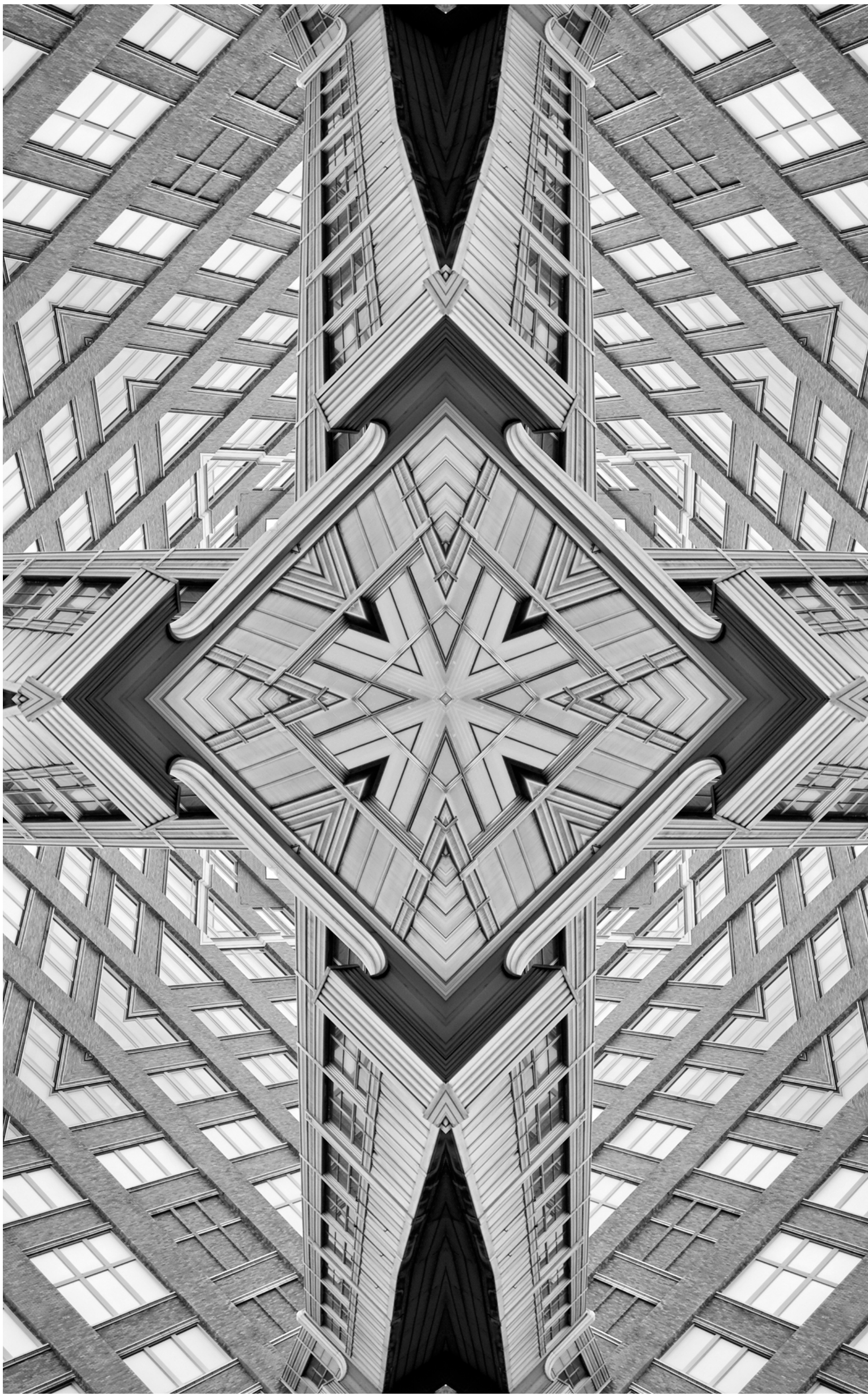
Issue Brief

ISSUE NO. 717
JULY 2024



The Dark Web as Enabler of Terrorist Activities

Soumya Awasthi

Abstract

The dark web and terrorism have become closely intertwined, presenting new challenges to existing security frameworks globally. This brief examines the role of the dark web in enabling terrorist activities, from communication and recruitment to radicalisation and propaganda dissemination. It reviews current literature to highlight the ecosystem of the dark web and its ramifications on national security. The analysis describes the strategies adopted by terrorists in cyberspace, from exploiting mainstream social media platforms to leveraging encrypted channels and clandestine marketplaces. It also highlights the challenges confronting law enforcement and regulatory bodies in monitoring and combating terrorist activities on the dark web, underlining the need for global collaboration. It outlines recommendations for policymakers and security stakeholders to fortify cyber counterterrorism efforts while examining the specific challenges to India.

Attribution: Soumya Awasthi, "The Dark Web as Enabler of Terrorist Activities," *ORF Issue Brief No. 717*, July 2024, Observer Research Foundation.

Introduction

Evolving terrorist tactics reflect a pragmatic adaptation to available resources and technological advancements. The vulnerability landscape is thus continually evolving, characterised not merely by conventional power differentials but by the emergence of novel susceptibilities.

