iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** VIII **Month of publication:** Aug 2023

DOI: https://doi.org/10.22214/ijraset.2023.55259

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue VIII Aug 2023- Available at www.ijraset.com

Combating Dark Web Terrorism: Strategies for Disruption and Prevention

Ngaira Mandela[1], Tumaini Mbinda[2], Felix Etyang[3]
School of Digital Forensics and Cyber Security, National Forensic Sciences University, Gandhinagar, India

Abstract: ***Dark web platforms have emerged as a significant concern in the context of global security, with the potential to facilitate and amplify terrorism activities. This paper presents an analysis of the evolving landscape of dark web terrorism and proposes strategies for combating this emerging threat. The study begins by examining the characteristics and functionalities of the dark web that make it attractive to terrorist organizations, including anonymity, encrypted communications, and illicit marketplaces. It further explores the methods employed by terrorists to exploit the dark web for recruitment, propaganda dissemination, and coordination of attacks. To counteract this growing menace, a comprehensive framework for combating dark web terrorism is introduced. The proposed strategies encompass various dimensions, such as technological advancements, international collaboration, legislative measures, and law enforcement efforts. Technological approaches focus on enhancing digital surveillance capabilities, developing advanced data analytics tools, and improving cybersecurity measures to disrupt terrorist networks operating in the dark web. International cooperation is emphasized to foster information sharing, intelligence coordination, and joint operations among nations to counter the cross-border nature of dark web terrorism. By implementing these multifaceted strategies, governments, law enforcement agencies, and technology providers can collectively mitigate the threats posed by dark web terrorism.***

Keywords: Dark Web, Darknet, Terrorism, Terrorist organizations, Tor browser, Dark web monitoring, internet governance

I. INTRODUCTION

The emergence of the Dark Web has introduced new challenges in the fight against terrorism. This covert and encrypted corner of the internet provides a breeding ground for illicit activities, including the recruitment, coordination, and financing of terrorist organizations [1]. As governments and law enforcement agencies strive to combat terrorism, it has become crucial to understand how terrorists exploit the Dark Web and to develop effective strategies to counter this emerging threat.

The Dark Web is the encrypted and anonymous part of the internet that cannot be accessed through traditional search engines. It operates on overlay networks and relies on encryption and anonymization technologies to ensure the privacy and anonymity of its users [2]. While the Dark Web offers a level of secrecy that can be appealing to various actors, it has also become an attractive platform for terrorists seeking to further their agendas.

This research paper aims to provide a comprehensive analysis of the use of the Dark Web for terrorism-related activities. By delving into the mechanisms employed by terrorist organizations, including recruitment, radicalization, fundraising, communication, and the acquisition of illicit goods and services, we can gain insights into the extent and impact of their activities on the Dark Web.

Understanding the tactics and strategies used by terrorists on the Dark Web is essential for policymakers, law enforcement agencies, and counterterrorism experts. It enables them to identify vulnerabilities, develop proactive measures, and formulate effective responses to mitigate the risks associated with this covert online environment.

This research paper will explore various case studies of prominent terrorist organizations and incidents where the Dark Web played a significant role. By analyzing these examples, we can gain a deeper understanding of the complexities and challenges posed by the intersection of terrorism and the Dark Web.

Furthermore, this study will delve into the technical challenges in monitoring and tracking terrorist activities on the Dark Web, as well as the legal and policy considerations that arise when combating terrorist use of this covert platform. Striking the right balance between security and privacy is a delicate task, and this research aims to shed light on the ethical and privacy implications associated with monitoring the Dark Web.

The insights and findings presented in this research paper will contribute to the ongoing discourse on counterterrorism strategies and inform the development of effective measures to combat the use of the Dark Web for terrorism-related activities. Collaboration between international agencies, law enforcement entities, and technology companies will be crucial in developing proactive approaches and enhancing information sharing to stay ahead of terrorists in this constantly evolving landscape

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue VIII Aug 2023- Available at www.ijraset.com

II. LITERATURE REVIEW

The Internet we inhabit is a complex, multi-layered structure, as depicted in the Internet iceberg diagram in figure 1. It comprises of the surface network and the deep web, which includes the dark web.

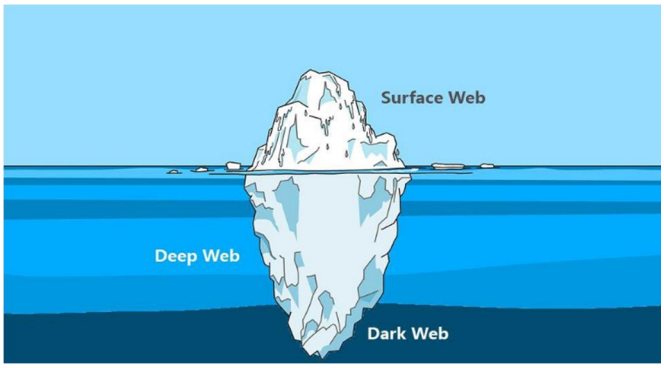


Figure 1: Internet anatomy[3]

The surface network encompasses websites that are readily accessible and searchable through standard search engines. These sites, such as news portals, shopping platforms, and forums, represent only a fraction of the entire Internet, roughly accounting for about 4% of its content [4]. However, it is crucial to note that this surface content merely scratches the surface, as there is much more hidden beneath.

