFFECT_OF_THE_DARK_WEB_ON_THE_SECURITY [accessed Oct 24, 2024].

**3-2-Classified information, intelligence gathering**

To ensure the sovereignty of nations and safeguard their constitutional order, it is imperative to protect military and state secrets against malicious attempts to obtain, expose, or alter them. The task typically lies with the national security services. They must identify and thwart endeavors and actions that jeopardize the political, economic, defense, and other interests of the nations. This assignment is exceedingly complex and carries significant responsibility, even in the absence of the Dark Web. This additional domain complicates and exacerbates their duty. The concealed geolocation and anonymity present new hurdles to these businesses. Currently, there is no viable solution for intercepting communications on the Dark Web, and the issues of de-anonymization and the identification of criminals remain significant concerns. The emerging difficulties necessitate novel solutions.

Covert communication can, in certain instances, replace human contact; thus, there is no necessity to arrange dead drops or personal letterboxes in the physical realm, as clandestine sources can transmit their messages to the intelligence officer through the Dark Web. It also enables the revelation of state secrets.

Regrettably, it is challenging or, in certain instances, unfeasible to identify the origins of disclosed state or corporate secrets.

An illustrative instance of the harm inflicted by hackers occurred in 2016 when the "Shadow Brokers" hacking group disseminated NSA's specialized software tools utilized for gathering intelligence on adversaries. Almost one year later, WikiLeaks released the Vault 7 and Vault 8 CIA projects, which are intricate covert information collection systems. The projects, along with their source codes and user instructions, are accessible on the Dark Web. On one side, these leaks inflicted significant damage on the US; on the other hand, they enabled resource-limited countries to enhance their cyber capabilities by utilizing the source codes to manufacture their own cyber weapons. Regrettably, these source codes and manuals are accessible to black hat hackers, enabling them to create malware. These instances have significantly altered the security environment; the losses and effects inflicted by leakers are incalculable in both the short and long term.[18]

**3-3- Public safety and security**

Many of the previously described offences jeopardize public safety and security in various ways. The Dark Web serves as an optimal setting for criminals due to its provision of anonymity and concealed geolocation for unlawful activity. The increasing popularity of cryptocurrency marketplaces is complicating the responsibilities of law enforcement agencies. Despite its relatively limited societal penetration, its threat is significantly more than it initially appeared. This new media presents unexpected capabilities and potential risks.

The perception of public safety and security relies on the belief that both major offenders and minor criminals are prosecuted and arrested by law enforcement agencies. However, on the Dark Web, the likelihood of apprehending minor criminal offenders is minimal, as the resources allocated to such identification are disproportionate to the potential gains. Most small criminals evade consequences for purchasing drugs, counterfeit items, and other misdemeanors. It conveys a detrimental and degrading message on social morality to society. This is one of the contributing elements to the increasing popularity of the Dark Web. Furthermore, these concealed systems exhibit enhanced security with an increased number of users. This is a quintessential catch-22 scenario. [19]

[18] Tranfield David, Denyer David, Smart Palminder, 2003, Towards a Methodology for Devel oping Evidence-Informed Management Knowledge by Means of Systematic Review, „British Journal of Management", t. 14(3), s. 207–222 (https://doi.org/10.1111/1467-8551.00 375).

[19] Przepiorka Wojtek, Norbutas Lukas, Corten Rense, 2017, Order without Law: Reputation Promotes Cooperation in a Cryptomarket for Illegal Drugs, „European Sociological Review", t. 33(6), s. 752–764.