The proliferation of the internet has exacerbated this trend, facilitating the recruitment and radicalisation of tech-savvy, self-radicalised individuals. The dark web,[a] in particular, has become a hotbed for cybercrime by non-state actors. Terrorist groups have expanded their cyber capabilities, using the dark web for recruitment drives, fundraising, and operational planning, facilitated by social media and emerging technologies such as Artificial Intelligence (AI). The dark web has progressed in the virtual space[1] and is used for circulating disinformation, as in the ongoing Hamas-Israel conflict.[2]

Technology has given these organisations unparalleled opportunities for their communications outreach. Terror groups are using innovative methods and platforms for swift messaging amongst their cadre, volunteers, and recruits. In addition to their own websites, e-magazines, and publishing houses, some groups are active on platforms such as Telegram, Facebook, Signal, and other chatrooms and forums, which enable them to recruit sympathisers and supporters and disseminate propaganda.

Traditional and cyber methods converge in contemporary terrorism, with technology being both a force multiplier and a double-edged sword. As such, counterterrorism efforts need to extend their focus beyond thwarting physical assaults to countering the narrative warfare propagated in the digital domain.

This brief discusses the ways in which terror organisations are exploiting the dark web for recruitment, radicalisation, and disinformation. Drawing insights from a case study, it offers policy recommendations for how India can adopt best practices to secure the country from the impact of the dark web.

Dark Web in the Cyberspace

The dark web and the deep web together constitute a significant part of cyberspace, spanning over 96 percent of the internet.[3] In 2023, the dark web had an average of 2.5 million daily visitors via Tor.[4] In September 2023,

[a] The dark web is a part of the internet that comprises hidden websites, mostly illegal in nature, that cannot be easily found through conventional search engines and which require specialised software to access the content. See: Brenna Cleary, “What is the Dark Web and How Do You Access It,” Norton, May 14, 2024, https://us.norton.com/blog/how-to/what-is-the-dark-web

Germany became the country with the highest user base for Tor,[b] displacing the United States (US).[5] Other countries with the highest numbers of Tor users are Finland, India, and Russia.[6]

Illicit content dominates the dark web, at 57 percent, including crypto accounts, online banking access, and e-wallets. Data breaches have a palpable economic toll, costing US$9.44 million per incident. Cybercriminals capitalise on the anonymity of the dark web by offering credit card details with substantial balances for a mere US$110.[7] Simultaneously, malware and Distributed Denial of Service (DDoS) attacks trade briskly, with 1,000 threat installations fetching US$1,800.[8]

Demographically, the dark web's population is predominantly male (84.7 percent).[9] Among these users, the majority fall within the age bracket of 36-45 and include malicious insiders, hacktivists, and nation-state actors[c] perpetuating cyber threats at a global scale.

Despite efforts to dismantle marketplaces like Silk Road and Alpha Bay, the dark web has witnessed the mushrooming of successors such as In The Box, Genesis Market, and 2Easy, which offer illicit wares ranging from cryptocurrency accounts to forged identities and contraband substances. The anonymity around these transactions presents formidable challenges for law enforcement agencies.

[b] The Onion Router (Tor) is a software that was created in 2002 and enables anonymous web search. It is one of the largest deployed anonymity networks, consisting of thousands of volunteer-run relays and millions of users. See: "Tor Metrics," https://metrics.torproject.org/

[c] Nation-state actors are individuals hired to steal sensitive data, gather confidential information, or disrupt another government's critical infrastructure. See: "What is a Threat Actor?" IBM, https://www.ibm.com/topics/threat-actor#:~:text=or%20sensitive%20information.-,Nation%2Dstate%20actors,disrupting%20another%20government's%20critical%20infrastructure

Dark Web and Terrorism

Technological innovations such as Tor, Bitcoin, and cryptocurrencies enable criminals to operate anonymously, which fuels the expansion of the dark web. Dark web activities are divided into four main categories:[10] network security; cybercrime; machine learning; and drug trafficking.

Terrorist entities leverage cyberspace for propaganda dissemination, engaging in information warfare on social media. The use of the internet to disseminate violent extremism exploits the medium for terrorist propaganda dissemination and recruitment, as seen in the case of the Christchurch shooting.[d,11]

Terrorist propaganda distribution involves publicly accessible anonymous proxy servers, anonymising services like Tor, and cryptocurrencies to perform financial transactions, all of which pose challenges to online surveillance and digital forensics. Secure mobile devices and encrypted communication applications like Telegram or Signal also provide terrorists with secure platforms for coordination, allowing them to evade detection.

The use of the dark web by the Islamic State of Iraq and Syria (ISIS) for the purposes of propaganda dissemination and operational coordination highlights the platform's appeal to terrorist groups. Notably, manuals such as "How to Survive in the West: A Mujahid Guide" provide instructions on internet privacy and the use of Tor, demonstrating terrorists' adaptability to technological advancements.[12] The group's media outlet, Al Hayat Media Centre, posts links and instructions on accessing their dark web site on forums associated with ISIS and distributes the information via their Telegram channel.[13]

In addition to establishing their online platforms, terrorists leverage interactive tools such as chatrooms, instant messengers, blogs, video-sharing sites, and social media networks like Facebook, MySpace, Twitter, Instagram, and YouTube for training and instruction.[14] The dark web is actively used for disseminating extremist content and facilitating illicit activities, thus facilitating terrorist communication and coordination. For example, the Turkish-language dark web forum, Turkish Dark Web, circulated manuals on building explosives and weapons and how to use a biological weapon, fostering discussions on their efficacy and potential applications.[15,16] Moreover, volunteers are trained to use the dark web to communicate with a global network of terrorists.[17]

[d] Terms like 'violent extremism' and 'cyberterrorism' comprise a spectrum of online activities aimed at advancing terrorist agendas, including cyberattacks and propaganda dissemination.