Underneath the surface network lies the deep web, comprising of information that cannot be accessed via conventional search engines. This includes private communication records like chat histories on messaging platforms such as WeChat, private messages on social media platforms like Weibo, and personal email information. Essentially, any content that is not crawlable by search engines falls into the category of the deep web. It is important to recognize that the deep web is a concept that pertains specifically to search engines and refers to private and inaccessible content [4]. Within the deep web, there exists a subset known as the dark web, which can be accessed but requires specialized tools and methods. The dark web employs encrypted communication, peer-to-peer networks, and obfuscation techniques to provide users with anonymous access to Internet resources. Anonymity is a central feature of the dark web, as it deliberately conceals relevant information to prevent identity tracing. Consequently, the dark web has become a breeding ground for cybercrime and poses significant challenges in combating various forms of criminal activities, including cyber fraud, which jeopardizes national security [5]. To access the dark web, specialized tools and software are required to ensure anonymity and secure communication. The most commonly used tool to access the dark web is the Tor (The Onion Router) network.

The Tor network is a system that enables anonymous communication and access to hidden services on the internet. It utilizes a multi-layered encryption and multiple forwarding mechanisms to ensure privacy and security for its users. The Tor network consists of routing nodes, an authoritative directory server, Tor clients, bridge nodes, and hidden servers [6].

Routing nodes are operated by volunteers around the world and form a distributed overlay of networks. The authoritative directory server manages these routing nodes and publishes information about them in a "consensus" list, which is updated every hour. Tor clients, installed on users' devices, access the authoritative directory server to obtain routing node information.

To establish an anonymous communication link, the Tor client selects three routing nodes: an entry node, an intermediate node, and an exit node. The client negotiates with each node to generate shared communication keys for each segment of the data transmission link. The Tor client encrypts the information in layers using the generated keys, creating a three-layer encrypted data packet resembling a wrapped onion [7].

The Tor client sends the encrypted data packet to the entry node, which decrypts the first layer of encryption. The entry node then forwards the packet to the intermediate node, which decrypts the second layer. Finally, the intermediate node sends the packet to the exit node, which decrypts the third layer and obtains the original information. The exit node can connect to the destination server, enabling anonymous communication from the user to the server [8].

Throughout the communication process, the Tor network ensures that the destination server can only detect the IP address of the exit node, making it difficult to trace the IP address of the information sender. The information content and forwarding routing information are encrypted layer by layer, and only the user's Tor client possesses all the decryption keys.

The Tor network started as a project of the U.S. military, aiming to provide anonymity for intelligence personnel. It was later released as a general user version in 2004 and is currently maintained by the Electronic Frontier Foundation (EFF). The Tor system has gained popularity among government departments, social organizations, and individual users seeking anonymous communication and internet access [9].

Apart from anonymous access to legitimate websites on the surface web, the Tor system also supports hidden services. Hidden servers and hidden service directory servers are integrated into the Tor software package. Hidden servers provide various network services while preserving the anonymity of the service providers and users. The hidden service directory server stores and provides information about hidden servers, such as introduction points and public keys.

The dark web, enabled by the Tor network, initially attracted groups marginalized by mainstream values, such as extreme liberals, anarchists, and those with discriminatory ideologies. However, it has also been exploited by criminals, leading to serious social harm. The dark web consists of secret websites that cannot be indexed by general search engines. Criminal activities, secret forums, chat rooms, and anonymous transactions take place within this hidden network [10].

The rise of encrypted digital currencies, starting with Bitcoin in 2009, further facilitated secret transactions on the dark web. Bitcoin introduced a decentralized electronic cash system that operates independently of central banks or financial institutions. Its characteristics of decentralization, algorithm-based generation, and cryptographic security makes it suitable for anonymous transactions and ownership protection.