**4-The Challenges of combating cybercrimes on the dark web**

Legislators, cybersecurity specialists, and law enforcement agencies encounter numerous challenges in combating cybercrimes on the dark web. The primary challenges include:

• Anonymity: The dark web provides a significant barrier for law enforcement agencies in identifying and apprehending cybercriminals due to the anonymity it affords. Advanced encryption and obfuscation methods may render conventional investigative approaches ineffective. [20]

• Jurisdictional Challenges: The worldwide nature of the internet complicates efforts to address cybercrimes on the dark web, particularly when such offences originate from nations with inadequate or absent cybercrime legislation. Foreign law enforcement agencies must collaborate and coordinate effectively to address these concerns. 21

• Technological Complexity: Cybersecurity professionals tasked with safeguarding against cybercrimes have an ongoing challenge due to the rapid advancement of technology. Defenders must consistently monitor and adjust to emerging tactics and strategies employed by cybercriminals to exploit vulnerabilities in hardware and software.

• Resource Limitations: Antiquated infrastructure, insufficient personnel, and limited financial resources are among the challenges commonly faced by law enforcement and cybersecurity agencies. The dark web necessitates

• Privacy Concerns: Politicians must navigate the delicate equilibrium between safeguarding privacy and anonymity and the imperative to combat cybercrimes. It is essential to use caution while formulating policies aimed at enhancing cybersecurity and combating cybercrime to safeguard individuals' civil liberties and privacy rights.

**5-International Digital Security Cooperation to Combat Cybercrime on the Dark Web:** Despite the advantages arising from technological progress, digital challenges remain due to widening digital gaps, electronic threats, and human rights violations on the internet. Combating internet crimes can only be achieved if international cooperation develops through direct communication among security agencies across nations, coordinating efforts to pursue criminals and combat crimes that transcend state boundaries. This digital security cooperation must be advanced enough to keep pace with the rapid development of internet crimes, effectively countering them and apprehending their perpetrators.[22]

This collaboration enables us to face a more secure and stable international digital community, reinforcing the rule of law and combating digital crime in all its forms. Moreover, international digital security cooperation significantly contributes to reducing and ultimately eliminating internet crime, necessitating active engagement

[20]Reid, J., & Fox, B. (2020). Human Trafficking and the Darknet: Technology, Innovation, and Evolving Criminal Justice Strate-gies. In Advanced Sciences and Technologies for Security Applications (pp. 77–96). Springer International Publishing. https://doi.org/10.1007/978-3-030-41287-6_5 *(PDF) THE EFFECT OF THE DARK WEB ON THE SECURITY*. Available from: https://www.researchgate.net/publication/354845415_THE_EFFECT_OF_THE_DARK_WEB_ON_THE_SECURITY [accessed Oct 24 2024].

[21] Brown, E. R. (2013). "Cyber Shadows: Exploring the Dark Side of the Internet." Journal of Cybersecurity Research, 4(2), 89-106.

[22] Gehl RW (2014) Power/freedom on the dark web: a digital ethnography of the dark web social network. New Media & Society, Oct 15. http://nms.sagepub.com/content/early/2014/10/16/1461444814554900.full#ref-38

among countries to enhance efforts in promoting and activating this cooperation, creating collaborative security measures capable of preventing these crimes and tracking their perpetrators when they occur.[23]

Such collaboration is crucial in fighting digital crime due to the nature and specificity of these offenses, as well as their status as one of the most dangerous modern criminal systems, given the severe damages they inflict on all facets of international and national society. In light of the changes occurring globally, no country, regardless of its power and development level, can confront crime alone due to the extensive scope of these crimes and their cross-border implications.[24]

Digital security cooperation among countries emphasizes the exchange of experiences among security agencies broadly, enhancing their capability to deter criminal groups. This digital cooperation provides information and data that would be impossible to gather at the level of a single state, facilitating monitoring and preparation against members of criminal, terrorist, and cyber groups. The cross-border nature of this crime necessitates broad and continuous channels, especially in terms of information gathering and inquiries.,**Therefore, countries must cooperate in the following areas**:[25]

