Darknet: The Study of Emerging Challenges of Cyber Terrorism and Organized Crimes

Dr. Atif Ali[*] & Dr. Muhammad Shareh Qazi[**]

Abstract

There are hints that terrorist organisations have begun using the dark web to conduct their illegal activities as law enforcement agencies have tightened oversight and control on the surface web. The most prevalent examples include using Bitcoin to request financial contributions, creating information-dissemination mirror websites, and making purchases on the dark web. Terrorist acts that are planned, carried out, and supported on the dark web are done with a higher level of expertise than those that are done on the open web. Cyber-terrorism is related to research on the symptoms and characteristics of terrorist offences on the dark web. This study may provide policy insights that may aid law enforcement officers in analysing the activities of terrorist organisations on the dark web.

Keywords: Darknet, Deep Web, Cyber Terrorism Crime, Pakistan.

[*]Dr. Atif Ali had a Postdoc in Artificial Intelligence from Malaysia (RMC Multimedia University Cyberjaya) and Ph.D. in Computer Science (Artificial Intelligence based Software Engineering) from PMAS Arid Agriculture university, Rawalpindi he is certified by OS Forensics. He is working hard to make the cyber world safe. He can be reached at atif.alii@yahoo.com.

[**]Dr. Muhammad Shareh Qazi is currently serving as an Assistant Professor at Department of Political Science, University of the Punjab Lahore. He is the author of the book titled 'Escalation Patterns in South Asia: Future of Credible Minimum Deterrence. He can be reached at shareh.polsc@pu.edu.pk.

1. Introduction

The internet's role in promoting terrorism has increasingly become more apparent since the 9/11 attacks in the USA. The security and stability of the nation are now threatened by a brand-new crime known as 'cyberterrorism'. Due to the focus of the international community, the struggle between law enforcement agencies and cyberterrorism offences has become more intense. Between June, 2015 and February, 2016, Twitter blocked 125,000 accounts associated with terrorism.[1]

1.1. History

On the one hand, these actions have severely punished those who commit cyberterrorism offenses and have slowed their growth; on the other hand, continually tightened network control has driven terrorists into a deeper network—the dark web. For example, the Islamic State's propaganda 'Al-Hayat Media Center', launched its new dark web website on the 'Shamikh' forum on November 15, 2015.[2] This website is the first infamous terrorist group's dark web presence. The Islamic State's declarations and their reactions to the terrorist attack in Paris (the series of coordinated terror attacks throughout the city that killed 130 and injured nearly 400 on November 13, 2015)[3], as well as songs and poems about the jihad that have been translated into English, Turkish, Russian, and other languages, are all included in the network's content. Although there has never been concrete evidence to support

[1] Onook Oh, Manish Agrawal, and H. Raghav Rao, "Information control and terrorism: Tracking the Mumbai terrorist attack through twitter," *Information Systems Frontiers, Springer* 13, no. 1 (2011): 33-43.
[2] Gabriel Weimann, "Terrorist migration to the dark web," *Perspectives on Terrorism, JSTOR* 10, no. 3 (2016): 40-44.
[3] Estrada, Mario Arturo Ruiz, and Evangelos Koutronas, "Terrorist attack assessment: Paris november 2015 and brussels march 2016," *Journal of Policy Modeling* 38, no. 3 (2016): 553-571.

this theory, some scholars and journalists have long held the belief that terrorist groups operate propaganda websites on the dark web. Their assessment was supported by the discovery of this website, showing that cyberterrorism offenses have spread to the "dark web world".[4]

It is crucial to have a thorough grasp of the types and traits of cyberterrorism crimes in the dark web world in order to effectively create anti-terrorism policies. There is not much systematic study on the types of darknet terrorism offenses, and research on the connection between terrorism and the darknet is largely fragmented. Domestic-related research lacking and foreign research is mostly focuses on darknet crimes and countermeasures. We mention the psychological need and demonstration of cyber terrorism crimes on the dark web. The final section is a succinct conclusion that summarises the arguments and analysis presented earlier and offers some closing remarks. The conclusion is a brief recap of the arguments and analysis offered earlier and includes some parting thoughts.