III. DARK WEB USAGE FOR TERRORISM

Terrorism has used the Internet as its tool since the beginning of the 21st century. In the beginning, terrorists mainly used the Internet to conduct internal communications, organize terrorist activities, and propagate extremist ideas, spread terrorist information, and recruit personnel on the surface network [11]. The trend of online terrorism has quickly attracted the attention of national security agencies and anti-terrorism departments around the world, and quickly mobilized forces to closely monitor terrorist websites and forums opened by terrorists in social media. In 2009, the United Nations Counter-Terrorism Task Force Task Force (CTTTF) defined cyber-terrorism crimes into four categories, namely, cyber-terrorist attacks, using the Internet to spread illegal information related to terrorist activities, using the Internet to communicate and finance terrorist activities, and using the Internet to communicate and finance terrorist activities. The Internet collects information and acquires technology [12]. Because the behavior of the surface network is easy to be located, tracked, and traced, with the continuous improvement and improvement of network anti-terrorism means, the risk of terrorists carrying out the above crimes is increasing. For example, every move of the "Islamic State" (ISIS) on the surface network is closely monitored by all countries. All countries use effective technical means to block or filter extremist content, and use IP address positioning and other means to track and arrest terrorists. In this case, the dark web undoubtedly provides a more ideal tool for terrorists. In recent years, terrorist activities have shifted to the dark web. The secret information services and secret transaction functions of the dark web have provided unprecedented convenience for terrorist activities and brought new severe challenges to combating cyber terrorism. At present, darknet terrorist activities mainly fall into the following categories [13].

A. Internal Liaison and External Publicity

The dark web provides terrorists with a Secure internal communication tool, enabling them to covertly exchange information and connect more broadly to plan, organize, deploy, and carry out terrorist activities. Terrorist organizations also use the dark web to promote extremist ideas [11].

For example, after Al Qaeda's propaganda activities on the surface network were attacked, in December 2015, they published the "Tor Browser Security Guidelines" online, detailing explanation on how to download, install and use the tool, they guided target users to transfer to the dark web, and taught them how to prevent being located and identified by anti-terrorism departments. The terrorist organization also backs up the propaganda information of the surface network to the dark web site. When the surface network website is blocked, it publishes the link address of the mirror site on the dark web through anonymous forums, chat rooms or emails, and directs members and supporters to go there. For example, in December 2015, Islamic State terrorists planned a shooting bombing in Paris, France, and then quickly moved their propaganda machine, the Al-Hayat Media Center, to the dark web and posted on the Shamikh forum. This website is a mirror website that mirrors the information of many bulletin boards, including videos and documents translated into multiple languages accumulated over the years [11].

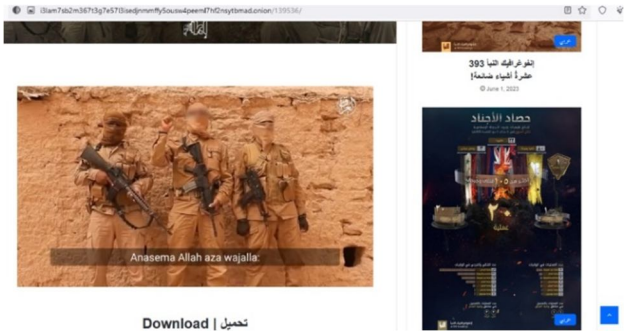


Figure 2: Communication videos by Islamic state on the dark web

B. Recruitment and Training of Personnel.

Terrorist organizations are also recruiting new members on the dark web and providing skills training for followers around the world, such as setting up training courses on how to make bombs and how to carry out terrorist attacks, especially training "lone wolf" attackers, which has caused huge losses. "Lone wolves" refers to people who have received radical education on terrorism, buy or self-made weapons and devices, and launch terrorist attacks on their own. Due to the anonymity of the dark web, the anti-terrorist department cannot know where and which people have been successfully brainwashed by terrorist organizations [14]. Therefore, the "lone wolf" attack has the characteristics of long incubation period and high randomness, which makes it hard for the security department to guard against and relies on the traditional anti-terrorist model which is difficult to deal with. From the above, it can be seen that terrorist organizations use the world connectivity and anonymity of the dark web to try their best to spread terrorism on a global scale, making the counter-terrorism situation even more severe.