Covert Use of the Dark Web

The use of the dark web for terrorist activities has evolved in the 21st century. Marc Sageman, author of the book *Understanding Terror Networks*, argues that the dark web creates a habitat for interaction and uses chat rooms to build ideological relationships—a vital tool in radicalising young people.[18] Terrorist organisations employ online platforms to establish communication channels, facilitating interactions among members, followers, media outlets, and the broader public. Terrorist groups perceive the dark web and similar channels as the most secure means of communication. ISIS, for example, despite intense scrutiny, has demonstrated significant adaptability by resorting to lesser-known social media platforms like Diaspora and VKontakte, Russia's largest social network.[19]

Recent trends reveal that ISIS and other jihadist factions have embraced novel online applications, enabling users to disseminate messages to an extensive audience through encrypted mobile applications like Telegram.[20,e] Groups like ISIS, Al-Qaeda, Hamas, and Hezbollah use Telegram for different reasons, such as finding new members, raising money, encouraging violence, and planning attacks. ISIS also uses social media to disseminate propaganda material[21] and has also created a list of communication applications.[22,23]

In 2015, the Islamic State issued a tech tutorial to its followers, guiding them on how to keep themselves secure from the government surveillance system. It gave a list of applications ranked based on the level of encryption of chat applications. The list ranked apps like SilentCircle, Redphone, and Signal as the 'Safest'; Telegram, Wickr, Threema, and Surespot as 'Safe'; and WeChat, WhatsApp, Hike, Viber, and Imo.im as 'Unsafe'.[24]

Terrorist groups like Al-Qaeda in the Arabian Peninsula (AQAP), Ansar al-Sharia in Libya (ASL), Jabhat al-Nusra (JN), and Jaysh al-Islam in Syria also use the dark web through similar means. Terrorist activities on the dark web primarily encompass the following categories:

[e] Another application that terrorists use is TrueCrypt (Ratliff, 2016).

- **Internal communication and external propagation**: The dark web provides terrorists with secure channels for internal communication, facilitating covert information exchange and broader connectivity for planning, organising, deploying, and executing terrorist operations. Terrorist organisations also leverage the dark web to disseminate extremist ideologies.[25]

- **Recruitment and training**: Terrorist groups recruit new members via the dark web and provide training to followers worldwide, including courses on bomb-making and executing terrorist attacks, mainly targeting "lone wolf" attackers. The anonymity afforded by the dark web complicates efforts by counterterrorism agencies to identify and thwart radicalised individuals.[26]

- **Fundraising and financial transactions**: In addition to conventional methods such as oil sales, smuggling, and kidnapping, terrorist organisations are increasingly utilising digital cryptocurrencies such as Bitcoin and the dark web for fundraising, including Bitcoin donations, online extortion, human trafficking, and organ trafficking. For example, a deep web page called 'Fund the Islamic Struggle without Leaving a Trace' uses a dark wallet app to receive donations through Bitcoin.[27,28] Recently, Islamic State Khorasan Province, through its magazine *Voice of Khorasan*, asked followers and sympathisers to make donations in cryptocurrencies like Monero (XMR) via the dark web.[29] Between 2020 and 2023, Hamas received around US$41 million in cryptocurrency, while the Palestine Islamic Jihad received about US$93 million in the same period.[30]

- **Procurement of weapons**: The dark web is a marketplace for terrorists to procure firearms and ammunition, with illegal trading sites like Silk Road facilitating transactions. For instance, *EuroGuns* is an online platform that sells weapons. There is also a threat of terrorists acquiring dual-use elements like chemicals and biological medicines, which they could use for improvising and making biological weapons.[31] Additionally, on sites like AlphaBay, terrorists can buy books like the *Terrorist's Handbook* and *Explosives Guide*. They can also procure fake documents and passports from services like the Fake Documents Service.[32] Terrorist organisations could also acquire uranium, plutonium, and other nuclear materials via the dark web.

- **Purchase of illicit drugs:** Among the range of illicit trade in dark web markets, also known as crypto markets, drug trafficking is being carried out frequently through dark web platforms. According to the 2023 annual report of the International Narcotics Control Board (INCB), South Asia has 39 percent of the global opiate consumer base, with India emerging as a focal point for opiate distribution.[f,33]

- **Use of AI and dark web:** Terrorists are using the dark web to create deepfakes, which can increase the reach of their propaganda dissemination. Tools like Google Gemini and ChatGPT allow easy access to manuals on making bombs at home. AI programs like 'Lavender' and 'Where is Daddy?'[34] are also enabling more refined and sophisticated warfare methods.

[f] The report underscores the nation's northeastern region as a hotspot for illicit opium cultivation and trafficking (United Nations, "Drug Use") while also highlighting the influx of heroin from Southeast Asia, notably Afghanistan. The Narcotics Control Bureau (NCB) of India has noted a surge in darknet-related drug seizures and trafficking incidents. Indian agencies, in collaboration with the US, conducted an operation in May 2024 that led to the seizure of INR 130 crores and the arrest of a cartel involved in cryptocurrency-facilitated darknet drug transactions ("ED Seizes Rs 130 Crore", 2024). In a separate incident in April 2024, the Gujarat police intercepted a consignment of LSD and hybrid cannabis valued at INR 43 lakh, procured from Bangkok via the dark web (Press Trust of India, 2024).

The Global Landscape of Dark Web Activities and Countermeasures

The United Nations is undertaking comprehensive research endeavours and collaborative events to combat the anonymity and intricacies of the dark web as well as its far-reaching implications on global security, with a specific focus on the illicit trade of small arms, light weapons, drug trade, and terror financing. Notably, the UN Office for Disarmament Affairs (UNODA) has examined how dark web platforms facilitate illegal arms trading and presenting formidable challenges for law enforcement agencies and global security mechanisms.[35] However, there has been no recent resolution by the United Nations Security Council (UNSC) after Resolutions 2178 (2014) and 2396 (2017) that discuss the rising threat of dark web. The Delhi Declaration 2022[36,g] under India's G20 Presidency is the latest proposal on countering the use of new and emerging technologies for terrorist purposes.

UN publications have also highlighted the exploitation of the dark web and social media platforms for drug distribution.[37] Concurrently, the UN Human Rights Council has underscored the growing prominence of the dark web in conjunction with escalating cybersecurity threats worldwide, as elucidated in the MUNUC35 publication by the Model United Nations of the University of Chicago in 2023.[38] According to estimates by the United Nations International Children's Emergency Fund (UNICEF), approximately 2.5 million individuals fall victim to trafficking globally at any given time, with children constituting nearly one-third of these victims[39] as a significant portion of child trafficking activities are facilitated through the dark web.

Reports from the Financial Action Task Force (FATF) External Affairs Committee underscored the focus of terrorist organisations on virtual currencies, online payment mechanisms, and dark web transactions.[40] A study conducted at King's College London revealed that over 60 percent of more than 2,700 darknet sites host illicit content.[41]

[g] The Delhi Declaration (MEA, 2022) spotlighted the escalating utilisation of new and emerging technologies by terrorists for diverse purposes, from recruitment and incitement to the financing and planning of illicit activities. The declaration emphasised the imperative for striking a balance between technological innovation and robust counterterrorism measures, urging all G20 member states to implement pertinent Security Council Resolutions (United Nations Security Council Counter-Terrorism Committee Executive Directorate, 2022).

• The Complex Landscape in India

In India, navigating the dark web and the deep web has implications for security and law enforcement efforts. Despite a lack of concrete evidence, the dark web serves as a hub for illicit activities such as drug sales and counterfeit currency circulation. This is exacerbated by factors like the private ownership of technological tools, a commercial-oriented mindset, and the prevalence of anonymity, which makes the entire ecosystem vulnerable.

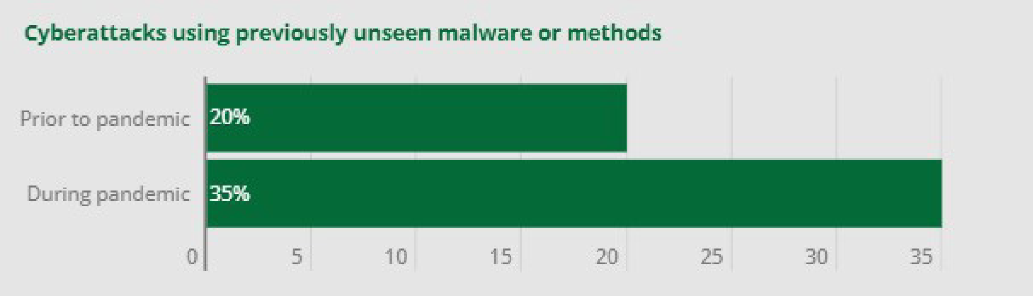
• Cybersecurity Consensus and Guidelines

In India, there is no explicit authorisation to conduct operations against terrorists on the dark web, unlike in countries such as China, the US, and various European nations. These countries empower their agencies to establish a visible presence on the dark web, engaging directly with terrorist groups to apprehend perpetrators. However, in India, the conversion rate of cyberattacks into capturing terrorists is less than 1 percent,[42] primarily due to the absence of legal mandates and established government guidelines defining cyberterrorism.

• Global Challenges and the Pandemic

The COVID-19 pandemic exacerbated challenges pertaining to the dark web and the deep web, resulting in a surge in illicit transactions, including the sale of counterfeit medical supplies and counterfeit COVID-19 vaccines.[43] The anonymity offered by the dark web has facilitated these illicit markets, presenting novel challenges for global law enforcement agencies tasked with combating the dissemination of misinformation and illegal commodities during a public health crisis.[44] Sophisticated cybercriminal tactics, exemplified by tools like OpenBullet, underscore the evolving nature of cyber threats during and after the pandemic.[45] These phenomena can be attributed to arrangements like ‘Bring Your Own Device’ (BYOD) setups, which were aimed to facilitate work from home (WFH).

Figure 1: Cyberattacks Before and During the COVID-19 Pandemic



Source: Nabe (2023)[46]

- **Surveillance and Detection**

The accessibility of the dark web has attracted both legitimate users and criminals. However, sophisticated encryption techniques complicate efforts to trace IP addresses, posing challenges to monitoring and combating criminal activities, particularly identifying leads, gathering evidence, and constructing criminal cases.[47]

- **The Privacy Paradox**

Balancing privacy concerns with combating crimes and terrorism on the dark web remains a massive challenge. Some internet companies refuse to cooperate with law enforcement, citing privacy concerns. Maintaining a balance between dark web crime and privacy protection has become a controversial subject for law enforcement.[48]

- **Weaknesses in Law Enforcement**

Dark web users utilise peer-to-peer networks and file-sharing services, which make it difficult for law enforcement to ascertain identities and activities. Some dark web platforms like Tor redirect their operations overseas, leveraging internet support while maintaining high concealment. Technical constraints and a lack of operational mandate further hinder monitoring efforts.[49]

The *Atmanirbhar* (Self-Reliant) Mission

In India, the technology industry can contribute to the fulfilment of the country's *atmanirbhar* mission by making radical changes in its infrastructure and legislation to counter terrorism on the dark web. The most crucial step that India can take as a Global South leader is to facilitate an agreement among its partners and allies about a standard definition of what constitutes a cyberattack, cyber threat, or terrorism on the dark web and eventually formulate guidelines and legal regulation that can be adopted at a bilateral and multilateral forum. India's IT industry needs to invest in funding and promoting indigenous and self-reliant cloud storage infrastructure that can ensure data safety.

India could also work on an Integrated National Cyber Doctrine that aims to address the issues of dark web. This could provide defence systems with an understanding of what constitutes an attack on the nation and what the protocol could be in warlike situations. Industry experts can create a Critical Information Infrastructure (CII) and secure it with quantum computing, developing high-grade encryption to shield the infrastructure.

Cloud Storage: Bolstering Security and Combating Crime

The integration of cloud storage solutions has revolutionised data security and law enforcement capabilities, particularly in combating criminal activities, including terrorism, on the dark web. Cloud storage platforms offer robust encryption and security measures, fortifying sensitive data against unauthorised access. Moreover, these platforms enable authorities to monitor and surveil activities on the dark web more effectively by leveraging real-time collaboration and intelligence-sharing among law-enforcement agencies and international partners. Through advanced forensic analysis and evidence-collection tools, cloud storage facilitates the reconstruction of digital trails and the gathering of evidence against perpetrators. Additionally, compliance monitoring and regulatory oversight features ensure adherence to data protection laws, preventing data misuse by criminal entities and enhancing public safety. Therefore, adopting cloud storage technology not only safeguards data but also empowers law enforcement agencies to disrupt terrorist networks and apprehend individuals involved in illicit activities, thus contributing to global security efforts.

Utilising Technology to Counter the Influence of the Dark Web

Leveraging technological advancements is crucial for combating the threat of the dark web. It involves exploring applications of the dark web while developing specialised monitoring technologies tailored for dark web activities. For example, the Defence Advanced Research Projects Agency (DARPA) has developed a set of tools called Memex to scan the dark web and find information that is not easily accessible on the surface web.[50] The UK's National Crime Agency (NCA) pioneered decoy websites mimicking DDoS-for-hire services, aiding in identifying and tracking cyber criminals.[51] Additionally, prioritising training initiatives equips law enforcement personnel with requisite digital evidence-handling skills, ensuring adeptness in tackling evolving cyber threats.

Bolstering Investigation and Enforcement Efforts

The fight against crime on the dark web requires dedicated organisations and institutions at various levels of government. Dismantling criminal syndicates associated with the dark web should be a primary focus, necessitating the integration of efforts into unique campaigns against organised crime. Social media platforms and law enforcement agencies can work as a team to collate and analyse material from radical groups to understand patterns and channel the resources to counter them.

Moreover, security agencies should be given a mandate to carry out operations on the dark web rather than acting as observers, which would also utilise capital and human resources more efficiently. The government could establish a dedicated regulatory body under the existing law enforcement agency to monitor, scrutinise, and audit the practices of companies involved with the internet and social media to ensure that they function as per the laws of the land. In India, organisations like the National Technical Research Organisation (NTRO) can collaborate with telecommunication organisations to monitor all Tor users and those who download an attack over Tor, which can defuse the work of terrorist organisations. For example, the US National Security Agency (NSA), through its intelligence directorate, is monitoring vast amounts of data as well as automatically taking fingerprints of all those who are downloading Tor.[52]

Reinventing International Collaboration

Given the transnational nature of dark web crimes, bolstering international cooperation is imperative. Establishing bilateral and multilateral agreements with mutually agreed guidelines and definitions of cyberterrorism is paramount to addressing the challenges of the dark web. The Tallinn Manual[53] could be used as a foundation for developing a revised and mutually agreed upon manual. Concurrently, forming regional alliances similar to the Five Eyes Intelligence Alliance,[54] with a specific mandate to counter terrorist activities on the dark web, is essential for focused efforts. Supported by robust legal frameworks and strategic investments, these proactive measures can stay ahead of cyber adversaries' rapidly evolving tactics and mitigate the significant risks of the dark web ecosystem.

Digital Literacy at All Levels

Enhancing digital literacy is crucial for combating dark web-related terror attacks. Through digital literacy initiatives, individuals can better understand the dark web, enabling them to recognise its risks and identify early-stage warnings of terrorist activities. Moreover, digital literacy promotes cybersecurity awareness, teaching individuals to safeguard against dark web threats and use online platforms responsibly. Schools, colleges, universities, start-ups, and small and medium businesses should be targeted.

Countering Early Signs of a Threat

The owners of software and AI tools should be urged to implement controlled measures for web searches, information dissemination, and the handling of sensitive data, particularly on platforms like Gemini and ChatGPT. For example, Tech Against Terrorism has collaborated with Facebook to carry out such initiatives.[55] It is imperative to recognise that countering potential threats demands a comprehensive strategy. Individuals and organisations need to remain vigilant, verifying email sources and employing VPNs for added security. Regular testing and patching of IT systems, including vulnerability scanning and penetration testing, are also critical. Additionally, software should be coded to flag hostile users in real time. Furthermore, frequent cybersecurity risk assessments are necessary to ensure robust defences against evolving cyber threats. Proactively leveraging cyber threat intelligence aids in identifying potential attacks and effectively mitigating known risks, strengthening the overall cybersecurity posture.

Conclusion

The dark web has added another dimension to terrorism, presenting massive challenges for security agencies worldwide.

Efforts to monitor and trace dark web activities are made complicated by sophisticated encryption techniques, decentralised networks, and the widespread use of cryptocurrencies, which provide a cloak of anonymity for illicit transactions. Moreover, the rapid evolution of technology and the increasing accessibility of the dark web to a broader range of users pose ongoing challenges for law enforcement and regulatory bodies.

Addressing these challenges requires a multifaceted approach. Technological advancements, such as specialised monitoring tools and semantic analysis algorithms, can enhance the capabilities of security agencies' to detect and disrupt terrorist activities on the dark web. Strengthening governance mechanisms to hold internet-connected entities accountable for facilitating dark web activities is essential for disrupting the ecosystem that sustains terrorist operations.

Furthermore, concerted efforts in investigation and enforcement, both at the national and international levels, are crucial to dismantling criminal syndicates operating on the dark web and prosecuting those involved in terrorist activities. Collaboration between governments, law enforcement agencies, and technology companies is essential to developing effective strategies and sharing intelligence to combat the illicit use of the dark web.

In essence, combatting the connection between terrorism and the dark web requires a thorough and synchronised strategy that utilises technological advancements, reinforces regulatory structures, bolsters enforcement capacities, and encourages global cooperation. By tackling these obstacles together, the international community can reduce the risks posed by terrorist groups in the dark web, thus protecting national security and fostering global stability.

Soumya Awasthi *is a freelance analyst working on issues of tech-driven terrorism, counterterrorism, and de-radicalisation.*

Endnotes

1 Aaron Holmes, "The Dark Web Turns 20 this Month," *Business Insider*, March 22, 2020, https://www.businessinsider.com/dark-web-changed-the-world-black-markets-arab-spring-2020-3?IR=T.

2 Dark Owl, "Dark Web Groups Turn their Attention to Israel and Hamas," October 10, 2023, https://www.darkowl.com/blog-content/dark-web-groups-turn-their-attention-to-israel-and-hamas/#:~:text=The%20world%20was%20shocked%20by,and%20dark%20 web%20adjacent%20sites.

3 Juan Hernandez, "Dark Web Statistics and Trends for 2024," Prey Project, https://preyproject.com/blog/dark-web-statistics-trends.

4 Tor Metrics, "Users," https://metrics.torproject.org/userstats-relay-country.html?start=2023-01-01&end=2023-12-31&country=all&events=off

5 Hernandez, "Dark Web Statistics and Trends for 2024"

6 Hernandez, "Dark Web Statistics and Trends for 2024"

7 Statista, "Selling Price of Illegal Digital Products on the Darknet 2023," September 19, 2023, https://www.statista.com/statistics/1275187/selling-price-illegal-digital-products-dark-web/

8 Statista Research Department, "Selling Price of Malware and DDoS Attack Services on the Darknet 2023," 2023, https://www.statista.com/statistics/1350155/selling-price-malware-ddos-attacks-dark-web/.

9 ID Agent, "Who are Today's Dark Web Users?" March 23, 2023, https://www.idagent.com/blog/who-are-todays-dark-web-users/

10 Raghu Raman et al., "Darkweb Research: Past, Present, and Future Trends and Mapping to Sustainable Development Goals," *Heliyon* 9, no. 11 (2023): E22269, https://doi.org/10.1016/j.heliyon.2023.e22269

11 S. Every Palmer, Cunningham (ed), "The Christchurch Mosque Shooting, the Media, and Subsequent Gun Control Reform in New Zealand; A Descriptive Analysis," *Psychiatr Psychol Law* 28, no. 2 (2020): 274-285, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8547820/

12 *The 'Dark Web' and Jihad: A Preliminary Review of Jihadis' Perspective on the Underside of the World Wide Web*, MEMRI JTTM, May 21, 2014, https://www.memri.org/jttm/dark-web-and-jihad-preliminary-review-jihadis-perspective-underside-world-wide-web

13 Gabriel Weimann, "Terrorist Migration to the Dark Web," *Perspectives on Terrorism* 10, no. 3 (2016): 40-44, http://www.jstor.org/stable/26297596

14 Evan F. Kohlmann, "Al Qaida's "MySpace": Terrorist Recruitment on the Internet," *CTC Sentinel* 1, no. 2 (2008): 1-3, https://ctc.westpoint.edu/al-qaidas-myspace-terrorist-recruitment-on-the-internet/.

15 Eric Liu, "Al Qaeda Electronic: A Sleeping Dog," *Critical Threats*, December 2015, https://www.criticalthreats.org/wp-content/uploads/2016/07/Al_Qaeda_Electronic-1.pdf

Endnotes

16 Heral Doornbos and Jenan Moussa, "Found: The Islamic State's Terror Laptop of Doom," *Foreign Policy*, August 28, 2014, https://foreignpolicy.com/2014/08/28/found-the-islamic-states-terror-laptop-of-doom/

17 Jasper Hamill, "ISIS Encyclopaedia of Terror: The Secrets Behind Islamic State's 'Information Jihad' on the West Revealed," *Mirror*, April 27, 2015, https://www.mirror.co.uk/news/technology-science/technology/isis-encyclopedia-terror-secrets-behind-5528461

18 M. Sageman, *Leaderless Jihad* (Philadelphia: University of Pennsylvania Press, 2008).

19 Gabriel Weimann, "Going Dark: Terrorism on the Dark Web," *Studies in Conflict & Terrorism* 39, no. 3 (2016): 195-206, https://doi.org/10.1080/1057610X.2015.1119546.

20 Margaret Coker, Sam Schechner, and Alexis Flynn, "How Islamic State Teaches Tech Savvy to Evade Detection," *The Wall Street Journal*, November 16, 2015, https://www.wsj.com/articles/islamic-state-teaches-tech-savvy-1447720824

21 Counter Extremism Project, *Terrorism on Telegram*, *February 2024*, https://www.counterextremism.com/sites/default/files/2024-02/Terrorists%20on%20Telegram_022024.pdf

22 Coker, Schechner, and Flynn, "How Islamic State Teaches Tech Savvy to Evade Detection"

23 Coker, Schechner, and Flynn, "How Islamic State Teaches Tech Savvy to Evade Detection"

24 Coker, Schechner, and Flynn, "How Islamic State Teaches Tech Savvy to Evade Detection"

25 EUROPOL Review, *Online Jihadist Propaganda*, European Union Agency for Law Enforcement Cooperation, 2022, https://www.europol.europa.eu/cms/sites/default/files/documents/Online_jihadist_propaganda_2022_in_review.pdf

26 John R. Vacca, ed., *Online Terrorist Propaganda, Recruitment, and Radicalisation* (New York: Taylor & Francis, 2019).

27 E. Dilipraj, "Terror in the Deep and Dark Web," *Air Power Journal* 9, no. 3 (2014): 121-140, https://capsindia.org/wp-content/uploads/2022/09/E-Dilipraj.pdf

28 The Department of the Treasury, *2024 National Terrorist Financing Risk Assessment, Washington DC,* 2024, https://home.treasury.gov/system/files/136/2024-National-Terrorist-Financing-Risk-Assessment.pdf

29 Anurag, "ISIS Mouthpiece Calls for Donations in Monero (XMR)," *OpIndia*, October 6, 2023, https://www.opindia.com/2023/10/isis-magazine-jihad-monero-terrorist-activities-cryptocurrenc-india-nirmala-sitharaman/

30 Liana W. Rosen et al., *Terrorist Financing: Hamas and Cryptocurrency Fundraising,* Washington DC, Congressional Research Service, 2023, https://crsreports.congress.gov/product/pdf/IF/IF12537#:~:text=In%202021%2C%20the%20U.S.%20cryptocurrency,groups%20between%202021%20and%202023

31 Lasha Giorgidze and James K. Wither, “Horror or Hype: The Challenge of Chemical, Biological, Radiological, and Nuclear Terrorism,” *Occasional Paper Number 31*, George Marshall European Center for Security Studies, December 2019, https://www.marshallcenter.org/en/publications/occasional-papers/horror-or-hype-challenge-chemical-biological-radiological-and-nuclear-terrorism-0#:~:text=Most%20likely%2C%20they%20will%20focus,of%20components%20for%20these%20devices

32 Giacomo Persi Paoli et al., “Behind The Curtain: Illicit Trade of Firearms, Explosives and Ammunition on the Dark Web,” RAND, 2017, https://www.rand.org/content/dam/rand/pubs/research_reports/RR2000/RR2091/RAND_RR2091.pdf

33 United Nations, *International Narcotics Control Board Report 2023*, Vienna, International Narcotics Control Board, March 2024, https://www.incb.org/documents/Publications/AnnualReports/AR2023/Annual_Report/E_INCB_2023_1_eng.pdf

34 Amy Goodman, “Lavender & Where’s Daddy: How Israel Used AI to form Kill Lists & Bomb Palestinians in their Homes”, *Democracy Now*, April 05, 2024, https://www.democracynow.org/2024/4/5/israel_ai

35 Giacomo Persi Paoli, 2018, “The Trade in Small Arms and Light Weapons on the Dark Web,” *Occasional Paper No. 32*, United Nations Office of Disarmament Affairs, 2018, https://front.un-arm.org/wp-content/uploads/2018/10/occasional-paper-32.pdf

36 United Nations Security Council Counter-Terrorism Committee, *Delhi Declaration 2022*, United Nations, 2022, https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2022/Dec/english_pocket_sized_delhi_declaration.final_.pdf

37 United Nations Office on Drugs and Crime, *World Drug Reports 2023*: *Use of Dark Web and Social Media for Drug Supply*, United Nations, 2023, https://www.unodc.org/res/WDR-2023/WDR23_B3_CH7_darkweb.pdf

38 United Nations, *Model United Nations of the University of Chicago*, United Nations Human Rights Council, 2023, https://munuc.org/wp-content/uploads/2022/12/UNHRC.pdf

39 United Nations International Children’s Emergency Fund, United Nations, 2018, https://www.unicef.org/press-releases/children-account-nearly-one-third-identified-trafficking-victims-globally

40 Financial Action Task Force, *Virtual Currencies Key Definitions and Potential AML/CFT Risks*, 2014, https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf

41 Daniel Moore and Thomas Rid, “Cryptopolitik and the Darknet,” *Survival* 58, no. 1 (2016): 7-38, https://www.tandfonline.com/doi/epdf/10.1080/00396338.2016.1142085?needAccess=true

42 Anupriya Chatterjee, “Why are Cybercrime Convictions Low in India? ‘Weak Forensic,

Endnotes

Dark Net & Cross-Border Attacks," *The Print*, December 21, 2022, https://theprint.in/tech/why-are-cybercrime-convictions-low-in-india-weak-forensics-dark-net-cross-border-attacks/1273191/

[43] INTERPOL, *Global Operation Sees a Rise in Fake Medical Products Related to COVID-19*, 2020, https://www.interpol.int/en/News-and-Events/News/2020/Global-operation-sees-a-rise-in-fake-medical-products-related-to-COVID-19

[44] Cedric Nabe, "Impact of COVID-19 on Cybersecurity," 2022, https://www2.deloitte.com/ch/en/pages/risk/articles/impact-covid-cybersecurity.html

[45] Jeremy Douglas and Neil J. Walsh, "Darknet Cybercrime Threats to Southeast Asia," United Nations Office on Drugs and Crime, Vienna, 2020 https://www.unodc.org/documents/Cybercrime/tools-and-resources/darknet_cybercrime_threats_to_southeast_asia_english_version.pdf

[46] Nabe, "Impact of COVID-19 on Cybersecurity"

[47] J. Besenyo and A. Gulyas, "The Effect of the Dark Web on the Security," *Journal of Security and Sustainability* 11, no. 1 (2021): 103-121, https://doi.org/10.47459/jssi.2021.11.7.

[48] H. Alghamdi and A. Selamat, "Techniques to Detect Terrorists/Extremists on the Dark Web: A Review," *Data Technologies and Applications* 56 no. 4 (2022): 461-482, https://voxpol.eu/file/techniques-to-detect-terrorists-extremists-on-the-dark-web-a-review/

[49] Weimann, "Terrorist Migration to the Dark Web"

[50] Pierluigi Paganini, "Memex- The New Search Tool to Dig also in the Deep Web," *Security Affairs*, February 10, 2015, https://securityaffairs.com/33336/cyber-crime/darpa-memex-deep-web.html

[51] Graham Cluley, "UK Police Reveal they are Running Fake DDoS-for-Hire Sites to Collect Details on Cybercriminals," Bitdefender, March 27, 2023, https://www.bitdefender.com/blog/hotforsecurity/uk-police-reveal-they-are-running-fake-ddos-for-hire-sites-to-collect-details-on-cybercriminals/

[52] Patrick Tucker, "If You Do This, the NSA Will Spy on You," Defense One, July 7, 2014, https://www.defenseone.com/technology/2014/07/if-you-do-nsa-will-spy-you/88054/

[53] Michael N. Schmitt, ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare* (United Kingdom: Cambridge University Press, 2013).

[54] Katherine Haan, "What is the Five Eyes Alliance?" *Forbes Advisor*, June 4, 2024, https://www.forbes.com/advisor/business/what-is-five-eyes/

[55] "Disrupting Terrorist Activity Online," Tech Against Terrorism, https://techagainstterrorism.org/about

Images used in this paper are from Getty Images/Busà Photography.

ORF OBSERVER RESEARCH FOUNDATION

Ideas . Forums . Leadership . Impact

20, Rouse Avenue Institutional Area,
New Delhi - 110 002, INDIA
Ph. : +91-11-35332000. **Fax :** +91-11-35332005
E-mail: contactus@orfonline.org
Website: www.orfonline.org