- **Enhancing communication channels** among their authorities, agencies, and relevant departments, establishing these channels when necessary, to facilitate the secure and rapid exchange of information regarding all aspects of crimes covered by this agreement, including their connections to other criminal activities such as the identities of suspected individuals, their locations and activities, the movement of criminal proceeds, and the movement of property or equipment used or intended for use in committing these crimes.
- **Establishing communication channels** among their specialized agencies and maintaining those channels to facilitate the desired rapid exchange of information related to all aspects of crimes occurring on the internet.
- **Creating a database** to collect and analyze information about these crimes, including information provided by countries and regional and international organizations, compiling comprehensive lists in this regard, retaining and updating them, and sharing information with countries on all crimes such as terrorism, organized crime (human trafficking, money laundering, child abduction, drug trafficking, etc.).
- **Ensuring that each state party notifies** any other state party promptly of any information it has regarding any crime occurring on the internet in general and particularly within the dark web's recesses that occur within its territory, specifying the circumstances surrounding the crime, the perpetrators, the victims, and the consequences, as well as the methods used in its commission, according to the applicable laws and regulations in the state.
- **Exchanging information and experiences** and establishing databases to collect and analyze information about criminal activities occurring in the dark web, detailing the names of offenders, their leadership, organizational structures, their locations, means of financing, and training methods, according to each party's internal laws and procedures.
- **Developing and strengthening monitoring methods** and information exchange to uncover plans or activities aimed at transporting, importing, exporting, storing, or using weapons, ammunition, explosives, and other materials that facilitate criminal acts across borders illegally.[26]

[23] Love D (2013) There's a secret internet for drug dealers, assassins, and pedophiles. Business Insider, Mar 6

[24] White, A. B. (2018). "Navigating the Shadows: Exploring Cybercrimes in the Dark Web." Cybersecurity Review, 12(3), 112-129.

[25] WoodhamsJessica,KloessJulianeA.,JoseBrendan,Hamilton-GiachritsisCatherineE.,2021, Characteristics and Behaviors of Anonymous Users of Dark Web Platforms Suspected of Child Sexual Offenses, „Frontiers in Psychology", t. 12 (https://doi.org/10.3389/fpsyg.2021. 623668).

[26] Garcia, M. S., & Patel, R. K. (2017). "Cybercrime Trends: Insights from Dark Web Marketplaces." Journal of Cybersecurity Analysis, 3(4), 201-218.

- **Cooperating in conducting investigations** to exchange information about specified crimes to identify individuals with reasonable suspicion of involvement in these crimes, their locations and activities, and the flow of funds connected to committing these crimes.
- **Exchanging information about advanced methods and new systems** to combat these crimes occurring on the dark web.
- **Creating a criminal record** whereby each state party may adopt any legislative or other measures necessary to take into account, as deemed appropriate, any conviction previously issued against the alleged perpetrator in another state for use in related criminal proceedings regarding a criminal act under this agreement.
- **Establishing a database** on national legislations, investigative techniques, and the most successful practices and experiences related to the prevention and combat of internet crimes.
- **Ensuring that state parties maintain the confidentiality** of exchanged information and do not provide it to any non-party state or entity without prior consent from the information source state.
- **Exchanging information and experiences** related to discovered crimes, the advanced and new systems in combating them, such as investigative techniques and preventive measures taken.
- **Cooperating in providing mutual assistance** to one another regarding the procedures and apprehension of fugitives involved in cases or those wanted for crimes committed on the dark web.
- **Enhancing capacities, knowledge, and technical capabilities** in the cyber field through training programs, projects, tools, and platforms to build cyber capabilities, enabling police forces in countries to effectively combat cybercrime.
- **Cooperating in combating cybercrime** by activating the role of joint training between police agencies at the level of investigations and technical examination tools and methods.
- **Establishing an independent administration** alongside the departments responsible for information networks that seek to mitigate internet risks, tasked with addressing the hidden internet (Dark Web & Deep Web), which poses significant dangers to society as it facilitates all types of violations, including the risks associated with the Internet of Things (IoT), given that the new generation of the internet represents a threat to society that must be confronted.[27]