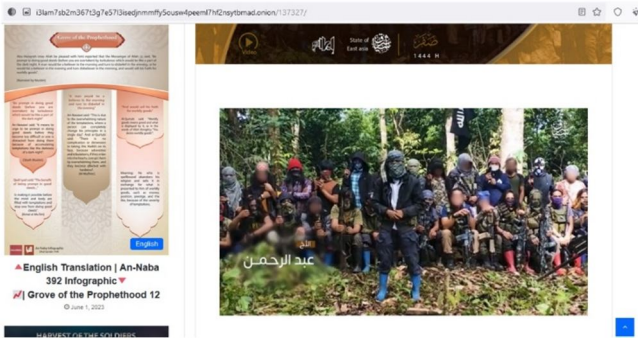


Figure 3:Terrorism training videos

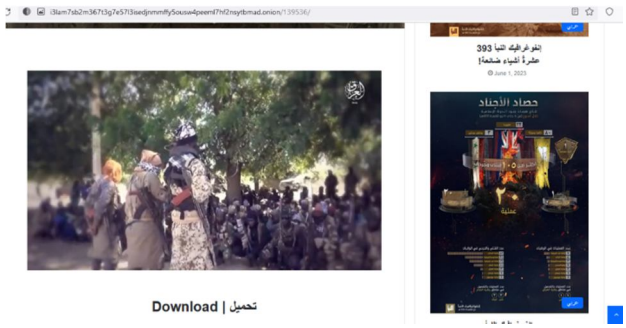


Figure 4: videos on the dark web training

C. Raising and Transferring Funds

In addition to traditional methods such as oil sales, smuggling, and kidnapping, terrorist organizations raise funds. In recent years, new methods have been derived from digital cryptocurrencies and the dark web, such as bitcoin donations, online extortion, human trafficking, and organ trading. An American terrorist group claiming to be linked to the Islamic State claimed in an online fundraiser: "It is impossible to transfer a bank to a jihadist group, and jihadists under infidel governments should be aware that a possible.

The way is to use Bitcoin to make anonymous donations, which can provide millions of dollars' worth of Bitcoin wealth to the jihad, and every penny in the pocket of every jihadist will become an inexhaustible motivation to support the jihad."[15] The hacker group Ghost Sec, which fights terrorist groups, has tracked down a bitcoin wallet worth $3 million, confirming that the digital currency has become a new channel for terrorist groups to raise funds. The characteristics of Bitcoin's suitability for money laundering have also been fully exploited by terrorists. For example, the funds accepted by the Jemaah Islamiyah are all through the Bitcoin trading platform of the "dark net", and the Fund the Islamic Straggle without Leaving a Trace), which converts jihadist fundraising funds into a dark web mirror of Bitcoin, and guides how to use the dark web for secret financial transactions through a tutorial called "Bitcoin and the Charity of Violent Physical Struggle"[16]. In addition, terrorist organizations also make money from illegal transactions on darknet platforms, such as human trafficking, sex slaves, the sale of looted antiques, and human organs harvested from captives.

D. Purchase of Weapons and Destructive Devices

The dark web black market has long been an "arsenal" for terrorists, and it is relatively easy to buy guns and ammunition on illegal trading sites such as "Silk Road". For example, the weapons used by the "Islamic State" in the Paris terrorist attack were purchased through the dark web. According to the official documents of the Stuttgart Prosecutor's Office, the gun dealer was the German dark web seller "DW Guns"[17]. In addition, some items that are more dangerous than guns are also entering the dark web black market. In April 2016, U.S. President Barack Obama, in his speech to heads of state and foreign ministers from 50 countries in Washington, described how terrorist organizations buy uranium, plutonium and other nuclear materials on the dark web, and said that if terrorists use drones to target civilians It would be America's biggest counter-terrorism nightmare.

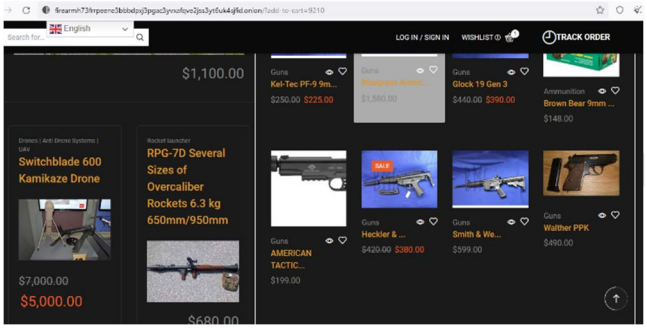


Figure 5: Guns in the dark web

E. Cyber Terrorism

Terrorist organizations face financial constraints, making cyberattacks an increasingly appealing option due to their lower cost and the need for fewer attackers. Terrorists with extensive computer knowledge can effectively conceal their identities and evade detection, technologically and geographically wise. The benefit of cyberattacks lies in their ability to be carried out from any location while maintaining anonymity. Combining cyberterrorism with physical terrorism is believed to yield the most impactful results. Potential targets for cyberterrorism include government computers and financial networks, with the intention of causing widespread chaos (Alghamdi & Selamat, 2022). Terrorists employ various tactics, such as accessing confidential information, deleting data, destroying websites, and inserting viruses, to breach secure systems and inflict damage. Cyberattacks serve as a means for terrorists to generate financial resources and disseminate propaganda.