2. Literature Review

The phrase 'Dark Web' crimes specifically refers to cyberterrorism offences committed on the dark web. Since this type of cybercrime has not received much attention in literature, the researcher here interprets it as darknet terrorism crime. This article briefly examines the distinct connotations of cyber terrorism and the dark web to help explain the

[4] Atif Ali et al., "Robotics: Biological Hypercomputation and Bio-Inspired Swarms Intelligence," *In 2021 1st International Conference on Artificial Intelligence and Data Analytics (CAIDA), IEEE,* pp. 158-163, 2021.

concept's special connotation, in order to define "dark web terrorist crime".[5]

3. Analysis of Cyber Terrorism Crimes

Crimes related to terrorism committed online are known as cyberterrorism crimes. The concept's definition varies from country to country, and there is no widespread consensus. In particular, this article believes that the following two factors are primarily responsible for the reasons: The perception of it belonging to the concept of terrorism crime varies. Second, different concepts perceive the network differently. Walter Laqueur, a renowned American researcher on terrorism, has stated: No single term can encapsulate the full history of terrorism.[6] Scholars, international organizations, and even various nations have varying interpretations of terrorist crimes, which results in varying definitions, cyber terrorism crimes. Some academics equate cyber-terrorism crimes with terrorist-like cyber-attacks, identifying the network as the attack and victimization target and believing that only violent Cyber terrorism is defined as cyber activities that directly disrupt networks and destroy data.[7] According to the literature, cyber-terrorist actions are planned, politically motivated attacks on data, information, computer systems, computer programs, and data by non-governmental organizations or covert organizations that result in violent acts against non-combat and targets. This viewpoint restricts the range of offenses related to cyberterrorism. In order to further their

[5] Amanda Wasielewski, "From City Space to Cyberspace," *In From City Space to Cyberspace, Amsterdam University Press*, 2021.
[6] Jonathan Matusitz, "Terrorism and communication," *Sage*, 2012.
[7] Michael Kenney, "Cyber-terrorism in a post-stuxnet world," *Orbis* 59, no. 1 (2015): 111-128.

political objectives, terrorist groups use the internet to frighten the people and the government.[8]

In this, attackers use the network as a target, and criminals use it as a conduit and staging area. However, Cyber-terrorism offences should also cover the online publication of terrorist information, the planning of terrorist acts, the acquisition of illicit supplies, and illicit cash transfers in addition to cyber-terrorist attacks. The United Nations Counter-Terrorism Implementation Task Force (CTITF) categorises cyber-terrorist offences as the attacks that for the spread of false information about terrorist actions online, the use of the internet for communication and funding of terrorist activities, as well as the use of the internet to gather intelligence.[9] Further, Cyber-terrorism crimes are classified as one of three categories by Ulrich Sieber of Max Planck Institute for Criminal Law in Germany.[10] These crimes include using the internet to carry out destructive attacks on computer systems, disseminate illegal content to the general public, and plan and support other terrorist activities based on computers.[11] Despite the fact that their content varies, all of these definitions involve criminal acts on the network as the goal of the attack and the network as the media platform.

[8] Khushboo Farid Khan et al., "Artificial Intelligence and Criminal Culpability", *International Conference on Innovative Computing (ICIC), IEEE,* November 2021. (pp. 1-7).

[9] UN, "Counter-Terrorism Implementation Task Force (CTITF)" https://www.un.org/victimsofterrorism/en/about/ctitf.

[10] Marianne Wade and Almir Maljevic, "A War on Terror?: The European Stance on a New Threat, Changing Laws and Human Rights Implications," *Springer Science & Business Media*, 2009.

