JAMBURA LAW REVIEW

Volume 7 Issue 01
JALREV 7 (1) 2025

January 2025
ISSN Print: 2654-9255
ISSN Online: 2656-0461

Beyond the Surface: Exploring the Next Level of Terrorism on the Dark Web

Nur Fadhilah Mappaselleng[1]
Nadiah Khaeriah Kadir[2]✉
Abd. Kadir Ahmad[3]
Zul Khaidir Kadir[4]
Normiati[5]

[1,4]Universitas Muslim Indonesia, Indonesia
[2]Universitas Hasanuddin, Indonesia.
[3]Badan Riset Inovasi Nasional, Indonesia.
[5]University of Birmingham, United Kingdom

✉ *nadiahkhaeriah@gmail.com*

Article Info

Submitted: Jun 06, 2024
Revised: Jan 29, 2025
Accepted: Feb 16 , 2025

***Keywords**:*
Anonymity; Cryptocurrency; Encryption; Dark Web; Terrorism.

***How to cite** [Chicago Manual of Style 17th edition (full note)]:*
Nur Fadhilah Mappaselleng, Nadiah Khaeriah Kadir, Abd. Kadir Ahmad, Zul Khaidir Kadir, Normiati, "Beyond the Surface: Exploring the Next Level of Terrorism on the Dark Web", *Jambura Law Review* 7, no. 1 (2025): 309–335.

Abstract

The lack of effective security mechanisms on the Surface Web facilitates the occurrence of cybercrime. The high accessibility of the Surface Web also allows law enforcement agencies to more easily track and identify perpetrators. However, this motivates criminals to migrate to the Dark Web, the deepest layer of the internet that offers a higher level of security. This research aims to analyze the communication patterns utilized by terrorists on the dark web, propaganda, recruitment, and the use of cryptocurrency in transactions and fundraising by terrorists. The research method used is normative legal research with a conceptual and case approaches and qualitative analysis. This research analyses that terrorists have transitioned to using the Dark Net in a similar manner to how they have utilized the Surface Web over the past several decades, but there are now additional opportunities for tech-savvy operatives. Three main features, anonymity, encrypted messaging, and the use of cryptocurrency, work together to provide an environment that is almost perfect for terrorists on the Dark Web. This combination allows terrorists to conduct their operations more effectively and covertly, making the Dark Web a highly valuable tool for achieving their goals without significant risk of exposure and disruption by security authorities.

1. Introduction

The Dark Web has become an increasingly popular topic of discussion among experts in recent years. On these platforms, users are required to pay to access certain data and information that are password-protected or concealed behind pay walls. There exists a "digital underground," reportedly much larger than the traditional Internet, where individuals engaged in unlawful activities such as hacking, terrorism, and criminal activities can do so without restrictions.[1] A part of the Internet, referred to as the Deep Web, is inaccessible through standard browsing technologies and tools. It is a segment of cyberspace that operates on standard protocols and services, but its use necessitates particular identification. Although entirely lawful, these services do not fall within the public category.

In addition to being inaccessible via standard browsing tools and methods, the Dark Web is a part of the Internet that necessitates the use of specialized knowledge or information to handle the various illegal activities that occur in cyberspace. The Dark Web is regarded as a "promised land" for individuals engaging in illicit activities such as the drug trade, procurement of human organs, weaponry, ammunition, explosives, or the financing of homicides.[2]

The Dark Web is an anonymous and encrypted section of the World Wide Web that is inaccessible via standard search engines. It protects users' privacy and anonymity by running on overlay networks and using encryption and anonymization technologies. The Dark Web's anonymity is appealing to some, but it has also become a magnet for terrorists to achieve their goals.[3]

---

[1] Amit Balhara et al., "Exploring and Analyzing Dark Web," in *SSRN Electronic Journal* (the International Conference on Innovative Computing & Communication (ICICC), SSRN, 2021), 1, https://www.ssrn.com/abstract=3879619.

[2] M. Vida Vilić, "Dark Web, Cyber Terrorism and Cyber Warfare: Dark Side of the Cyberspace," *Balkan Social Science Review* 10 (2017): 8.

[3] Ngaira Mandela, Tumaini Mbinda, and Felix Etyang, "Combating Dark Web Terrorism: Strategies for Disruption and Prevention," *International Journal for Research in Applied Science and Engineering Technology* 11, no. 8 (2023): 857, https://doi.org/10.22214/ijraset.2023.55259.

Terrorists have been active on the Surface Web since the late 1990s,[4] leveraging multiple social networking sites including the Yahoo Group to discuss with each other, spread propaganda, and recruit members.[5] Before 1999, the United States Government identified approximately 30 (thirty) terrorist factions active in the digital space. However, following the heightened significance of the Internet in the aftermath of the September 11th attacks, the Al-Qaeda's command attempted to disseminate videos of their concealment in Pakistan via Al-Jazeera television.[6] They encountered frustration due to the limited airtime available, which could potentially lead to misinterpretations of their messages. Consequently, they opted to utilize the Internet to upload their content more clearly and comprehensively and without editing. However, the majority of terrorist activities, previously conducted in plain sight on the Surface Web for purposes such as sharing information, recruiting, radicalizing, spreading propaganda, fundraising, and coordinating attacks, have now transitioned to the obscured layers of the Internet. For instance, terrorist propaganda materials are currently stored on the Dark Web.[7] Over the last decade, communication channels utilized by al-Qaeda leaders worldwide have gravitated towards the deepest corners of the Internet, often denoted as the Deep Web and the Dark Web.

Al Qaeda released its "Tor Browser Security Guidelines" online following clampdowns on its Surface Web propaganda activities. These guidelines offer instructions on downloading, installing, and using the Tor browser, encouraging target users to transition to the Dark Web while providing tips on avoiding detection and identification by counterterrorism agencies.[8] Additionally, terrorist groups transfer propaganda materials from the Surface Web to the Dark Web sites as a backup

[4] Eda Sönmez and Keziban Seçkin Codal, "Terrorism in Cyberspace : A Critical Review of Dark Web Studies under the Terrorism Landscape," *Sakarya University Journal of Computer and Information Sciences* 5, no. 1 (2022): 1, https://doi.org/10.35377/saucis.05.01.950746.

[5] Kristin Finklea, "The Dark Web: An Overview" (Congressional Research Service, 2024), https://crsreports.congress.gov.

[6] Nadiah Khaeriah Kadir, Judhariksawan Judhariksawan, and Maskun Maskun, "Terrorism and Cyberspace: A Phenomenon of Cyber-Terrorism as Transnational Crimes," *Fiat Justisia: Jurnal Ilmu Hukum* 13, no. 4 (2019): 340, https://doi.org/10.25041/fiatjustisia.v13no4.1735.

[7] Gabriel Weimann, "Terrorist Migration to the Dark Web," *Perspectives on Terrorism* 10, no. 3 (2016): 41.

[8] Mandela, Mbinda, and Etyang, "Combating Dark Web Terrorism: Strategies for Disruption and Prevention," 857.

measure. If a Surface Web site is blocked, they disseminate the link addresses of mirrored sites on the Dark Web via anonymous forums, chat rooms, or email, instructing their members and supporters to access these spaces. Islamic State of Iraq and Syria (ISIS) utilizes the Darknet as a tool for terrorism, streaming live footage of executions and broadcasting clips of their brutal activities. The Al-Hayat Media Center, an ISIS-affiliated media outlet, disseminates links and instructions for accessing its Darknet site on ISIS-related forums. For instance, following the December 2015 Paris attacks, ISIS swiftly shifted its propaganda operations, including the Al-Hayat Media Center, to the Dark Web, and distributed content through platforms like the Shamikh forum.[9] This site serves as a mirrored platform hosting content accumulated over time from various message boards, showcasing videos and documents available in multiple languages.

Moreover, terrorists often use so-called cyber-attacks to launch their attacks on the Dark Web. The following objectives can be used to identify cyberattacks: Access to computers and information regarding the final objectives of attacks that may include financial harm (by deploying hacking techniques), data collection, manipulation, or destruction. Websites could become less accessible due to the use of botnets. Furthermore, it could also include tampering with IT systems that manage and control physical infrastructure (airports, trains, and subways).[10]

The novelty of the present study lies in its in-depth exploration of the technological evolution that has transformed how terrorist organizations operate on the Dark Web. Unlike previous studies that primarily focused on terrorism in cyberspace, this research highlights how advancements in encryption, decentralized platforms, and blockchain technology have significantly enhanced the efficiency of propaganda, recruitment, communication, and financing. By comparing the transition from the Surface Web and Deep Web to more sophisticated Dark Web operations, this article provides a unique perspective on how these groups leverage anonymous

[9] Saiba Nazah et al., "Evolution of Dark Web Threat Analysis and Detection: A Systematic Approach," *IEEE Access* 8 (2020): 171802, https://doi.org/10.1109/ACCESS.2020.3024198.
[10] Eduard Ivanov, "Combating Cyberterrorism under International Law," *Baltic Yearbook of International Law* 14 (2014): 62.

cryptocurrencies and encrypted messaging services to strengthen their networks while evading detection.

2. Problem Statement

The Dark Web, an anonymized part of the Internet accessible only through specialized software like Tor, has become a fertile ground for criminal activities. Terrorist organizations are increasingly leveraging its capabilities to enhance their operations, thus raising new challenges for security and law enforcement agencies. Traditional counter-terrorism methods are being outpaced by the sophisticated use of digital platforms that offer anonymity and untraceable communication channels. Exploring the next level of terrorism on the Dark Web is critical for understanding and countering the emerging threats in this digital underworld.

3. Methods

This study uses a descriptive normative research method that is more focused on literature analysis. The main aim of this research is to achieve a deeper understanding of the investigated topic by examining various relevant literature sources.[11] In doing so, the researcher reviewed various legal documents such as laws and regulations related to the research subject. Additionally, this study also refers to other literature sources such as books, papers, articles, scientific journals, and magazines that discuss the same or related topics, which enables the researcher to acquire a comprehensive and thorough understanding of the legal framework and concepts associated with the research object.

The normative legal research method, which combines conceptual approaches and case studies, is highly significant for comprehending and responding to the dynamics of terrorism on the Dark Web. The conceptual approach plays a key role in unraveling and analyzing the fundamental principles underlying terrorist activities there, such as anonymity, encryption, and the use of cryptocurrency. Anonymity protects terrorists

[11] Dian Ekawaty Ismail et al., "Collocation of Restorative Justice with Human Rights in Indonesia," *Legality : Jurnal Ilmiah Hukum* 32, no. 2 (September 20, 2024): 394–417, https://doi.org/10.22219/ljih.v32i2.35374; Novendri Nggilu et al., "Judicial Review of Constitutional Amendments: Comparison Between India, Germany, Colombia, and the Relevancy with Indonesia," *Lex Scientia Law Review* 8, no. 1 (September 22, 2024), https://doi.org/10.15294/lslr.v8i1.1901.

by concealing their identities while communicating or conducting transactions, while encryption ensures that messages sent remain protected and inaccessible to third parties. The use of cryptocurrencies also facilitates terrorist funding in ways that are difficult for security authorities to trace.

The case-based approach provides an important practical dimension by offering empirical evidence of how existing laws are implemented in real-world situations. This may include case studies of terrorist groups using the Dark Web to disseminate propaganda, recruit new members, plan attacks, and engage in financial transactions. By integrating conceptual approaches and case studies, normative legal research can generate a deeper and more comprehensive understanding of terrorism on the Dark Web. This understanding will enable policymakers and regulators to develop more effective and responsive regulations to address the threats posed, thereby enhancing global efforts toward prevention and counterterrorism. Thus, this method plays a crucial role in combating the increasingly complex and diverse terrorism activities in the digital era.

4. Terrorism on the Dark Web

Numerous individuals hold the misconception that the terms "Internet" and "Web" are interchangeable.[12] Actually, these terms refer to different concepts even though they share some common elements. The Internet is a global network consisting of various smaller networks and a very large and complex infrastructure. This infrastructure includes hardware, such as routers, servers, and fiber optic cables, as well as communication protocols that enable devices worldwide to connect and exchange data. The primary function of the Internet is to connect millions of computers and facilitate fast and efficient communication and data exchange globally. The Web is one of the services that run on the Internet infrastructure. It provides a medium for accessing information globally. Conceptually, the Web is a collection of content organized into websites that can be accessed through browsers like Google Chrome, Firefox, etc. These websites consist of text, images, videos, and various other types of

[12] Arbër Beshiri and Arsim Susuri, "Dark Web and Its Impact in Online Anonymity and Privacy: A Critical Analysis and Review," *Journal of Computer and Communications* 7 (2019): 31, https://doi.org/10.4236/jcc.2019.73004.

media linked together by hyperlinks, creating a network of information that users can explore.

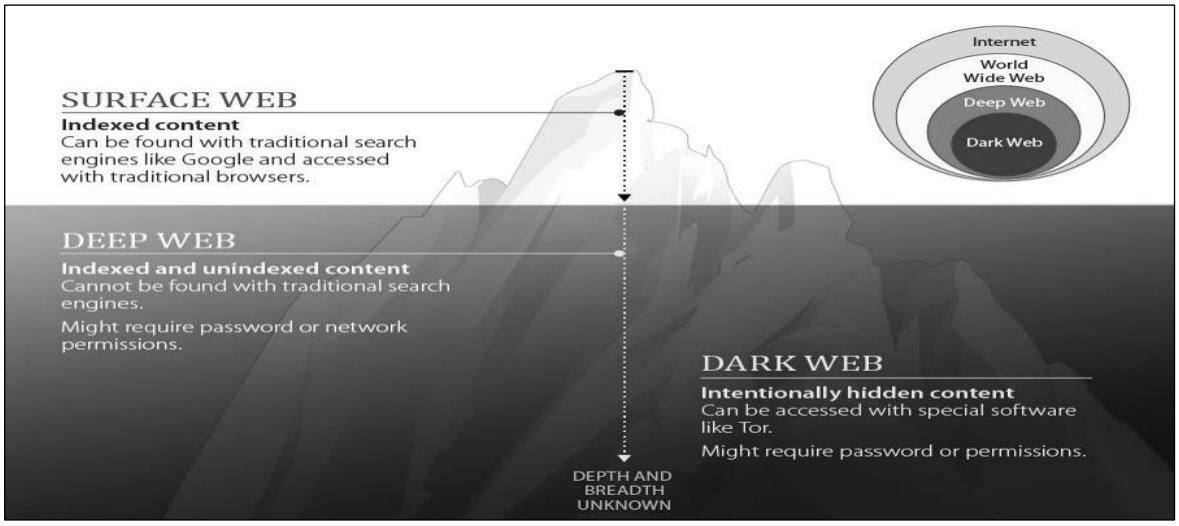
The main difference between the Internet and the Web lies in their functions. The Internet is the network infrastructure that enables various forms of data communication, while the Web is an information system that utilizes this network to provide and access content. Although interdependent, they operate at different levels: the Internet is the foundational physical and logical infrastructure, and the Web is an application that leverages this infrastructure to deliver information services to users. The Web can be further divided into three main categories. The first category is the Surface web which is accessible to the public without requiring authentication or payment. It is indexed by search engines, such as Google,[13] allowing stakeholders to be identified, thus making it susceptible to law enforcement. The second is the Deep Web which comprises sections of the Internet not publicly accessible or indexed by search engines. Access to this part of the Web is restricted either due to authentication requirements or because it is part of a private network. As a result of these authentication measures, there is an increased level of accountability compared to the Surface Web. Typically, search engines use web crawlers to locate and retrieve data stored on the World Wide Web. These crawlers, also known as spiders, navigate through hyperlinks to access various domains. However, search engines cannot index information stored within the Deep Web.[14]

Finally, the Dark Web, also identified as dark nets or anonymous services, constitutes the part of the Internet which is not listed by search engines and necessitates custom software for access. This section encompasses both accessible and secured areas that can be accessed by public or individuals with credentials, provided they utilize the appropriate software.[15] The primary distinction between the Dark Web and the Surface or Deep Web lies in the absence of accountability. Users remain unidentified by the

[13] Finklea, "The Dark Web: An Overview," 1.
[14] Radhika Bailurkar and Aniket Goswami, 'The Deep Web', *International Journal of Scientific & Engineering Research* 9, no. 3 (2018): 1230.
[15] Abhineet Gupta, Sean B Maynard, and Atif Ahmad, "The Dark Web Phenomenon: A Review and Research Agenda" (Australasian Conference on Information Systems, Perth: Association for Information Systems Electronic Library, 2019), 2, https://aisel.aisnet.org/acis2019/1.

network or any monitoring entities, effectively anonymizing their activities. Furthermore, the Dark Web enables the provision of online service that uphold anonymity concerning genuine IP addresses and locations, even among users utilizing these services. The Dark Web enables private communications among individuals by offering anonymity.

Figure 1. *Layers of the Internet*



Source: Gupta, A., Maynard, S. B., & Ahmad, A. (2019). The Dark Web Phenomenon : A Review and Research Agenda. Australasian Conference on Information Systems, 1–12.

As shown in Figure 1, the Dark Web encompasses web pages hosted on Internet networks that evade indexing by traditional search engines and can only be accessed through specialized software such as The Onion Router (Tor). Operating within the Tor network allows encrypted communication which enables content providers to share material anonymously.[16] Initially intended to safeguard classified information at the United States Naval Research Laboratory, the Tor network has evolved into an encryption tool used to obscure user activity and IP addresses.

Several protocols and tools have been employed to build the Dark Web, including browsers for access, encryption methods to secure data, Virtual Private Networks (VPNs) for data transmission, and routing algorithms.[17] Remaining anonymous is

[16] Dario Bermudez et al., "Under and over the Surface: A Comparison of the Use of Leaked Account Credentials in the Dark and Surface Web," *Crime Science* 7, no. 17 (2018): 2, https://doi.org/10.1186/s40163-018-0092-6.
[17] Shubhdeep Kaur and Sukhchandan Randhawa, "Dark Web: A Web of Crimes," *Wireless Personal Communications* 112, no. 1 (2020): 4, https://doi.org/10.1007/s11277-020-07143-2.

critical to access the Dark Web. In addition to a browsers, reliable Virtual Private Networks (VPNs) are required to provide anonymity. It might be a paid NordVPN or a phantom VPN. NordVPN operates as a personal VPN service provider and offers applications for macOS, Windows, Linux, iOS, and Android. Phantom VPN prevents ISPs, Internet snoops, and ads from tracking your Internet activity.

Spalevic and Ilic identified five types of terrorist activities occurring on the Internet.[18] These include communication through emails, digital photos, and chat sessions; recruitment and training involving persuading individuals to join jihadist or other extremist organization and providing web-based training, fundraising consisting of remitting funds, committing credit card fraud, and participating in money laundering; and seeking by conducting online surveillance to identify insecurities in possible targets, such as airports.

In this case, terrorists use the following types of cyberattacks: An incursion is an attack meant to violate security and obtain access to a computer system or network to obtain or alter data. Owing to computer systems' and networks' insecurity, terrorists can alter crucial information and harm a person or an organization.[19] Destruction involves using an attack to break into computer systems and networks to severely harm or destroy them. An organization suffering from one of these attacks would have to pay a high price to restart its operations. Disinformation is an attack that disseminates false information that can harm a specific target. These attacks can cause uncontrollable situations either within the organization or nationally. Denial-of-service attacks aim to take down or interfere with a network by sending an enormous amount of packets to the target server, making it impossible for the latter to respond to regular service requests from authorized users. This could cause massive losses to businesses. Website defacement involves attacks aimed at damaging the targeted websites. The primary goal of these attacks is to alter a website's content, often by redirecting users or embedding cyberterrorist messages.

[18] Zaklina Spalevic and Milos Ilic, "The Use of Dark Web for the Purpose of Illegal Activity Spreading," *Ekonomika* 63, no. 1 (2017): 76, https://doi.org/10.5937/ekonomika1701073S.
[19] Kanika Sharma and Tanvi Bhalla, "Future Towards Danger: The Terror of Cyber Attacks," *IITM Journal of Management and IT* 6, no. 1 (2015): 91–92.

What terrorists do on the Dark Web may be described simply as "more of the same but more secretly".[20] Although, However, this is only partially accurate. Terrorists use the Dark Web in the same way that they have used the Surface Web for a long time, however, new possibilities have emerged for cyber-savvy operations as well. They have utilized the Internet to share information, recruit and radicalize others, distribute propaganda, generate cash, and coordinate operations and assaults.[21] However, these activities have now moved to the deeper levels of the Internet, i.e., the Dark Web. This encompasses the facilitation of instructional sessions on bomb-making and the execution of terrorist operations, particularly targeting the preparation of "lone wolf" assailants, which has considerable ramifications. Propaganda materials include articles, videos, images, and even fabricated news bulletins. Their principal objectives are to fortify extremist ideologies, foment animosity, and incite and expand their follower base. By disseminating their propaganda on the Dark Web, terrorist groups can reach a broader audience without being detected by authorities.

"Lone wolves" denotes individuals who have undergone extremist indoctrination, procuring or manufacturing their own armaments and executing acts of terrorism autonomously. Owing to the anonymity afforded by the Dark Web, counterterrorism entities encounter difficulties in discerning the identities of those influenced by terrorist groups.[22] Consequently, lone-wolf assaults are characterized by protracted planning periods and unpredictable occurrences, presenting obstacles to security apparatuses and necessitating recourse to conventional anti-terrorism methodologies that are resistant to adaptation. It is apparent that terrorist entities exploit global interconnectedness and the obscurity conferred by the Dark Web to proliferate terrorism on an international level, thereby amplifying the complexities surrounding counter-terrorism actions.

[20] Gabriel Weimann, "Going Darker? The Challenge of Dark Net Terrorism" (Washington, DC: Wilson Center, 2018), 5.
[21] Snezhana Krumova, "From Surface to the Dark Web in the Realm of Terrorism," Law and Internet Foundation, accessed February 13, 2025, https://www.netlaw.bg/en/a/from-surface-to-the-dark-web-in-the-realm-of-terrorism.
[22] Mandela, Mbinda, and Etyang, "Combating Dark Web Terrorism: Strategies for Disruption and Prevention," 859.

4.1. Anonymity

Terrorist activities conducted on the Dark Web are characterized by more clandestine methods than those on the Surface networks. This enables users to explore websites without exposing personal information. Consequently, using technologies like Tor, individuals can easily establish servers that remain anonymous and untraceable for various activity, Such anonymity allows terrorist organizations to conceal their identities and illicit actions.[23] Even software developers, ISPs, and law enforcement organizations struggle to trace routing information, thus remaining unaware of the operator's identity or the server's location. Software developers, ISPs, and law enforcement agencies also find it difficult to track routing data, making it impossible for them to identify the operator or determine the server's location.

The Merriam-Webster Dictionary defines anonymity as the quality or state of being anonymous or one that is anonymous,[24] meaning not being named or recognized, and lacking distinctiveness or individuality.

As users interact online, their actions create digital footprints on the Internet. The assurance of anonymity depends on the inability to trace the associated Internet Protocol (IP) addresses.[25] The following are the different techniques commonly used to ensure anonymity on the Dark Web:[26]

1) Proxy. Acting as a filtering and bypassing service, a proxy serves as an intermediary server between users and the Internet, effectively separating them from the websites they access.
2) Virtual Private Network (VPN). A VPN establishes a secure "tunnel" from a user's device to the Internet, employing encryption methods to safeguard sensitive data. Users can subscribe to paid VPN services like Personal VPN

[23] Atif Ali and Muhammad Shareh Qazi, "Darknet: The Study of Emerging Challenges of Cyber Terrorism and Organized Crimes," *Pakistan Journal of Terrorism Research* 4, no. 2 (2022): 101.
[24] "Anonymity," Merriam-Webster, accessed February 14, 2025, https://www.merriam-webster.com/thesaurus/anonymity.
[25] Beshiri and Susuri, "Dark Web and Its Impact in Online Anonymity and Privacy: A Critical Analysis and Review," 34.
[26] Javeriah Saleem, Rafiqul Islam, and Muhammad Ashad Kabir, "The Anonymity of the Dark Web: A Survey," *IEEE Access* 10 (2022): 33635, https://doi.org/10.1109/ACCESS.2022.3161547.

Provider, Paid Nord, or Phantom VPN to ensure that their online activities remain untraceable.

3) Domain Name System (DNS) Based Bypassing. While regular web browsers rely on DNS indices to access indexed websites conveniently, dark websites circumvent DNS-based indexing. This separation ensures that the Dark Web and the regular Web remain distinct entities.
4) Onion Routing. By employing encryption during transmission, onion routing enables anonymous connections by encrypting messages in layers, similar to those of an onion. This method, which effectively conceals the identities of both the client and server, is a critical feature of the Dark Web.

The use of an anonymous network provides terrorists with several advantages, allowing them to streamline their planning, coordination, and execution of criminal activities while avoiding legal consequences through the assurance of network security.[27] Furthermore, terrorists utilize VPNs and proxy servers to evade geolocation tracking, providing them with a shield against law enforcement and intelligence agencies who seek to monitor their movements and operations. These tools, though not entirely impervious to traffic analysis, significantly obstruct it, often redirecting investigators to intermediary countries. These countries may lack reciprocal legal agreements or be less inclined to classify cyber activities as criminal, complicating their investigative efforts.[28]

In 2015, an undercover BBC journalist via Twitter contacted Junaid Hussain, an ISIS recruiter who had traveled from Birmingham to Syria in 2013. Despite Hussain's death in a drone attack that took place in August 2015, another anonymous recruiter carried on the conversation by inviting the reporter to discuss privately using an encrypted communication tool.[29] Once on this restricted site, the recruiter allegedly tried to convince the secret journalist to conduct attacks in London, proposing plans strikingly

[27] Ali and Qazi, "Darknet: The Study of Emerging Challenges of Cyber Terrorism and Organized Crimes," 101.
[28] Roderic Broadhurst et al., "Cyber Terrorism: Research Review" (Australian National University, Cybercrime Observatory, 2017), 54.
[29] Nikita Malik, "Terror in the Dark: How Terrorists Use Encryption, the Darknet, and Cryptocurrencies" (London: The Henry Jackson Society, 2018), 22.

similar to those that happened in Westminster and on London Bridge in March and June 2017, in that order. Although it remains unclear how Youssef Zaghba, one of the London Bridge attackers, was radicalized, his computer skills might have led him to encounter ISIS websites on the Dark Web.

4.2. Encryption

In addition to anonymous communication, terrorists can access the Dark Web using unique downloadable software programs that support encrypted channels. Dark Web software programs conceal the Internet Protocol (IP) address of a computer within various layers of encrypted web traffic. The encrypted data is then moved through randomly selected computers across the network known as relay computers, and are routed through a series of paths called nodes. Each node reveals only the destination computer that is next in line. The final node is revealed only when the message reaches its intended destination. These specialized browsers generally allow users to securely access Dark Web sites without being identified.

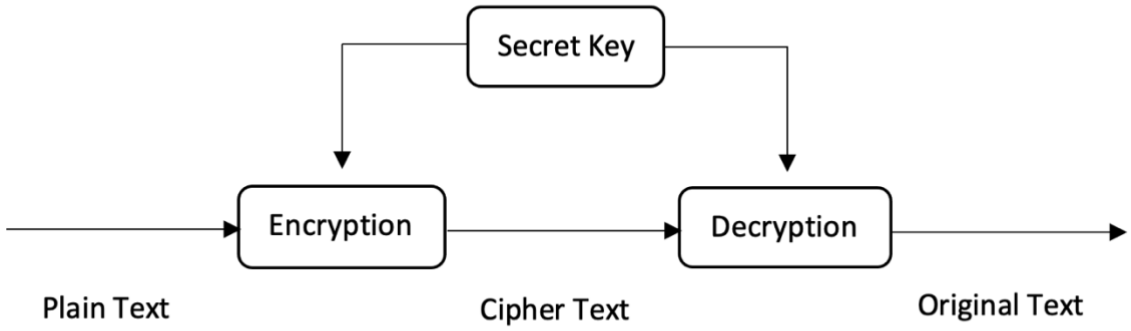
Encryption involves encoding data through mathematical algorithms, where conversation is intentionally obscured or disguised to prevent unauthorized access. Encrypted content is wrapped in layers of coded information, preventing third-party access until the data reaches its intended destination. Thus, encryption protects the identities of both the sender and receiver of the message.[30] It is a key component of cryptography. Cryptography enables the transmission of data over networks in a format that is unrecognizable and unreadable by unauthorized parties. Only the sender can understand the content of the message, and the legitimate receiver can read it only by using the key provided by the sender.[31]

Cryptography comprises of two main concepts, encryption and decryption. Encryption converts information into a form that is unreadable to anyone except those who have the key or the password sent by the sender to the message's recipient. Cryptography is categorized into two main types: symmetric key cryptography and asymmetric key cryptography. Symmetric key cryptography relies on one key for both encryption and

[30] Malik, 17.
[31] B Nithya and P Sripriya, "A Review of Cryptographic Algorithms in Network Security," *International Journal of Engineering and Technology* 8, no. 1 (2016): 324.

descryption. This key is private and must be kept confidential by both parties (see Figure 2).

Figure 2. *Symmetric Key Encryption*



Source: Nithya, B., & Sripriya, P. (2016). A Review of Cryptographic Algorithms in Network Security. International Journal of Engineering and Technology (IJET), 8(1).

In the symmetric key encryption process shown in Figure 2, terrorist groups encrypt files containing critical information, such as attack strategies, member lists, or bomb-making procedures. The algorithms commonly used in symmetric key cryptography include Advanced Encryption Standard (AES) and Triple Data Encryption Standard (3DES). AES is a symmetric encryption algorithm and a type of block cipher.[32] As a symmetric algorithm, it uses a single key for both encoding and decoding. This requires both the sender and receiver to know about and use the same secret encryption key. Unlike asymmetric encryption, which relies on different keys to encrypt and decrypt data, AES operates with a single shared key. Additionally, as a block cipher, AES divides a message into smaller segments and encrypts each block individually, transforming the plaintext into an encrypted format known as the ciphertext.

Triple DES is an encryption methods derived from the original Data Encryption Standard (DES). As a symmetric encryption method, it enhances security by applying multiple rounds of the DES algorithm. It is called Triple DES because it encrypts data

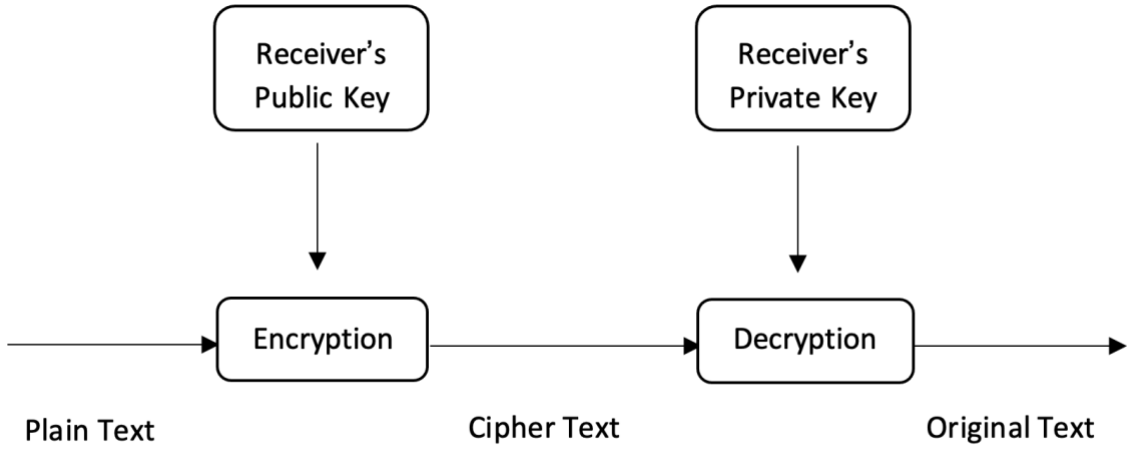
[32] TechTarget, "Advanced Encryption Standard (AES)," accessed February 13, 2025, https://www.techtarget.com/searchsecurity/definition/Advanced-Encryption-Standard.

three times using the DES cipher. It essentially functions as a block cipher and processes data in 64-bit blocks for encryption. In terms of security, Triple DES provides stronger protection compared to the original DES. However, it is less efficient and operates at a slower speed than the AES.[33]

These documents are then transmitted through anonymous servers on the Dark Web or stored in encrypted drives to avoid detection by legal authorities. Terrorists often use highly complex and lengthy passwords to enhance security. Encryption is further reinforced by adding additional layers, such as encrypted zip files or RAR files locked with long passwords, making access even more difficult for outsiders.

Furthermore, asymmetric key cryptography utilizes a two-key system, where one key is used to encrypt the plaintext while the other is responsible for decrypting the encoded text. This system comprises a publicly available key and a private key that is kept confidential (see Figure 3).

Figure 3. *Assymmetric Key Encription*



Source: Nithya, B., & Sripriya, P. (2016). A Review of Cryptographic Algorithms in Network Security. International Journal of Engineering and Technology (IJET), 8(1).

Figure 3 illustrates that terrorists utilize PGP encryption, an asymmetric cryptography-based system, to secure messages and documents sent via email or discussion forums on the Dark Web. In this method, by using the recipient's public key, the sender

[33] "Triple DES (3DES)," GeeksforGeeks, accessed February 14, 2025, https://www.geeksforgeeks.org/triple-des-3des/.

encrypts the message, and it can only be decrypted by the recipient with the corresponding private key.

This provides secure communication because third parties intercepting the message will be unable to read it without the private key. Terrorists also apply asymmetric cryptography to Bitcoin transactions and other cryptocurrencies, where each transaction is encrypted using a private key-based digital signature to ensure security and authenticity.

Pretty Good Privacy (PGP) is an essential encryption technique for protecting various types of sensitive information and communication. It is designed to provide security by ensuring integrity, authentication, privacy, and preventing repudiation.[34] PGP works with asymmetric encryption, which involves using two different keys: a public key and a private key. The public key is available to anyone and is used to encrypt data, and only the corresponding private key can decrypt it. If someone encrypts a message with the public key, only someone with the private key can decrypt and read it. Besides protecting data, PGP is also used to verify identity by combining the hashing process and public key encryption. To maintain privacy, PGP combines secret key encryption with public key encryption.

It is believed that Al Qaeda members communicate by sending encrypted messages. However, encryption is not as secure as it once was, as intelligence agencies have developed advanced systems capable of breaking encryption codes.[35] Despite this, encrypted messages continue to appear on various online forums, where terrorist organizations often leave encrypted text messages for their cells, which can later be accessed by them publicly. Tracing users involved in encrypted communication for terrorist activities on certain Internet forums is nearly impossible.

At the beginning of 2007, Al-Qaeda introduced an encryption tool named 'Mujahidin Secrets' (also known as Asrar al Mujahideen), followed by an updated version released in January 2008, called 'Mujahidin Secrets 2'.[36] Anwar al-Awlaki, the cleric of Al-Qaeda

[34] Kaur and Randhawa, "Dark Web: A Web of Crimes," 4.
[35] Vilić, "Dark Web, Cyber Terrorism and Cyber Warfare: Dark Side of the Cyberspace," 14.
[36] Robert Graham, "How Terrorists Use Encryption," *CTC Sentinel* 9, no. 6 (2016): 22.

in the Arabian Peninsula, used this tool in 2009 to contact operatives in the West, and in June 2010, a four-page tutorial on how to use it was featured in Al-Qaeda's magazine, Inspire. ISIS released a 15-page guide named 'Sécurité Informatique' in April 2008 in the online French magazine Dar Al-Islam, emphasizing the importance of secure communication for the group. The guide explains how to configure Tails, access the Tor network to mask one's location and IP address, create PGP software keys, encrypt emails, and utilize various secure communication tools.

Terrorist organizations have embraced new online platforms, allowing them to spread their messages to a large audience through encrypted mobile apps such as Telegram. The Telegram app, launched on August 14, 2013, gained popularity among both regular users and terrorists. The introduction of 'channels' in September 2015 marked the point when the Terrorism Research & Analysis Consortium (TRAC) saw a noticeable migration from platforms like Twitter to Telegram.[37] Within just four days of the introduction of channels on Telegram, ISIS media operatives on Twitter began advertising the group's own channel, Nashir, which means 'Distributor' in English.

Following the Paris attacks in November 2015, Telegram changed its official stance by committing to remove ISIS accounts, bots, and chats from public channels.[38] According to an ICT special report, the use of Telegram by both ISIS and Al-Qaeda increased remarkably from September 2015 onward. As many as 700 new channels were created in March 2016 linked to ISIS were created, marking a notable surge in the platform's adoption by these groups.[39]

Terrorists use a multilayered technique to encrypt their communications. Initially, the message is inserted into an Excel file that uses its macros to encrypt the content. Next, the encrypted text is transferred into a Word document protected by Microsoft's "password protection" feature, making the breaking of a strong, complex password

[37] TRAC, "Massive Migration to Telegram, the New Jihadist Destination," accessed February 13, 2025, https://trackingterrorism.org/chatter/trac-insight-massive-jihadi-migration-twitter-telegram/.
[38] Counter Extremism Project, "Terrorists on Telegram," accessed February 13, 2025, https://www.counterextremism.com/terrorists-on-telegram.
[39] Barak Michael, "The Telegram Chat Software as an Arena of Activity to Encourage the 'Lone Wolf' Phenomenon," International Institute for Counter-Terrorism (IST), 2016, https://ict.org.il/the-telegram-chat-software-as-an-arena-of-activity-to-encourage-the-lone-wolf-phenomenon/.

nearly impossible. In the third stage, the Word file is compressed and further encrypted using the RAR software, rendering it secure when paired with a long and intricate password. Finally, the encrypted file is uploaded to a hosting platform using a URL shortener to conceal any associated metadata, ensuring further anonymity.

This encryption method was utilized by a disciple of the Yemeni radical cleric, Anwar Al-Awlaki.[40] During the period from 2009 to 2010, he, along with Rajib Karim, a British Airways call center worker from Newcastle, developed a complex encrypted communication system to coordinate attacks on British and American aviation. Karim adopted strict operational security practices by using tools like "Windows Washer" and other Windows utilities to erase any incriminating evidence from his laptop. In addition, he employed full disk encryption to secure his plans and encrypted messages with Al-Awlaki, and stored them on an external hard drive separate from his main device. To further obscure his data, Karim applied volume/container files for comprehensive disk encryption. He assigned deceptive names for these files, such as "Quran DVD Collection 1.rar," making them appear as compressed archive files. However, these files were actually PGP disk-encrypted volumes disguised under a different extension.

4.3. Cryptocurrency

Cryptocurrency is generally used by terrorists for illicit transactions because it provides similar advantages to the hawala system, an unofficial method of transferring money internationally, which has been associated with various terrorist organizations, such as Al-Qaeda and ISIS.[41] Cryptocurrencies are garnering increasing attention due to their role in facilitating online payments without the need for a central authority.[42] In addition, they are based on three core principles: decentralization, pseudo-anonymity, and transparency. Decentralization implies that, instead of being governed

[40] Vikram Dodd, "British Airways Worker Rajib Karim Convicted of Terrorist Plot," *The Guardian*, accessed February 14, 2025, https://www.theguardian.com/uk/2011/feb/28/british-airways-bomb-guilty-karim.
[41] Malik, "Terror in the Dark: How Terrorists Use Encryption, the Darknet, and Cryptocurrencies."
[42] Muh. Firmansyah Isa, "Causes and Efforts to Counter a Crime," *Estudiante Law Journal* 4, no. 2 (October 15, 2022): 788–800, https://doi.org/10.33756/eslaj.v4i2.18273; Zulkifli T. Abas, Fence M. Wantu, and Lisnawaty W. Badu, "The Police's Part in Preventing Online Prostitution Utilizing MiChat Application in Gorontalo City," *Distruption Law Review* 1, no. 1 (2023): 43.

by a central authority, they operate on a peer-to-peer network, with a majority agreement required to validate transactions and branches in the distributed digital ledger known as the 'blockchain'.[43] Blockchain is the fundamental technology underlying cryptocurrencies. Cryptocurrencies are considered pseudo-anonymous because they use hashed public keys to identify users instead of account numbers or usernames, which results in a decentralized identity management system independent of real-world identities. Despite not being directly linked to individuals or organizations, cryptocurrencies are still considered pseudo-anonymous due to the transparent nature of their transactions, as all transactions are publicly recorded on the blockchain.

Currently, there are a wide range of cryptocurrencies, each operating according to different technical principles. Besides Bitcoin, other popular cryptocurrencies include Ethereum, Ripple, and Litecoin.[44] The adoption and utilization of cryptocurrency systems by terrorist organizations are contingent upon the technological capabilities and attributes of the available cryptocurrencies as well as the specific needs and capacities of the organizations themselves. Emerging cryptocurrencies may possess features that are more attractive to terrorist groups compared to those currently used. For instance, if a forthcoming cryptocurrency provides enhanced anonymity for large-scale transactions relative to Bitcoin, these groups may be more inclined to adopt it for specific activities. Hence, it is crucial to analyze the distinct requirements of individual terrorist organizations and compare them with the characteristics of existing cryptocurrencies.

For example, there exists a Dark Web page named "Fund the Islamic Struggle without Leaving a Trace," which requests contributions for Jihad via transactions to a designated Bitcoin address.[45] Similarly, a PDF file associated with Amreeki Witness, entitled "Bitcoin wa Sadaqat Al Jihad" or "Bitcoin and the Generosity of Violent Physical

[43] Arianna Trozze et al., "Cryptocurrencies and Future Financial Crime," *Crime Science* 11, no. 1 (2022): 2, https://doi.org/10.1186/s40163-021-00163-8.
[44] Josh Kamps and Bennett Kleinberg, "To the Moon: Defining and Detecting Cryptocurrency Pump-and-Dumps," *Crime Science* 7, no. 18 (2018): 2, https://doi.org/10.1186/s40163-018-0093-5.
[45] Weimann, "Terrorist Migration to the Dark Web," 42.

Struggle," functions as a guidebook for carrying out covert financial transactions within the Dark Web.

Table 1. *Terrorist Financing Activities in the Context of Cryptocurrency Characteristics*

	Fundraising	Illegal Drug and Arms Trafficking	Remittance and Transfer	Attack Funding	Operational Funding
Anonimity	Moderate Importance	Critical Importance	Moderate Importance	Critical Importance	Lesser Importance
Usability	Critical Importance	Lesser Importance	Lesser Importance	Lesser Importance	Lesser Importance
Security	Moderate Importance	Critical Importance	Critical Importance	Critical Importance	Critical Importance
Acceptance	Lesser Importance	Lesser Importance	Lesser Importance	Moderate Importance	Moderate Importance
Reliability	Lesser Importance	Critical Importance	Critical Importance	Critical Importance	Moderate Importance
Volume	Moderate Importance	Critical Importance	Critical Importance	Critical Importance	Critical Importance

Source: Dion-Schwarz, C., Manheim, D., & Johnston, P. B. (2019). Terrorist Use of Cryptocurrencies. Technical and Organizational Barriers and Future Threats.

According to Table 1, Al-Qaeda, ISIS, Hezbollah and lone-wolf attackers seek anonymous, secure, and readily available funding, which makes cryptocurrencies potentially valuable to them.[46] They engage in five financial activities using cryptocurrencies: fundraising, illegal trafficking, fund diversion, attack financing, and operational funding, considering aspects like anonymity, usability, security, acceptance, reliability, and volume. Anonymity protects users' identities; usability ensures easy transactions; security guarantees transaction confidentiality, integrity, and accuracy; acceptance denotes user community acceptance; and reliability refers to transaction speed and availability.

5. Artificial Intelligence Strategies for Detecting and Countering Dark Web Threats

Artificial Intelligence (AI) is crucial to combat cybercrime. These technologies enhance detection capabilities across various layers of the Internet, from the Surface Web to the Dark Web. By leveraging AI, complex risk factors and key threat signals can be

[46] Cynthia Dion-Schwarz, David Manheim, and Patrick Johnston, "Terrorist Use of Cryptocurrencies: Technical and Organizational Barriers and Future Threats" (Santa Monica, Calif: RAND Corporation, 2019), 13, https://doi.org/10.7249/RR3026.

identified, providing a significant advantage in proactively addressing and reducing cyber threats through data analysis and pattern detection.[47] AI offers advanced tools and techniques to aid law enforcement and cybersecurity professionals in more effectively identifying and combating the threats of the Dark Web.

AI as a transformative tool in threat intelligence that systematically analyzes extensive Dark Web datasets to identify patterns and trends associated with illicit activity. This analytical capability enhances the precision of law enforcement operations and informs the design of more resilient cybersecurity frameworks.[48] AI's ability to detect threats in real time enables it to swiftly identify and react to harmful activities such as malware distribution or the sale of stolen data, thus reducing potential damage by intervening before harm occurs. In the fight against fraud, AI excels at detecting irregularities in extensive datasets, uncovering fraudulent practices such as the trafficking of counterfeit products or the exploitation of fabricated identities. Moreover, AI can conduct sentiment analysis to assess the tone and context of discussions on Dark Web forums and other online platforms, allowing for the early detection of emerging dangers. This deeper insight aids law enforcement in predicting risks and developing targeted responses to the dynamic tactics of cybercriminals.[49]

To monitor criminal and terrorist activities on the Dark Web, researchers and security agencies consistently observe Dark Web Online Social Networks (OSNs) that facilitate illegal actions and forbidden content. These initiatives have led to the development of multiple AI models designed to examine sensitive data and related files.[50] One such model, created by scholars, employs AI to build a detailed dataset that captures

[47] Giuseppe Cascavilla, Damian Tamburri, and Willem-Jan Heuvel, "Cybercrime Threat Intelligence: A Systematic Multi-Vocal Literature Review," *Computers & Security*, 2021, 2, https://doi.org/10.1016/j.cose.2021.102258.
[48] Dipesh Ranjan, "Mitigating Dark Web Risks: The Role Of AI And Machine Learning," Forbes, accessed February 13, 2025, https://www.forbes.com/councils/forbestechcouncil/2023/05/18/mitigating-dark-web-risks-the-role-of-ai-and-machine-learning/.
[49] Cici Riski Sufi Amalia et al., "Non-Penal Policy in Tackling Cyber-Bullying Through Integrated Cyber-Prevention," *JURNAL LEGALITAS* 17, no. 1 (April 29, 2024): 38–48, https://doi.org/10.33756/jelta.v17i1.24900; Sofyan Rauf, "The Ideal Model for Returning Criminal Case Files Based on the Integrated Criminal Justice System Approach," *Philosophia Law Review* 4, no. 1 (2024): 21–42.
[50] Romil Rawat et al., "Autonomous Artificial Intelligence Systems for Fraud Detection and Forensics in Dark Web Environments," *Informatica* 47 (2023): 59, https://doi.org/10.31449/inf.v46i9.4538.

fingerprints and signatures associated with terrorist and criminal activities on Dark Web OSNs.

The model comprises of the following steps:

1) Data Collection Program: Detects OSN platforms that contain harmful content, messages, and files related to terrorism.
2) Terrorism Advance Passenger Information (API): Deploys web crawlers to gather data from selected malicious content such as hashtags, keywords, symbols, weapon images, and masked facial photos.
3) Dataset Creation: Organizes these data into a dataset that identifies high-risk scenarios and helps identify the locations and members of organizations participating in these activities, including actions such as liking, sharing, and commenting.
4) Classification Program: Categorizes event details and threats planned by cybercriminals, including their specific targets.
5) Data Cleaning involves refining the information to focus on critical threats, such as bombings, mass killings, and government attacks.

This structured approach enables the precise identification and monitoring of threatening activities, enhancing the ability of law enforcement and security professionals to effectively counteract these risks.

6. Conclusion

The increasing reliance of terrorist organizations on the Dark Web poses a growing challenge to global security. Through anonymity, encryption, and decentralized financial systems, groups such as Al-Qaeda, ISIS, and Hezbollah have successfully exploited the Dark Web to spread extremist propaganda, recruit new members, and finance operations without detection. The use of encrypted communications and cryptocurrency transactions further complicates counterterrorism efforts, allowing these groups to operate with minimal risk of exposure. The findings of this research emphasize that traditional counterterrorism methods are becoming insufficient for tackling cyber-enabled terrorism, necessitating a more adaptive and technology-driven approach.

To counter this evolving threat effectively, policymakers and law enforcement agencies must take the following actions: 1) Enhancing Cybersecurity Measures: Governments must develop AI-driven threat-detection systems to monitor encrypted terrorist communications and detect illicit cryptocurrency transactions in real time. Blockchain analytics tools can be leveraged to track suspicious financial activities. 2) Multidisciplinary Collaboration: Foster collaboration among cybersecurity experts, law enforcement, cultural and linguistic experts, and counterterrorism professionals. This collaborative approach can help us understand the nuances of terrorist communication in different cultural and social contexts and improve the accuracy of threat detection. 3) Regulating Dark Web Infrastructure: Lawmakers must introduce stricter policies to monitor VPN services, Tor networks, and encrypted messaging platforms that are frequently used by terrorists, while still preserving online privacy rights for legitimate users. Developing Advanced Legal Frameworks: Current international legal instruments must be updated to incorporate provisions for digital evidence collection, cybersecurity laws, and counter-terrorism measures tailored to the digital era.

Acknowledgments

The authors would like to thank Universitas Hasanuddin for resources provided to conduct this research. Sincere gratitude also goes to the reviewers and editors who have provided constructive feedback so that this manuscript looks worth reading and citing.

References

Abas, Zulkifli T., Fence M. Wantu, and Lisnawaty W. Badu. "The Police's Part in Preventing Online Prostitution Utilizing MiChat Application in Gorontalo City." *Distruption Law Review* 1, no. 1 (2023): 43.

Ali, Atif, and Muhammad Shareh Qazi. "Darknet: The Study of Emerging Challenges of Cyber Terrorism and Organized Crimes." *Pakistan Journal of Terrorism Research* 4, no. 2 (2022): 96–113.

Balhara, Amit, Sunil Ubba, Yugal Sharma, and Pronika Chawla. "Exploring and Analyzing Dark Web." In *SSRN Electronic Journal*, 1–5. SSRN, 2021. https://www.ssrn.com/abstract=3879619.

Bermudez, Dario, Jeremiah Onaolapo, Gianluca Stringhini, and Mirco Musolesi. "Under

and over the Surface: A Comparison of the Use of Leaked Account Credentials in the Dark and Surface Web." *Crime Science* 7, no. 17 (2018): 1–11. https://doi.org/10.1186/s40163-018-0092-6.

Beshiri, Arbër, and Arsim Susuri. "Dark Web and Its Impact in Online Anonymity and Privacy: A Critical Analysis and Review." *Journal of Computer and Communications* 7 (2019): 30–43. https://doi.org/10.4236/jcc.2019.73004.

Broadhurst, Roderic, Hannah Woodford Smith, Maxim Donald, and Bianca Sabol. "Cyber Terrorism: Research Review." Australian National University, Cybercrime Observatory, 2017.

Cascavilla, Giuseppe, Damian Tamburri, and Willem-Jan Heuvel. "Cybercrime Threat Intelligence: A Systematic Multi-Vocal Literature Review." *Computers & Security*, 2021, 1–26. https://doi.org/10.1016/j.cose.2021.102258.

Counter Extremism Project. "Terrorists on Telegram." Accessed February 13, 2025. https://www.counterextremism.com/terrorists-on-telegram.

Dion-Schwarz, Cynthia, David Manheim, and Patrick Johnston. "Terrorist Use of Cryptocurrencies: Technical and Organizational Barriers and Future Threats." Santa Monica, Calif: RAND Corporation, 2019. https://doi.org/10.7249/RR3026.

Dodd, Vikram. "British Airways Worker Rajib Karim Convicted of Terrorist Plot." *The Guardian*. Accessed February 14, 2025. https://www.theguardian.com/uk/2011/feb/28/british-airways-bomb-guilty-karim.

Finklea, Kristin. "The Dark Web: An Overview." Congressional Research Service, 2024. https://crsreports.congress.gov.

Firmansyah Isa, Muh. "Causes and Efforts to Counter a Crime." *Estudiante Law Journal* 4, no. 2 (October 15, 2022): 788–800. https://doi.org/10.33756/eslaj.v4i2.18273.

GeeksforGeeks. "Triple DES (3DES)." Accessed February 14, 2025. https://www.geeksforgeeks.org/triple-des-3des/.

Graham, Robert. "How Terrorists Use Encryption." *CTC Sentinel* 9, no. 6 (2016): 20–25.

Gupta, Abhineet, Sean B Maynard, and Atif Ahmad. "The Dark Web Phenomenon: A Review and Research Agenda." Perth: Association for Information Systems Electronic Library, 2019. https://aisel.aisnet.org/acis2019/1.

Ismail, Dian Ekawaty, Yusna Arsyad, Ahmad Ahmad, Novendri M. Nggilu, and Yassine Chami. "Collocation of Restorative Justice with Human Rights in Indonesia." *Legality : Jurnal Ilmiah Hukum* 32, no. 2 (September 20, 2024): 394–417. https://doi.org/10.22219/ljih.v32i2.35374.

Ivanov, Eduard. "Combating Cyberterrorism under International Law." *Baltic Yearbook of International Law* 14 (2014): 55–69.

Kadir, Nadiah Khaeriah, Judhariksawan Judhariksawan, and Maskun Maskun. "Terrorism and Cyberspace: A Phenomenon of Cyber-Terrorism as Transnational Crimes." *Fiat Justisia: Jurnal Ilmu Hukum* 13, no. 4 (2019): 333–44. https://doi.org/10.25041/fiatjustisia.v13no4.1735.

Kamps, Josh, and Bennett Kleinberg. "To the Moon: Defining and Detecting Cryptocurrency Pump-and-Dumps." *Crime Science* 7, no. 18 (2018): 1–18. https://doi.org/10.1186/s40163-018-0093-5.

Kaur, Shubhdeep, and Sukhchandan Randhawa. "Dark Web: A Web of Crimes." *Wireless Personal Communications* 112, no. 1 (2020): 1–28. https://doi.org/10.1007/s11277-020-07143-2.

Krumova, Snezhana. "From Surface to the Dark Web in the Realm of Terrorism." Law and Internet Foundation. Accessed February 13, 2025. https://www.netlaw.bg/en/a/from-surface-to-the-dark-web-in-the-realm-of-terrorism.

Malik, Nikita. "Terror in the Dark: How Terrorists Use Encryption, the Darknet, and Cryptocurrencies." London: The Henry Jackson Society, 2018.

Mandela, Ngaira, Tumaini Mbinda, and Felix Etyang. "Combating Dark Web Terrorism: Strategies for Disruption and Prevention." *International Journal for Research in Applied Science and Engineering Technology* 11, no. 8 (2023): 856–63. https://doi.org/10.22214/ijraset.2023.55259.

Merriam-Webster. "Anonymity." Accessed February 14, 2025. https://www.merriam-webster.com/thesaurus/anonymity.

Michael, Barak. "The Telegram Chat Software as an Arena of Activity to Encourage the 'Lone Wolf' Phenomenon." International Institute for Counter-Terrorism (IST), 2016. https://ict.org.il/the-telegram-chat-software-as-an-arena-of-activity-to-encourage-the-lone-wolf-phenomenon/.

Nazah, Saiba, Shamsul Huda, Jemal Abawajy, and Mohammad Mehedi Hassan. "Evolution of Dark Web Threat Analysis and Detection: A Systematic Approach." *IEEE Access* 8 (2020): 171796–819. https://doi.org/10.1109/ACCESS.2020.3024198.

Nggilu, Novendri, Mohamad Rivaldi Moha, Muhammad Ridho Sinaga, and Adelia Rachmaniar. "Judicial Review of Constitutional Amendments: Comparison Between India, Germany, Colombia, and the Relevancy with Indonesia." *Lex Scientia Law Review* 8, no. 1 (September 22, 2024). https://doi.org/10.15294/lslr.v8i1.1901.

Nithya, B, and P Sripriya. "A Review of Cryptographic Algorithms in Network Security."

International Journal of Engineering and Technology 8, no. 1 (2016): 324–31.

Ranjan, Dipesh. "Mitigating Dark Web Risks: The Role Of AI And Machine Learning." Forbes. Accessed February 13, 2025. https://www.forbes.com/councils/forbestechcouncil/2023/05/18/mitigating-dark-web-risks-the-role-of-ai-and-machine-learning/.

Rauf, Sofyan. "The Ideal Model for Returning Criminal Case Files Based on the Integrated Criminal Justice System Approach." *Philosophia Law Review* 4, no. 1 (2024): 21–42.

Rawat, Romil, Olukayode Oki, Rajesh Chakrawarti, Temitope Adekunle, José Gonzáles, and Sunday Ajagbe. "Autonomous Artificial Intelligence Systems for Fraud Detection and Forensics in Dark Web Environments." *Informatica* 47 (2023): 51–62. https://doi.org/10.31449/inf.v46i9.4538.

Saleem, Javeriah, Rafiqul Islam, and Muhammad Ashad Kabir. "The Anonymity of the Dark Web: A Survey." *IEEE Access* 10 (2022): 33628–60. https://doi.org/10.1109/ACCESS.2022.3161547.

Sharma, Kanika, and Tanvi Bhalla. "Future Towards Danger: The Terror of Cyber Attacks." *IITM Journal of Management and IT* 6, no. 1 (2015): 90–94.

Sönmez, Eda, and Keziban Seçkin Codal. "Terrorism in Cyberspace : A Critical Review of Dark Web Studies under the Terrorism Landscape." *Sakarya University Journal of Computer and Information Sciences* 5, no. 1 (2022): 1–21. https://doi.org/10.35377/saucis.05.01.950746.

Spalevic, Zaklina, and Milos Ilic. "The Use of Dark Web for the Purpose of Illegal Activity Spreading." *Ekonomika* 63, no. 1 (2017): 73–82. https://doi.org/10.5937/ekonomika1701073S.

Sufi Amalia, Cici Riski, Arista Ulfa Anggraini, Dominikus Rato, and Fendi Setyawan. "Non-Penal Policy in Tackling Cyber-Bullying Through Integrated Cyber-Prevention." *JURNAL LEGALITAS* 17, no. 1 (April 29, 2024): 38–48. https://doi.org/10.33756/jelta.v17i1.24900.

TechTarget. "Advanced Encryption Standard (AES)." Accessed February 13, 2025. https://www.techtarget.com/searchsecurity/definition/Advanced-Encryption-Standard.

TRAC. "Massive Migration to Telegram, the New Jihadist Destination." Accessed February 13, 2025. https://trackingterrorism.org/chatter/trac-insight-massive-jihadi-migration-twitter-telegram/.

Trozze, Arianna, Josh Kamps, Eray Arda Akartuna, Florian J. Hetzel, Bennett Kleinberg, Toby Davies, and Shane D. Johnson. "Cryptocurrencies and Future Financial Crime." *Crime Science* 11, no. 1 (2022): 1–35. https://doi.org/10.1186/s40163-021-00163-8.

Vilić, M. Vida. “Dark Web, Cyber Terrorism and Cyber Warfare: Dark Side of the Cyberspace.” *Balkan Social Science Review* 10 (2017): 7–25.

Weimann, Gabriel. “Going Darker? The Challenge of Dark Net Terrorism.” Washington, DC: Wilson Center, 2018.

———. “Terrorist Migration to the Dark Web.” *Perspectives on Terrorism* 10, no. 3 (2016): 40–44.