IV. CHALLENGES FACED BY LAW ENFORCEMENT IN COMBATING CRIMES ON THE DARK WEB

A. Tracking and Tracing Crimes on the Dark Web: A Daunting Challenge for Law Enforcement

As the accessibility of the dark web continues to increase and user-friendly tools, such as dark web browsers, navigation engines, and search platforms, become readily available, the general population are gaining easier entry to this realm. This growing popularity of accessing information on the dark web has led to a mixture of legitimate users and criminals, resulting in a surge of illegal activities. In particular, the dark web employs sophisticated encryption techniques, utilizing private keys, meeting point IPs, cookies, and Tor routing, making it incredibly arduous to trace the source of IP addresses. As a result, law enforcement and regulatory agencies at all levels face significant challenges in supervising and combating crimes on the dark web, especially when it comes to identifying criminal leads, gathering evidence, and building criminal cases [18].

B. Cryptocurrencies Fueling the Rise of Dark Web Crimes

Digital virtual currencies have become a preferred method for money laundering and illicit transactions within the dark web. Cybercriminals exploit various tactics, such as illegal mining, blackmail, and theft, to acquire digital virtual currencies, which are then used for transactions on the dark web, generating substantial profits. The integration of cryptocurrencies and the dark web has created an independent and secure payment system, which has further concealed the nature of dark web transactions and led to a continuous surge in dark web crimes. Monitoring and statistics conducted by the 360-security team on an active Chinese trading forum within the dark web revealed a rapid growth in activity since 2017. The number of trading posts have significantly increased, with a peak in November, indicating the widespread involvement of cryptocurrencies in these transactions and the extensive range of criminal activities [19].

C. Platformization of Cybercrime: The Dark Web's Growing Influence

With the increasing popularity of the dark web, cybercrimes have evolved into highly organized platforms offering a range of services. For instance, one can now purchase comprehensive ransomware services directly from the dark web. Some platforms even provide step-by-step instructions for carrying out ransomware attacks, allowing individuals to specify their target and paying a commission from the obtained ransom. The extreme privacy measures implemented by darknet members on these platforms make it tremendously challenging for law enforcement agencies to gather evidence in such environments. Combating these types of crimes becomes even more difficult due to the intricate nature of dark web platforms [20].

D. Data Storage Complicates Dark Web Counterterrorism Efforts

The widespread adoption of cloud services for data storage and exchange on the internet has significantly enhanced the concealment of illegal activities on the dark web, making it increasingly difficult for relevant authorities to track and monitor them. For example, the development of Amazon Corporation's EC2 elastic computing cloud allows the support of virtual computers and bridges that facilitate communication through interconnected devices and secret networks, including the dark web. This integration enables terrorist organizations to operate more covertly, posing significant challenges in combating terrorism on the dark web[21].

E. Privacy Protection Dilemma: Exploitation of the Dark Web

While the emergence of the dark web initially addressed the privacy concerns of certain internet users, it has also inadvertently become a "safe haven" for criminals and terrorists. Following incidents like the "Prism Gate," public awareness regarding privacy protection has increased. However, this poses a complex problem when combating crimes and terrorism on the dark web, as some internet companies often refuse to cooperate with law enforcement agencies citing privacy protection concerns. The delicate balance between dark web crime and privacy protection has become a challenging issue for law enforcement, particularly due to controversies surrounding personal privacy in existing laws and regulations [22].

Concealment Challenges: The Cost of Law Enforcement

Dark web users predominantly disseminate illegal information through peer-to-peer networks and utilize file-sharing and downloading services, making it exceedingly difficult for law enforcement agencies to ascertain the true identities and activities of users. Additionally, the use of sophisticated technologies, such as smart devices and stealth applications, further complicates the extraction of criminal evidence from the dark web, significantly increasing the cost of tracking and tracing by law enforcement agencies. Some dark web platforms redirect their operations overseas, leveraging the support of the internet while maintaining a high level of concealment. Consequently, law enforcement agencies face tremendous obstacles in monitoring the access patterns of dark web users due to various technical limitations, regardless of whether or not any clues are left behind by the perpetrators [23].

V. PROPOSED COUNTERMEASURES AGAINST DARK NET CRIMES

The following are the proposed countermeasures to secure the dark web.

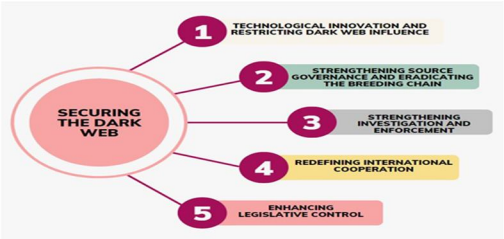


Figure 6 Proposed strategies

A. *Technological Innovation and Restricting Dark Web Influence*

To combat the dark web threat, it is crucial to leverage technological advancements. This includes utilizing the potential of the dark web for positive applications, such as military communications and secure e-commerce, while simultaneously developing comprehensive monitoring technologies and technical tools specifically designed for the dark web. Investing in research and development efforts to advance tools and techniques for monitoring and infiltrating the dark web is essential. Collaboration between government entities and private enterprises should be fostered to develop technologies that block and dismantle sources of illegal and criminal information on the dark web, while also protecting personal anonymity.