**Conclusions**

This study elucidates the backdrop of the dark web and its implications for national security challenges. Crimes in the new digital realm adversely affect nearly every aspect of national interests, as demonstrated in the preceding sections. The prevalence of the Dark Web in countries today remains comparatively limited; nonetheless, its impact on societies is more significant than anticipated given its size. This segment of the cyber realm obscures physical and moral borders, presenting a substantial and escalating threat to national security, with ramifications for the economy, public safety, public health, and democratic institutions. The European Union recognized that the sole remedy for emerging sickness is the collaboration among Law Enforcement Agencies. Europol has formed a specialized Dark Web Team to collaborate with EU partners in reducing the prevalence of illicit cryptocurrency exchanges. The team will build a coordinated strategy that includes information exchange, operational support, and experience in various crime types, as well as the creation of tools, tactics, and procedures to assist investigators in identifying threats and targets. An exemplary instance of cooperation is the closing of the “Alpha Bay” and “Hansa” cryptocurrency markets. The two markets accounted for almost 350,000 illegal items, including narcotics, weapons, and cybercrime equipment. Europol, 2018Dark Web applications are created by passionate volunteers whose objective is not to facilitate criminal activity, but rather to offer digital freedom to individuals who deem it essential. There are specialized platforms for whistleblowers and journalists' informants, as well as for human rights campaigners, revolutionaries, and free thinkers in repressive nations. The potential for unrestricted speech devoid of restraint

[27] Kim, D. H., & Lee, S. H. (2016). "Unmasking Cybercriminal Networks: A Case Study of Dark Web Operations." International Journal of Cyber Investigations, 9(2), 145-162.

**References**

Abbasi, Chen H (2007) Affect intensity analysis of dark web forums, presented at the IEEE intelligent of security information, May 2007

Akhoondi M, Yu C, Madhyastha HV (2012) LASTor: a low-latency AS-aware tor client, presented at the IEEE symposium of security privacy, May 2012

Alipoaie A, Shortis P (2015) From dealer to doorstep—how drugs are sold on the dark net, GDPO situation analysis, Swansea University, Global Drugs Policy Observatory, Swansea, U.K., Technical Report

Alnabulsi Hussein, Islam Rafiqul, 2018, Identification of Illegal Forum Activities inside the Dark Net, w: Proceedings — International Conference on Machine Learning and Data Engineering, IEEE, s. 30–34.

Biddle P, England P, Peinado M, Willman B (2003) The Darknet and the future of content protection. In: Feigenbaum J (eds) Digital rights management. DRM 2002. Lecture notes in computer science, vol 2696. Springer, Berlin, Heidelberg

Butler S (2018) Dark web history. https://www.technadu.com/dark-web-history/52017/

Gehl RW (2014) Power/freedom on the dark web: a digital ethnography of the dark web social network. New Media & Society, Oct 15. http://nms.sagepub.com/content/early/2014/10/16/1461444814554900.full#ref-38

Love D (2013) There's a secret internet for drug dealers, assassins, and pedophiles. Business Insider, Mar 6

Smith, J. (2020). "Dark Web Chronicles: Unveiling the Underworld of Cybercrime." Journal of Cybersecurity Studies, 8(2), 45-62.

Johnson, L. R. (2019). "The Anatomy of Cybercrime: Understanding Dark Web Operations." International Journal of Cybersecurity Research, 5(1), 78-91.

White, A. B. (2018). "Navigating the Shadows: Exploring Cybercrimes in the Dark Web." Cybersecurity Review, 12(3), 112-129.

Radha Ranjan, Dr. Pallavi Singh, (2023) Cyber Crime Against Women in Cyber Space: A Critical Analysis of Indian Legislations, Kanpur Philosophers Journal Volume X, Issue I(A),79-85.

Garcia, M. S., & Patel, R. K. (2017). "Cybercrime Trends: Insights from Dark Web Marketplaces." Journal of Cybersecurity Analysis, 3(4), 201-218.

Kim, D. H., & Lee, S. H. (2016). "Unmasking Cybercriminal Networks: A Case Study of Dark Web Operations." International Journal of Cyber Investigations, 9(2), 145-162.

Patel, N. J., & Chen, L. (2014). "From Hacking Havoc to Cyber Warfare: Battling Threats in the Digital Age." International Journal of Cybersecurity Policy, 2(1), 56-73.

D.W. Perkins, 2020. Cryptocurrency: The Economics Of Money And Selected Policy Issues. [ebook] Washington: Congressional Re-search Service, Available at: https://crsreports.congress.gov/product/pdf/R/R45427 [Accessed 1 January 2021]

(PDF) THE EFFECT OF THE DARK WEB ON THE SECURITY. Available from:

https://www.researchgate.net/publication/354845415_THE_EFFECT_OF_THE_DARK_WEB_ON_THE_SECURITY [accessed Oct 24, 2024].

Europol. 2018. Crime on The Dark Web: Law Enforcement Coordination Is The Only Cure. [online] Available at: https://www.europol.europa.eu/newsroom/news/crime-dark-web-law-enforcement-coordination-only-cure [Accessed 9 January 2021].

(PDF) THE EFFECT OF THE DARK WEB ON THE SECURITY. Available from: https://www.researchgate.net/publication/354845415_THE_EFFECT_OF_THE_DARK_WEB_ON_THE_SECURITY [accessed Oct 24 2024].

Reid, J., & Fox, B. (2020). Human Trafficking and the Darknet: Technology, Innovation, and Evolving Criminal Justice Strate-gies. In Advanced Sciences and Technologies for Security Applications (pp. 77–96). Springer International Publishing. https://doi.org/10.1007/978-3-030-41287-6_5
*(PDF) THE EFFECT OF THE DARK WEB ON THE SECURITY*. Available from: https://www.researchgate.net/publication/354845415_THE_EFFECT_OF_THE_DARK_WEB_ON_THE_SECURITY [accessed Oct 24 2024].

Reid, J., & Fox, B. (2020). Human Trafficking and the Darknet: Technology, Innovation, and Evolving Criminal Justice Strate-gies. In Advanced Sciences and Technologies for Security Applications (pp. 77–96). Springer International Publishing. https://doi.org/10.1007/978-3-030-41287-6_

Reidy, E., 2020. How Did COVID-19 Affect Migration In 2020?. [online] The New Humanitarian. Available at: https://www.thenewhu-manitarian.org/news-feature/2020/12/22/Migration-forced-displacement [Accessed 23 December 2020]
*(PDF) THE EFFECT OF THE DARK WEB ON THE SECURITY*. Available from: https://www.researchgate.net/publication/354845415_THE_EFFECT_OF_THE_DARK_WEB_ON_THE_SECURITY [accessed Oct 24 2024].

Pete Ildiko, Hughes Jack, Chua Yi T., Bada Maria, 2020, A Social Network Analysis and Comparison of Six Dark Web Forums, w: IEEE European Symposium on Security and Privacy Workshops, IEEE, s. 484–493 (https://doi.org/10.1109/EuroSPW51379.2020.00 071).

Przepiorka Wojtek, Norbutas Lukas, Corten Rense, 2017, Order without Law: Reputation Promotes Cooperation in a Cryptomarket for Illegal Drugs, „European Sociological Review", t. 33(6), s. 752–764.

Tranfield David, Denyer David, Smart Palminder, 2003, Towards a Methodology for Devel oping Evidence-Informed Management Knowledge by Means of Systematic Review, „British Journal of Management", t. 14(3), s. 207–222 (https://doi.org/10.1111/1467-8551.00 375).

Hilbert M (2020) Digital technology and social change: the digital transformation of society from a historical perspective. Dialog Clin Neurosci 22(2):189–194. https://doi.org/10.31887/dcns.2020.22.2/mhilbert

WoodhamsJessica,KloessJulianeA.,JoseBrendan,Hamilton-GiachritsisCatherineE.,2021, Characteristics and Behaviors of Anonymous Users of Dark Web Platforms Suspected of Child Sexual Offenses, „Frontiers in Psychology", t. 12 (https://doi.org/10.3389/fpsyg.2021. 623668).