[11] Lisa Davidson, "Defining the Workforce and Training Array for the Cyber Risk Management and Cyber Resilience Methodology of an Army," *In ECCWS 2020 20th European Conference on Cyber Warfare and Security, p. 466. Academic Conferences and publishing limited, 2020.*

4. Difference between Dark Web and the Deep Web

The network's have borderless, zero-distance, immediacy features and function as connectivity, aggregation, and sharing, making it the perfect platform for auxiliary tools and propaganda used by terrorist organizations. On the other side, the network is neither unrestrained nor under any control. In order to control network content, network law enforcement personnel use information technology and government authorities to gather counterterrorism intelligence, take down terrorist organization websites, and restrict terrorist accounts. Terrorist groups have started to use the dark web, which has softer regulations and more anonymity. The definition of the dark web differs in describing the technical details. According to Tor's official website, the dark web is a collection of difficult websites to access. According to Daniel Moore, the dark web refers to a hidden network of encrypted sites.[12] According to Patrick Tucker, the dark web is a website that can mask a server's IP address, and he believes that the dark web is not so much a network; it is a way to achieve online anonymity. Whereas, the researchers describe the characteristics of the dark web as converging and believe that the security based on anonymous services is the unique advantage of the dark web. The dark web mainly includes the Tor network, I2P network, and free network. The largest of them is the Tor network, followed by the I2P network. The deep web, often confused with the dark web, refers to a collection of websites that are not searchable by search engines. The invisible web is another name for the deep web. The Surface web, also known as the visible web, is a collection of

[12] Jones, Sir Kenneth Lloyd, (Sir Ken), (born 13 June 1952), global counter terrorism, policing and cyber security consultant, since 2015; Defence and Security Adviser, British Embassy, Washington DC, 2013–14. *Who's Who*, 2009.

websites that can be retrieved. The deep web has a very vast capacity. Barker said that the network's overall capacity should be 500 times the content capacity that search engines can search. On the other hand, past studies divide the deep web into six categories: dynamically generated webpages, webpages that can be browsed in specific scenarios, non-HTML/scripted content, unlinked sites, private sites, and restricted-access sites.[13] The deep web, or one of its subcategories called limited access sites, includes the black web. It is challenging to determine the precise extent of the dark web due to its anonymity. Researchers believe the dark web is much smaller than the deep web, and it is likely to be smaller than the surface web.

5. Analysis of Cyber Terrorism Crimes and the Dark Web

The needs of cyberterrorism criminals on the dark web can be divided into two categories: the security demand for anonymous actions and the psychological desire for cultural identity.

5.1. Cultural Identity-Related Psychological Needs

Different countries have different cultures in the real world, and the online world is no exception. On the internet, communities are formed by homogeneous people who share interests and ideals, splitting the online world into discrete regions. In contrast to the territorial boundary in the real-world geographical sense, the borders of various territories in the online world are shaped by culture. The subculture theory holds that society has a mainstream culture as well as a number of subcultures

[13] Maura Conway, "What is Cyberterrorism and How Real is the Threat?: A Review of the Academic Literature, 1996–2009" *Cyber Behavior: Concepts, Methodologies, Tools, and Applications* (2014): 217-245.

that are specific to different groups.[14] The development, propagation, and dissemination of terrorist activities are all significantly influenced by violent subcultures, which also provide crucial moral justifications for individuals to engage in terrorist and violent behavior. Terrorists' cultural tendencies are frequently disregarded and excluded on the surface web, where mainstream culture predominates; however, on the dark web, deviant behaviors that go against mainstream culture and society's established order are protected by anonymous services to expand living space. Here, the widely known subculture of terrorist groups can flourish, luring in like-minded individuals and broadening their cultural influence.[15]

5.2. Anonymous Operations

Anonymity can help cyber-terrorists plan, organize, and commit crimes while avoiding legal repercussions by ensuring the network's safety. There is no anonymous mechanism built into the surface network. Law enforcement agencies easily monitor the activities of terrorist organizations, and network behaviors are easily tracked, traced, and analyzed. Unlike the surface network, the dark network was created to provide anonymity services to its users. “The Tor network, for example, was created by the US Naval Research Laboratory and launched in 2002 to enable virtual communication.”[16] The I2P network is an anonymous project that allows users to surf anonymously, chat anonymously, write blogs, and send information without being

[14] Kawser Ahmed, "Canada’s cyber security in a globalized environment," *Routledge Companion to Global Cyber-Security Strategy*, 2021, 451-462.
[15] Ibid.
[16] Beshiri, Arbër S., and Arsim Susuri, "Dark web and its impact in online anonymity and privacy: A critical analysis and review," *Journal of Computer and Communications* 7, no. 03 (2019): 30.

monitored by network monitoring tools. As some proponents have stated, anonymity is the soul of the dark web, and this characteristic is exactly what cyber-terrorism activities demand.[17]

5.3. Dark Web Search Engines

It is possible to access dark websites through an anonymous proxy using TOR2WEB-type services regularly indexed on Google. However, accessing dark websites through an anonymous proxy is not recommended due to concerns about attribution. Traditional search engine crawlers such as Google and Bing cannot access TOR-connected sites, which means that content on the Dark Web must be found through non-standard crawling and indexing services.[18] Some search engines are superior to others in terms of performance such as in terms of results (due to the websites that their platforms crawl), advanced search options (such as boolean or multilingual searching), and intent. Investigators should search multiple search engines and compare results as part of their investigation or narrow to search engines that provide a specific service.

5.4. The Demonstration of Terrorism Crimes on the Dark Web

Research on cyberterrorism offenses on the dark web and their means of expression can theoretically serve as a guide for practice and has good propositions for cyber-terrorism. Although the dark web theoretically offers special conditions for cyber terrorism offenses, due to its anonymity and frequent domain name changes, it is challenging

[17] Marshall W. Fishwick, "Cyberspace" *Popular Culture*, 140-143, 2021.

[18] Martin Steinebach, et al., "Detection and analysis of tor onion services," *In Proceedings of the 14th International Conference on Availability, Reliability and Security*, pp. 1-10. 2019.

to gather criminal evidence there.[19] Terrorist organisations have not frequently used the dark web to commit atrocities. The potential of anonymous services and their attraction to Islamic State of Iraq and Syria (ISIS) and other terrorist organisations cannot be ignored by intelligence officials. But according to this article, the amount of confirmed criminal cases will rise over time as network reconnaissance technology advances.

5.5. Use of Bitcoin to Raise Funds / Financial Crimes

The network domain name address for the virtual currency known as Bitcoin (BitCoin) is made up of 64-bit digits that have meaning. Today, it is a brand-new method of Internet finance. Transactions with Bitcoin have the features of anonymity because they are totally based on peer-to-peer networking and do not require the personal information of both buyers and sellers. The 'Hawala' network or conventional banking are the two methods available for traditional fund transfers. In this way, trust is the foundation of the Hawala network, which uses it to thwart terrorist actions. The banking system makes use of established international standards for cross-border fund transfers. The use of banks by terrorist organizations, in contrast, puts their identifying information at risk, compromises the security of fund transfers, and endangers members' personal safety. Bitcoin, in contrast to the other two systems, takes technical efficiency and security into account. Fast

[19] Robert Brinson, Hayden Wimmer and Lei Chen, "Dark Web Forensics: An Investigation of Tracking Dark Web Activity with Digital Forensics," *In 2022 Interdisciplinary Research in Technology and Management (IRTM), IEEE,* pp.1-8, 2022.

internet transactions protect both parties' identities throughout the transfer of funds.[20]

According to the thirteenth news channel of KRDO in the United States, users claimed to permit visitors to donate Bitcoin to terrorist organisations. They also promoted the anonymity of Bitcoin transactions and encouraged supporters to do so. Deutsche Welle and Ghost Sec, a hacker group opposed to the Islamic State, both reported on the use of virtual currencies by the Islamic State for Iraq and Syria (ISIS), claiming that "an Islamic State's Bitcoin wallet had received $23 million worth of Bitcoin within a month".[21] Although these examples demonstrate how Bitcoin has been used by terrorist groups to generate money, it's vital to keep in mind that Bitcoin only represents a small portion of the total funding available to terrorist groups. Terrorist groups continue to use kidnapping, extortion, smuggling, oil sales, organ trafficking, and other conventional means of funding as well.

5.6. Use of Mirror Sites

Because dark web login takes additional tools and the domain name is difficult to remember, there are significantly fewer users of the dark web than there are of the surface web. Additionally, the dark web's access speed is slower than the surface web's due to the complicated security systems' design, which somewhat deters users from visiting the dark web. Due to the small audience size, the propaganda function of the dark web has been significantly diminished. As a result, rather than serving as a terrorist organization's primary means of

[20] Todd Sandler, "Role of Terrorist Groups," *Terrorism*, 2018.

[21] Gabriel Weimann, "Going dark: Terrorism on the dark web," *Studies in Conflict & Terrorism* 39, no. 3: 195-206, 2016.

dissemination, the dark web functions more like a reserve army and emergency force. On the dark network's website, the terrorist organisation supports the resources used by the surface network. By sharing the link address of the dark network mirror website in anonymous forums, chat rooms, or emails, members and supporters can be routed to the new Positions after the surface network website is taken down. For example, on December 15, 2015, a mirror website was uncovered on the Islamic State's covert website. The website replicated many bulletin board posts, including files and movies that over time were translated into numerous languages. On April 29, 2016, two additional Islamic State dark websites were uncovered. Compared to the previous one, the web pages were incomplete and only included basic information.

5.7. Usage of Black-Market Platforms to Purchase Materials

The dark web's anonymity gives terrorists a forum for unrestrained expression while also allowing for illicit behaviour. One of the most crucial is a trading platform for the underground market. Alpha Bay, Agora, SilkRoad, Crypto Market, and others[22] are dark web trading platforms similar to eBay, Amazon, and other surface network trading platforms. These platforms sell legal and illegal goods and services, such as drugs, firearms, pornography, stolen accounts, fake passports, and hacker job, because terrorist organizations and lone wolves can easily obtain these illegal services. For this some refer to the dark web as a "terrorist shopping paradise".[23] Even though these websites are

[22] Kamshad Mohsin, "The Internet and its Opportunities for Cybercrime–Interpersonal Cybercrime," Available at SSRN 3815973 (2021).

[23] Tim Owen, "Cyberterrorism: some insights from Owen's genetic-social framework," *Rethinking Cybercrime, Palgrave Macmillan, Cham,* pp. 3-22, 2021.

illegal, shutting them down is extremely difficult due to the protection provided by dark web anonymity technology. To combat criminal activities, the US Federal Bureau of Investigation (FBI) shut down the Silk Road website. The Silk Road 2.0 website went live in less than a month. The FBI tracked users and servers for a year before blocking them again, but Silk Road version 3.0 is back online.[24] The operation of 16 darknet shopping platforms was studied in the literature from 2013 to 2015, and it was discovered that the platform's main transaction items were various drugs. For example, ecstasy and marijuana transaction accounted for 25% of the total.

6. Characteristics of Darknet Terrorism Crimes

6.1. Concealment

Terrorism crimes on the darknet are more hidden in their methods than terrorism crimes on the surface network. Hence, users can browse websites anonymously without revealing their identities. Thus, anyone can set up untraceable servers for anonymous activities using dark web technologies like Tor. This anonymous service helps terrorist organisations hide their identities and criminal activity. Even software developers, ISPs, and law enforcement organisations struggle to track routing information. They are unable to know the identity of the operator or the location of the server. After establishing the Tor connection, all messages between the server and the user are encrypted. Further, terrorist organizations can make inflammatory statements, engage in illegal activity, and carry out criminal operations covertly by using content-blocking tools. This approach makes it difficult to

[24] Silviu-Elian Mitră, "The Structure of Cyber Attacks," *International Journal of Information Security and Cybercrime (IJISC)* 9, no. 1, pp: 43-52, 2020.

prosecute terrorists since it keeps them hidden on the dark web. The Department of Defense Advanced Research Projects Agency (DARPA) in the United States is working on a project called MEMEX to investigate methods for de-anonymizing TOR users.[25] The Federal Bureau of Investigation (FBI), the National Security Agency (NSA), and the Department of Homeland Security (DHS) work on projects investigating TOR's flaws and vulnerabilities.[26] TOR's core framework, on the other hand, has remained safe so far. Users can still effectively ensure their behavior and identity are hidden by updating and upgrading Tor programs.

6.2. Technical

It is seen that Darknet terrorism crimes are more technically sophisticated than surface-layer terrorism crimes. Terrorist organizations can use Google to find the necessary websites and social networking sites like Facebook and Twitter to spread ideological propaganda and communication. These mature commercial network platforms and tools are designed for everyday users. These have a user-friendly interface, and simple operation, and can be used effectively without complicated settings. The need for anonymity protection raises the technical threshold for dark web terrorist crimes for two reasons: First and foremost, anonymity services must be provided via specialized software. To access the dark web anonymously, users must use TOR, I2P, Freenet, and other programs with some basic settings, which adds to the operation's complexity. Second, the dark web's

[25] Ehney, Ryan, and Jack D. Shorter, "Deep Web, Dark Web, Invisible Web and the Post ISIS World," *Issues in Information Systems* 17, no. 4, 2016.
[26] Danny Bradbury, "Unveiling the dark web," *Network security* 2014, no. 4, pp: 14-17, 2014.

anonymity isn't always guaranteed. Anonymity is only a relative concept in the game process of researching flaws, gaps, and techniques of deanonymization with law enforcement agencies. Users must therefore update tools regularly to maintain their anonymity and security. They must know about various auxiliary software, which raises the dark web's technical bar.

6.3. Auxiliary

Darknet terrorism crimes are to assist in surface network terrorism crimes. Thomas Rid of King's College London's Department of War Studies maintained that although there are countless criminal acts on the Deep Web and evidence of terrorist organizations using the Deep Web to commit crimes is very rare so far.[27] On the one hand, since it's hard to conduct an investigation on the dark web because of anonymity, hence, Dark web terrorism crimes, on the other hand, do not dominate cyber terrorism crimes.[28] The dark web's usage for terrorist and criminal purposes has also been impeded by its technical faults and restrictions. Thomas Reid is of the opinion that the anonymity service on the dark web can occasionally be sluggish and inconsistent, making it challenging to use.

[27] Thomas Rid and Peter McBurney, "Cyber-weapons" *the RUSI Journal* 157, no. 1, pp: 6-13, 2012.
[28] Ibid.

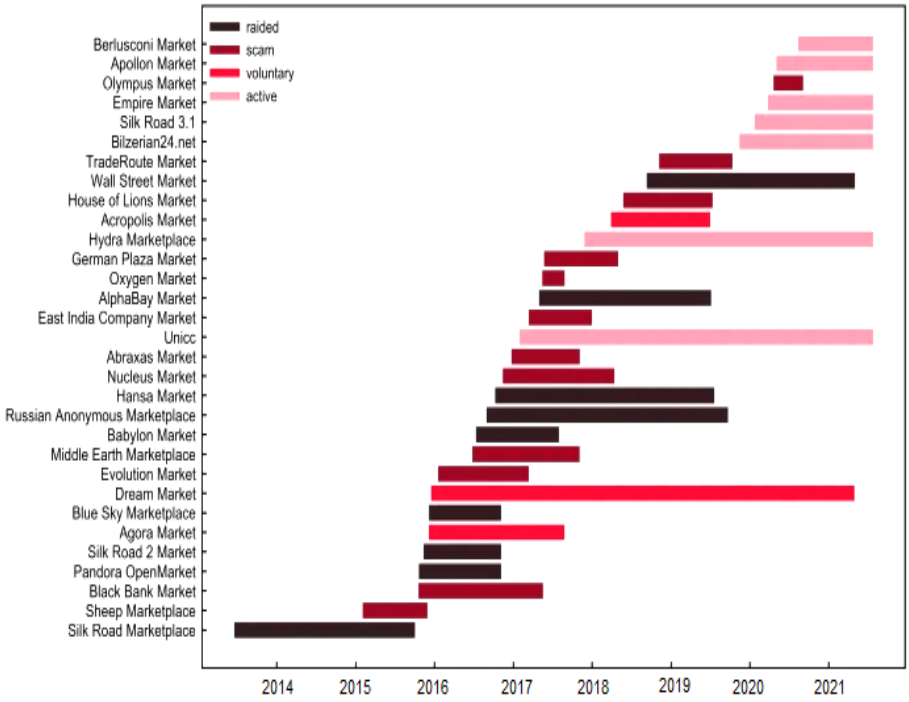

Figure 2: Trend Analysis of Darknet market.[29]

7. Conclusion

Evidence suggests that about the same time that law enforcement organizations tightened their oversight and control over the surface web, terrorists started using the dark web to carry out illegal acts. The most typical manifestations include the following: Mirrored websites are being created to make the usage of Bitcoin for fundraising easier. Terrorism crimes committed on the dark network are more difficult to detect, more technically complex in their execution, and more auxiliary in their role than terrorism crimes committed on the surface network. They are used to disseminate ideas and get goods in the black market.

[29] Ball, Matthew, and Roderic Broadhurst, "Data capture and analysis of darknet markets," Available at SSRN 3344936, 2021.

Investigating the manifestations and traits of terrorist offenses on the dark web also helps law enforcement organizations gain a better understanding of the specific actions of terrorist organizations on the dark web, which can be helpful in combating online piracy. To battle cyberterrorism crimes and create anti-terrorism policies in the new environment, one must have a complete understanding of the forms and traits of cyberterrorism crimes in the "dark web world." While Pakistani case studies are few in number, international research studies mainly focus on darknet crimes and countermeasures. There is a lack of systematic studies on the different sorts of darknet terrorism offenses, and there is scattered research on the connection between terrorism and the darknet. As People engage in covert activity and leave no paper trail on the dark web. It acts as a hub for trade in guns, drugs, and child pornography. The anonymity of this forum is what drives these actions. On the dark web, new substantial marketplaces will emerge that might offer an increasing variety of risky products and activities. The criminal underworld would become more difficult to investigate if it were fragmented into dark nets or private networks. To address similar incidents, security professionals and law enforcement must create new methods to quickly identify hostile online behavior.

Western academics are much interested to study the connection between the dark web and terrorism. The first evidence that terrorist organizations were doing this was the propaganda website of the Islamic State (ISIS), which was discovered on the dark web in November 2015. This research introduces dark web terrorism crime and outlines the contributions of three elements—anonymity, technicality, and auxiliary—to its features. In theory, the anonymity and underground culture of the dark web provides an environment that

is favorable for terrorist activities. However, terrorist organizations use the dark web to carry out other illicit activity mostly. The great degree of complexity of the inquiry is one of the primary reasons for the low user base, unstable nature, and high threshold of dark web technologies. On the dark web, there is a demand for terrorism that cannot be ignored. As technology advances, the dark web will likely see an increase in activity from terrorist organizations. Therefore, tracking and analyzing how terrorist offenses operate on the dark web has a significant impact on counterterrorism initiatives.