B. *Strengthening Source Governance and Eradicating the Breeding Chain*

Effective governance of the sources and platforms that facilitate dark web activities is crucial. Implementing a dual investigation system can enforce responsibility and accountability for security management among internet-connected entities and enterprises. Strict investigations and punishments should be imposed for non-compliance with internet security regulations. Intensifying crackdowns on illegal content within the dark web, including pornography, gambling, drugs, firearms, and personal information trafficking, is necessary. Efforts should be made to address the root causes of dark web crimes by protecting citizens' personal information, dismantling online black and gray industry chains, and restricting criminals' access to secure spaces within the internet.

C. *Strengthening Investigation and Enforcement*

The fight against dark web crimes should be prioritized at various government levels, establishing dedicated organizations and institutions. Strategies and measures should be improved, proactively planning and taking robust actions to suppress emerging criminal activities on the dark web. Dismantling criminal syndicates associated with the dark web should be a primary focus, incorporating efforts into special campaigns against organized crime. Joint investigations and enforcement should be strengthened, with timely and accurate research, analysis, and innovative tactics to deter crimes on the dark web.

D. *Redefining International Cooperation*

International cooperation is crucial to effectively combat the global nature of dark web crimes. Close collaboration and information exchange mechanisms should be established within the international framework. Strengthening the extradition process and facilitating cross-border cooperation in investigating and prosecuting dark web criminals is essential. Collaboration should extend to establishing a shared governance model, emphasizing shared powers and responsibilities among nations to effectively combat dark web activities. Capacity building initiatives, including training programs, technical assistance, and knowledge sharing, should be promoted to empower nations with the necessary expertise and tools to combat dark web crimes.

E. *Enhancing Legislative Control*

Legislation specific to dark web security should be expedited and enforced. Comprehensive legal frameworks should be developed that address the challenges posed by the dark web while respecting individual privacy rights and civil liberties. Specific regulations and guidelines should be developed for the supervision of dark web information security, defining the responsibilities and rights of network service providers and users. Restrictions on dark web encryption services should be reinforced, ensuring regulatory interfaces and registration systems are in place.

VI. CONCLUSION

The use of the Dark Web for terrorism-related activities poses significant challenges to global security. This research paper has explored the phenomenon of terrorist utilization of the Dark Web, highlighting the various ways in which terrorist organizations exploit this hidden realm for recruitment, radicalization, fundraising, communication, and procurement of illicit goods and services. Through case studies, we examined the involvement of prominent terrorist organizations, such as ISIS and Al-Qaeda, and the implications of their activities on the Dark Web.

The research has shed light on the technical, legal, and policy challenges associated with monitoring and countering terrorism on the Dark Web. From the technical perspective, the encryption, anonymity, and decentralized nature of the Dark Web present obstacles to effectively identifying and tracking terrorist activities. Legal and policy considerations require striking a balance between proactive counterterrorism measures and safeguarding civil liberties and privacy rights. International collaboration, public-private partnerships, and continuous research and analysis were identified as crucial factors in addressing these challenges.

Recommendations were provided to guide future efforts in combating the use of the Dark Web for terrorism. Enhancing monitoring capabilities through technological advancements, strengthening international collaboration and information sharing, fostering public-private partnerships, and updating legal frameworks were among the key recommendations. Furthermore, promoting public awareness and education, as well as conducting continuous research and analysis, were highlighted as essential for staying ahead of terrorists in this evolving landscape.

It is imperative for policymakers, law enforcement agencies, cybersecurity professionals, and the wider society to remain vigilant and proactive in countering the use of the Dark Web for terrorism-related activities. By adopting a multidimensional approach that encompasses technology, collaboration, legal frameworks, public awareness, and research, we can mitigate the risks and protect our communities from the threats posed by terrorists operating on the Dark Web. As technology continues to evolve, so too will the tactics and strategies of terrorist organizations. Therefore, ongoing research, adaptability, and innovation will be vital in addressing emerging threats and staying ahead of those who seek to exploit the Dark Web for nefarious purposes. Through collective efforts and a commitment to security, we can create a safer digital environment and combat terrorism effectively in the modern age.

REFERENCES

[1] S. Nazah, S. Huda, J. Abawajy, and M. M. Hassan, "Evolution of dark web threat analysis and detection: A systematic approach," IEEE Access, vol. 8, pp. 171796–171819, 2020, doi: 10.1109/ACCESS.2020.3024198.

[2] N. Mandela, A. A. S. Mahmoud, and A. K. Agrawal, "A Forensic Analysis of the Tor Network in Tails Operating system," Proceedings of the 17th INDIACom; 2023 10th International Conference on Computing for Sustainable Global Development, INDIACom 2023, pp. 546–551, 2023.

[3] M. Muir, P. Leimich, W. B.-D. Investigation, and undefined 2019, "A forensic audit of the tor browser bundle," Elsevier, Accessed: Apr. 01, 2023. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1742287619300829

[4] K. Jacka, "Beyond the Surface Web: How Criminals Are Utilising the Internet to Commit Crimes," Advanced Sciences and Technologies for Security Applications, pp. 109–118, 2023, doi: 10.1007/978-3-031-09691-4_6/COVER.

[5] M. Lakomy, "Dark web jihad: exploring the militant Islamist information ecosystem on The Onion Router," https://doi.org/10.1080/19434472.2022.2164326, 2023, doi: 10.1080/19434472.2022.2164326.

[6] R. Montasari and A. Boon, "An Analysis of the Dark Web Challenges to Digital Policing," Advanced Sciences and Technologies for Security Applications, pp. 371–383, 2023, doi: 10.1007/978-3-031-20160-8_19.

[7] A. Baraz and R. Montasari, "Law Enforcement and the Policing of Cyberspace," Advanced Sciences and Technologies for Security Applications, pp. 59–83, 2023, doi: 10.1007/978-3-031-09691-4_4/COVER.

[8] H. Al Jawaheri, M. Al Sabah, Y. Boshmaf, and A. Erbad, "Deanonymizing Tor hidden service users through Bitcoin transactions analysis," Comput Secur, vol. 89, p. 101684, Feb. 2020, doi: 10.1016/J.COSE.2019.101684.

[9] M. R. Arshad, M. Hussain, H. Tahir, S. Qadir, F. I. Ahmed Memon, and Y. Javed, "Forensic Analysis of Tor Browser on Windows 10 and Android 10 Operating Systems," IEEE Access, vol. 9, pp. 141273–141294, 2021, doi: 10.1109/ACCESS.2021.3119724.

[10] A. Ahmed, A. R. Javed, Z. Jalil, G. Srivastava, and T. R. Gadekallu, "Privacy of Web Browsers: A Challenge in Digital Forensics," Lecture Notes in Electrical Engineering, vol. 833 LNEE, pp. 493–504, 2022, doi: 10.1007/978-981-16-8430-2_45/COVER.

[11] E. Sonmez and K. Seckin Codal, "Terrorism in Cyberspace: A Critical Review of Dark Web Studies under the Terrorism Landscape," SAKARYA UNIVERSITY JOURNAL OF COMPUTER AND INFORMATION SCIENCES, vol. 5, no. 1, 2022, doi: 10.35377/saucis.05.01.

[12] V. M. Vilić, "DARK WEB, CYBER TERRORISM AND CYBER WARFARE: DARK SIDE OF THE CYBERSPACE," 2017. [Online]. Available: http://hackdefencesecurity.blogspot.rs/2012/02/1.html

[13] V. Mahor, R. Rawat, A. Kumar, M. Chouhan, R. N. Shaw, and A. Ghosh, "Cyber Warfare Threat Categorization on CPS by Dark Web Terrorist," in 2021 IEEE 4th International Conference on Computing, Power and Communication Technologies, GUCON 2021, Institute of Electrical and Electronics Engineers Inc., Sep. 2021. doi: 10.1109/GUCON50781.2021.9573994.

[14] S. Alayda, N. A. Almowaysher, F. Alserhani, and M. Humayun, "Terrorism on Dark Web," 2021.

[15] E. Kokolaki, E. Daskalaki, K. Psaroudaki, M. Christodoulaki, and P. Fragopoulou, "Investigating the dynamics of illegal online activity: The power of reporting, dark web, and related legislation," Computer Law and Security Review, vol. 38, Sep. 2020, doi: 10.1016/j.clsr.2020.105440.

[16] H. Thorat, S. Thakur, and A. Yadav, "Categorization of Illegal Activities on Dark Web using Classification," International Research Journal of Engineering and Technology, 2020, [Online]. Available: http://parazite.nn.fi/roguesci/

[17] J. K. Saini and D. Bansal, "A Comparative Study and Automated Detection of Illegal Weapon Procurement over Dark Web," Cybern Syst, vol. 50, no. 5, pp. 405–416, Jul. 2019, doi: 10.1080/01969722.2018.1553591.

[18] J. Besenyő and A. Gulyas, "The Effect of the Dark Web on the Security," Journal of Security and Sustainability Issues, vol. 11, no. 1, pp. 103–121, Mar. 2021, doi: 10.47459/jssi.2021.11.7.

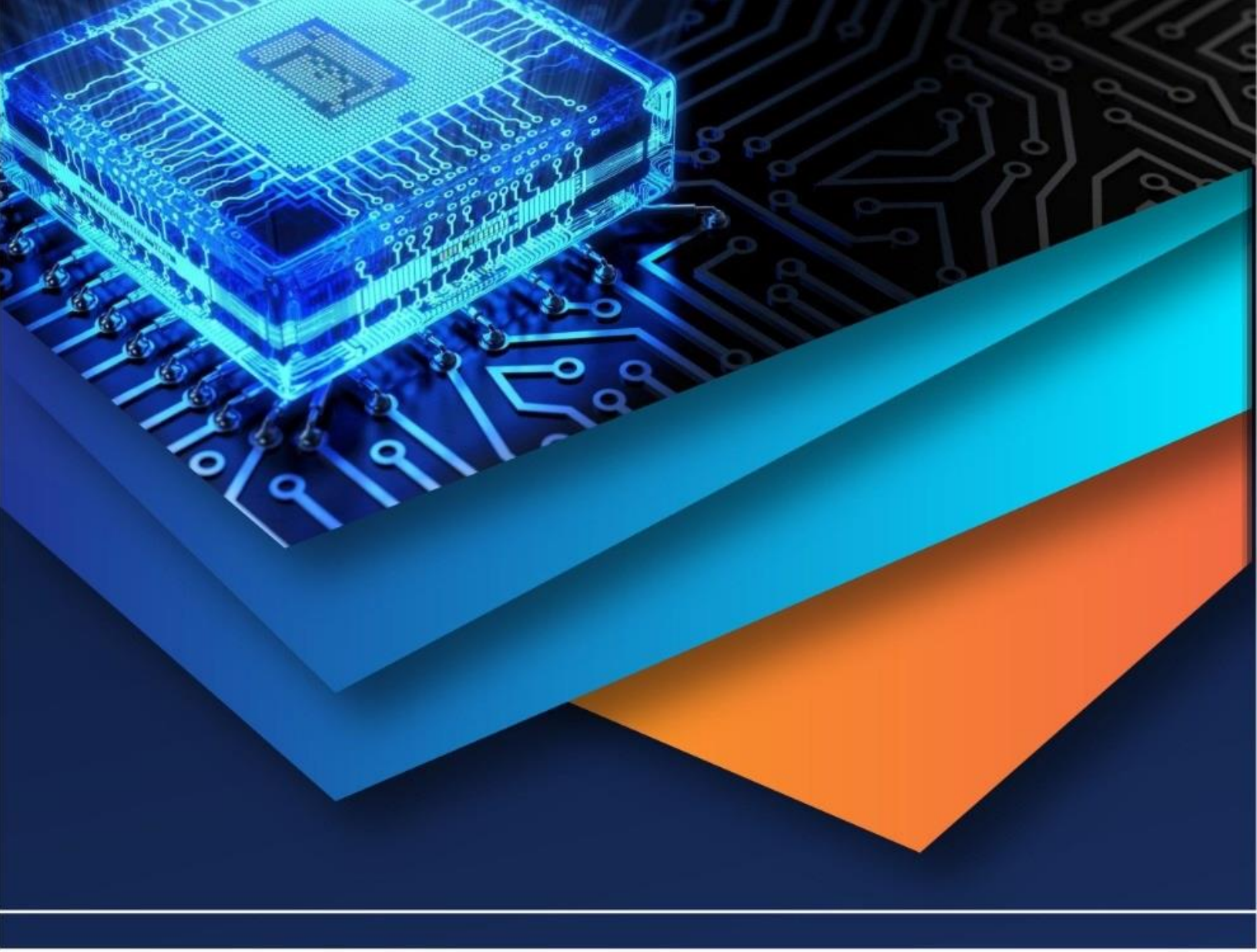
[19] M. Dawson, "A brief review of new threats and countermeasures in digital crime and cyber terrorism," New Threats and Countermeasures in Digital Crime and Cyber Terrorism, pp. 1–7, Apr. 2015, doi: 10.4018/978-1-4666-8345-7.CH001.

[20] B. Akhgar, M. Gercke, S. Vrochidis, and H. Gibson, "Security Informatics and Law Enforcement Series Editor: Babak Akhgar Dark Web Investigation." [Online]. Available: http://www.springer.com/series/15902

[21] N. D. W. Cahyani, N. H. A. Rahman, W. B. Glisson, and K. K. R. Choo, "The Role of Mobile Forensics in Terrorism Investigations Involving the Use of Cloud Storage Service and Communication Apps," Mobile Networks and Applications, vol. 22, no. 2, pp. 240–254, Apr. 2017, doi: 10.1007/s11036-016-0791-8.

[22] H. Alghamdi and A. Selamat, "Techniques to detect terrorists/extremists on the dark web: a review," Data Technologies and Applications, vol. 56, no. 4. Emerald Publishing, pp. 461–482, Aug. 23, 2022. doi: 10.1108/DTA-07-2021-0177.

[23] G. Weimann, "Terrorist Migration to the Dark Web," 2016



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY