Journal of Engineering, Science and Technological Trends (JESTT)
Vol. 1, Issue 2, August 2024
DOI: https://doi.org/10.48112/jestt.v1i2c.4

Review

Review of Various Aspects of Digital Violence

Jamil Afzal[1*], Chen Yongmei[1], Adeena Fatima[2] and Anam Noor[3]

[1]Southwest University of Political Science and Law, Chongqing, China

[2]Department of Physics, University of Management & Technology, Lahore, Pakistan

[3]Department of Computer Science, University of Agriculture Faisalabad, Pakistan

* Corresponding Email: sirjamilafzal@gmail.com (J. Afzal)

Received: 03 July 2024 / Revised: 15 August 2024 / Accepted: 16 August 2024 / Published Online: 31 August 2024

ABSTRACT

This study aims to elaborate on different aspects of digital violence; several key trends and challenges are shaping the landscape of digital law. With the rise in data breaches and the misuse of personal information, governments are likely to implement more stringent data protection regulations. Innovations such as blockchain for secure data storage and AI for compliance monitoring and enforcement are expected to play significant roles. As cyber threats become more sophisticated and cross-border in nature, international cooperation and harmonization of cyber security laws will be crucial. Determining liability for cyber incidents will be an expanding area, including the responsibility of companies to protect data and the extent of government oversight.

Keywords*:* Cyber Terrorism; Digital Law; Digital Terrorism; Digital Violence

1. Introduction

Nowadays, a computer and the World Wide Web are an essential part of daily life and have become one of the biggest sites for the transmission of files, online commerce, and entertainment[1]. The Internet has advanced significantly since the late 1960s when it was first established as a network of Wide-Area Networks (WAN), Metropolitan Area Networks (MANs), and Local Area Networks (LANs) connected by various architectures. Routers, Switches, and other equipment all have various safety protocols and structures, and the degrees of safety also vary widely. In summary, the Internet has evolved from a small-centralized to a widely spread yet autonomous framework [2]. Nevertheless, any discovery or inquiry has advantages and disadvantages depending on how its users behave. Comparably, the information-rich portion of the Internet called the "Dark Net" is an encrypted haven for hackers and other cybercriminals that is unobserved and unaffected by law enforcement. It can only be accessible through specialized software, browsers, and protocols. Criminals and scammers frequently use such protected environments for their illicit activities, such as exchanging dangerous ideas, taking over or hacking websites, stealing private data like bank account information and related details, and taking advantage of weak points in cameras on any internet-connected device, such as a computer, to introduce malware, disrupt regular operations, and alter stored data to profit [3].

Cybercriminals thus operate in the background to damage the gadget, which results in the victim user losing important data[4]. The skill and expertise of these crooks in disguising or sheathing their malware codes to safely circumvent the latest protection measures have coincided with technological advancements [5]. Ransomware is a type of computer malware that is generated. Since multi-phase ransomware is easily accessible on the dark web in several thousand-dollar bundles, spreading the virus via it doesn't require a high level of expertise. Moreover, there are organized and well-funded gangs that operate various encrypted dark net zones and are responsible for the development of ransomware. Because the criminals constantly incorporate new technological advancements into their ransomware and employ them more quickly than others, their ransomware is incredibly successful. For example, these criminals can trick anyone by creating an authentic-looking fake website or application, marketing, or email using the well-known phenomena of social engineering and disguised [6].

This article provides a review of different aspects of digital violence. Determining liability for cyber incidents will be an expanding area, including the responsibility of companies to protect data and the extent of government oversight. The shift in terrorist tactics from conventional methods to more intricate, technology-driven schemes necessitates a multifaceted, intelligent response that incorporates social, technological, and international measures. This study has great significance; terrorist groups often use social media, forums, and other online platforms to recruit new members and spread their ideology. They can target vulnerable individuals and communities, using sophisticated propaganda to radicalize them. Terrorist organizations use encrypted messaging apps, emails, and other digital communication tools to coordinate their activities and plan attacks while avoiding detection by authorities.

2. Evolution of Ransomware

Primitive format restricts the purpose of virus design to identify a computer's weaknesses. Malware, to put it simply, is any nefarious software that can hack, steal, and spy on sensitive data while also interfering with the system's regular operations. Malware as a whole comprises, as shown in Figure 1, viruses, Trojan horses, spyware, ransomware, logic bombs, adware, rootkits, and many more. Brain A is the first malware designed to expose vulnerabilities on a PC. It was created by Pakistani developers Bait and Amjad, and it starts by infecting a floppy diskette's boot sections [7]. Subsequently, the infection method evolved to include erasing, altering, or shredding PC File Tables.

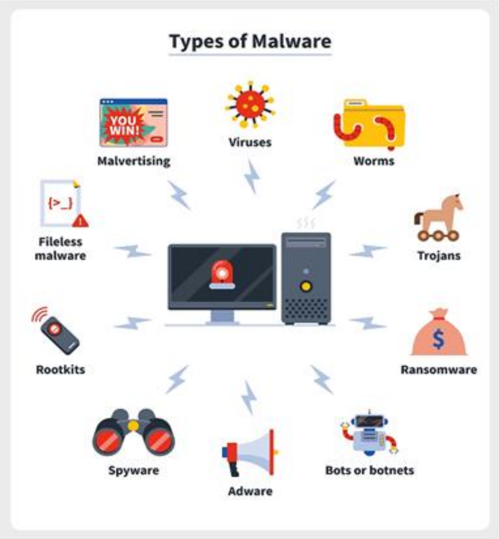

Figure 1: *Various types of Malware in Ransomware [7]*

Malware gradually began to employ polymorphism and mutation to increase its resistance to built-in security mechanisms. Years before the Internet became commercially available, in the late 1980s or early 1990s. In 1971, the first virus ever discovered was called Creeper and was created by Bob Thomas and used in the BBN Technologies Lab. After Creeper was discovered to be a worm rather than a virus, Reaper, an antivirus program, was created to prevent it from transmitting or showing messages going forward [8]. After starting with reproduction, viruses rewrote boot sectors, destroyed the File Allocation Table (FAT), and then infected the Master Boot Record (MBR). To cause further problems for the Windows operating system, the virus first infects Portable Executable (PE) files and then gains the power to kill itself. Advanced polymorphic virus variants can successfully elude antivirus software's auto-detection mechanism. Thousands of viruses infiltrated different systems throughout the world throughout this journey, but stealth viruses are more common these days [9].

Worms: To take advantage of any weakness on the device linked to the IP address, worms have an inbuilt scanning algorithm that examines the network address depicted in Figure 2. Worms also possess a greater ability to defend against security solutions. In 1988, the first worm, dubbed "Morris," appeared by mistake swamped the network with load and caused the Internet to crash [10].

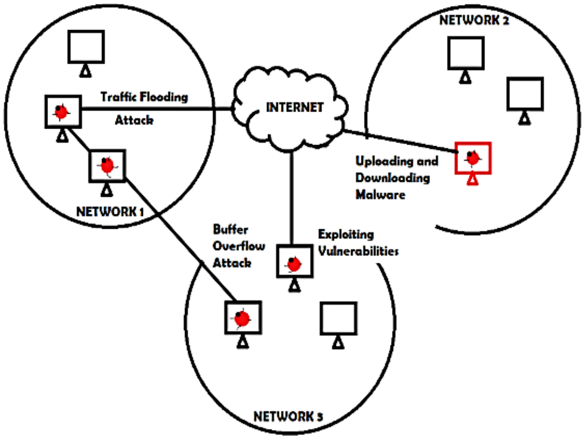

Figure 2: *Depiction of Network of worm spread in computers [7]*

Both user-mode and kernel-based mode rootkits share the same goal of altering the operating system by seizing system data and remaining undetected as demonstrated in Figure 3. Another ability of rootkits is to build a botnet made up exclusively of compromised computers, and then use that botnet to propagate other infections.

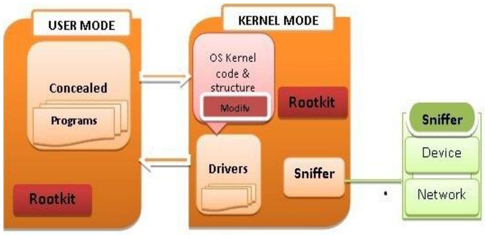

Figure 3: *ROOTKIT illustration Based On User& kernel mode [11]*

Mebroot is one such rootkit that searches for browser security holes to propagate malware. It even designates monitoring instruments that converse with hackers to pilfer any kind of victim. Its ability to return error codes or faults to the developer is an improvement that encourages debugging and fixing[12]. Trojans are a kind of malware that poses as legitimate programs, files, or apps to trick people into downloading it and unintentionally giving it access to their machines. Once installed, a trojan can carry out its intended function, which could be to corrupt, interfere with, steal from, or do other malicious things to your data or network [13]. Trojan malware, sometimes referred to as a Trojan horse or Trojan horse virus, is frequently distributed through direct messages; website downloads, and email attachments. Like viruses, they too need to be activated by the user. The distinction between trojans and malware viruses is that the former are not host-dependent, while the latter are. Unlike viruses, Trojans are unable to self-replicate. Malicious adverts that pose as trustworthy ones on websites are comparable to adware. By hacking the website, the adware may have been introduced. When an enticing advertisement is clicked, dangerous payload-containing adware is launched, causing the installation of adware from the internet or software that has been downloaded. Adware typically interferes with a computer's operation by launching a series of windows that serve as an injector for other malware [14].

Malware like Stuxnet [15], and Flame[16] are in circulation in that era. Malicious tools written in high-level programming languages like OOC, C++, and Lua are included in this malware, which also compiles with genuine programs like Microsoft Visual Studio.

The globe suffered a severe blow in the final month of 1989 when the first ransomware attack infiltrated computer systems with a floppy diskette-based malicious program. The use of such technology in recent complex malware (from the 21st century) allows them to purposefully create generations of damage, disrupt system functionality, and steal reliable data and information. Some of them are shown in Figures 4 & 5.

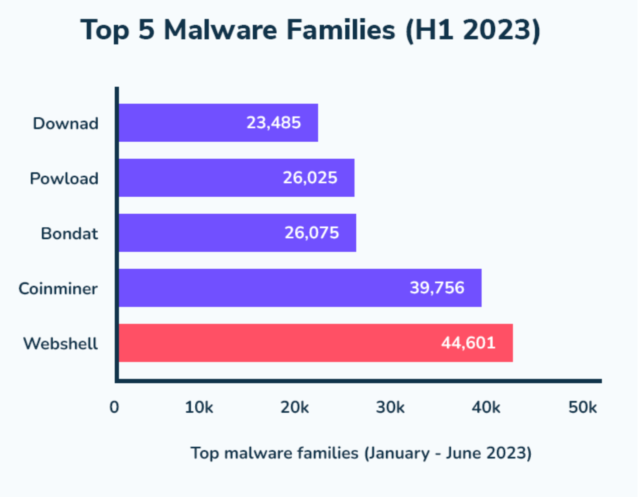

Figure 4: *Top 5 Malware Statistics in specific times span*

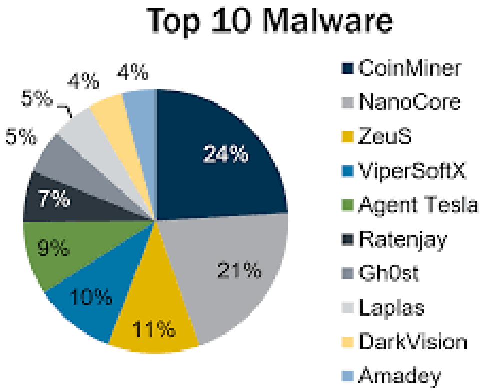

Figure 5: *Top listed Detection of Malware types in the 21st century era [17]*

3. Key Aspects of Digital Terrorism

The way terrorist groups have adapted to the digital era in light of the expanding cybertechnological milieu demonstrates a substantial and complex challenge. Terrorist organizations have changed and evolved as a result of the rapid progress of cybertechnologies, taking advantage of the opportunities presented by the internet to expand their influence, capability to operate, and impact. In the past, terrorist attacks have typically involved physical force against important targets or monuments to spread fear and further political goals. Communication's potential reach and effect were constrained by its reliance on traditional channels like print media and broadcast networks. Intelligence collecting, physical network disruption, and international collaboration were the main focuses of counterterrorism tactics to obstruct assaults and destroy organizational frameworks. Nonetheless, the advent and spread of digital technologies have drastically changed the environment in which terrorism operates. Recent Research has shown how terrorist operations in cyberspace are becoming more sophisticated and impactful, indicating a significant shift away from traditional forms of terrorism and towards more sophisticated, based on technology tactics.

For example, Kim & Yun [18] have emphasized how psychological warfare is conducted in cyberspace, where terrorist organizations actively participate in propagandistic recruiting, the rationale of acts of violence, and their spread. Buresh [19], who affirms the existence and development of digital terrorism and highlights its unique characteristics from traditional terrorism, lends additional credence to this.

Furthermore, the influence of cyberterrorism on stock market valuations, as demonstrated by Smith et al., [20] highlights the economic and societal risks associated with these terrorist operations of the digital age. The internet's ability to break through geographical boundaries, for example, enables terrorist organizations to get by censors in traditional media and spread false information to a worldwide audience directly, use social media to spread the word, encourage participation, and cultivate online terrorist networks. Digital capabilities also make it possible to produce and distribute excellent multimedia propaganda that is targeted at certain populations. A refined and convincing story is presented in video productions, interactive content, and online publications, humanizing offenders and defending violent acts.

Recognizing the quick development and accessibility of digital technology, the UN has expressed concerns over the possible exploitation of these tools by terrorist organizations. This includes worries about how the internet is being used for terrorist employment, disinformation, and organizing, as well as the abuse of increasingly sophisticated technology like cyber tools, robotics, and artificial intelligence to launch attacks or improve their capabilities. One such new and developing concern is the use of 3D printing technology in terrorism. One new facet of terrorism in the digital era is the capacity to create weapons with 3D printers, as demonstrated by events like the Halle attack, which involved handmade firearms [18]. This technology circumvents conventional approaches to arms control and acquisition, which presents serious difficulties for law enforcement and counterterrorism initiatives.

4. Historical view of Digital Terrorism

There is no general agreement on the definition of terrorism, making it a difficult topic. While historically it involved the use of force to instil fear and accomplish political objectives, there have been many differences in how it has been applied. From its original connotation of state aggression, the phrase has come to refer to non-state entities that attack governments or civilian populations. The transition from physical to digital terrorism signifies a dramatic change in the strategies and tactics used by terrorist organizations, which are distinguished by the growing use of technology to support terrorist actions, especially internet-based systems and digital communication tools Important historical events can be used to illustrate this shift from conventional techniques to the use of cybertechnologies. Each of these events demonstrated the growing influence of cybertechnologies in enabling these assaults, in addition to signalling a change in the methods and techniques used by terrorist organizations [21]. Al-Qaeda's 9/11 assaults signalled a paradigm change in terrorism, particularly concerning the use of cyber technology. This incident launched a new era in terrorist tactics and demonstrated the capability of Al-Qaeda. Following 9/11, terrorist organizations, such as Al-Qaeda, started utilizing the internet extensively for propaganda, which was a big departure from earlier techniques. The widespread dissemination of ideas was made possible by the internet's global reach, which included the sharing of video messages from influential figures like Osama bin Laden on a variety of online venues [22]. As terrorist groups use websites, social media, and online forums, the internet has also become essential for radicalization and recruiting. These online communities provided a safe place for community development and indoctrination while maintaining anonymity, which ultimately led to radicalization.

4.1. Technology-Aided Terrorism

The Mumbai attacks of 2008, a pivotal moment in Terrorists used GPS and satellite phones for communication and navigation during the attacks, making it easier for them to travel from Karachi to Mumbai and stay in touch. This is an example of how terrorism uses cyber technology [23]. This expert use of technology for preparation and execution brought attention to the necessity of reassessing international counterterrorism plans, with a particular emphasis on the function of digital communications and real-time media coverage in such situations. It also emphasized how counterterrorism strategies must change to keep up with new technologies like massive data sets, artificial intelligence, and Blockchain [24]. The terrorists' desire and ability to use technology to improve their operations was demonstrated by the Mumbai attacks.

4.2. New Technologies and Potential Terrorism Threats

New technologies are always changing the terrain of terrorism, offering intricate difficulties and fresh chances for both terrorists and counterterrorism initiatives. The prediction and combating of threats are made more difficult by the diversification of terrorist ideology and the increase of decentralized assaults, which are frequently fueled by internet propaganda shown in Figure 6. Technology's accessibility has reduced barriers to entry and democratized terrorism, as anybody with an internet connection can launch an assault. Disinformation tactics, which make use of emerging media technologies such as AI-driven content and deepfakes, are essential in the recruitment and radicalization of terrorists. There are serious security worries over the possibility of terrorist operations abusing cutting-edge technologies like artificial intelligence (AI), drones, 3D printing, and cloud services for anything from advanced attacks to the spread of disinformation [25].

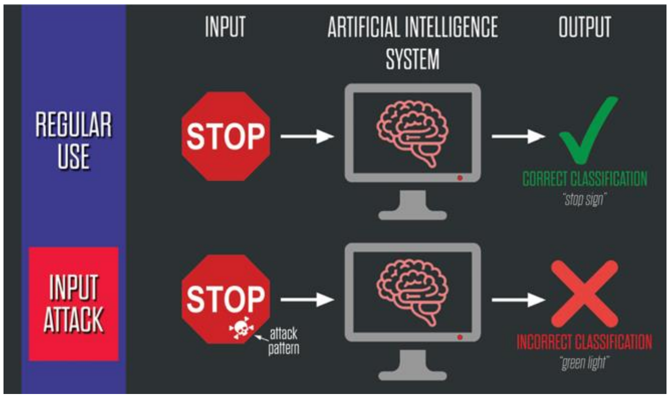

Figure 6: *The AI scam among original and morphing by cutting-edge technologies [25]*

4.3. Role of Artificial Intelligence (AI)

As our reliance on digital infrastructure grows, questions have been raised regarding AI's potential role in cyberterrorism, which includes disseminating false information and breaching important systems [26]. Because AI is so quick and effective at gathering intelligence, more control of the technology is required to stop terrorist organizations from abusing it, as depicted in Figure 7. Terrorists could use sophisticated artificial intelligence (AI) systems, such as those used in automation to map surroundings and identify impediments, to acquire information on particular targets, posing serious concerns to national security [27].

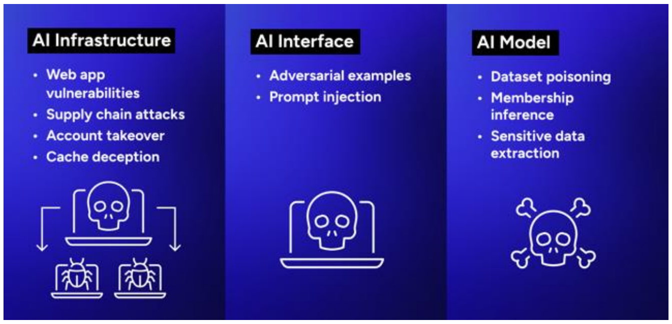

Figure 7: *Various AI Terrorism shown via different Interfaces [27]*

In contrast to the four billion dollars that was spent on research and development in 2020, the worldwide commercial sector has made significant investments in AI technology. Given the substantial cash that terrorist groups have access to, they may have access to these sophisticated artificial intelligence technologies, which are getting cheaper as a result of technology breakthroughs. This hypothetical situation highlights the necessity of strict regulation and oversight of AI technology to stop terrorist groups from using it and to maintain peace and safety around the world [27].

4.4. BROAD FAKES

The development of deep fake technology, which produces incredibly lifelike media utilizing machine learning and artificial intelligence, poses a serious risk to national security, particularly when it comes to terrorism. Deepfakes, which can produce immersive experiences, phone identities, and deceptive narratives, are abundant in this setting. While useful in programs like Google Assistant, techniques like text-to-speech and StyleGAN2 also carry a risk of being used for voice phishing and the creation of false online profiles.

Terrorist organizations in India, have incited violence, especially among young people, by using deepfake images and videos. As AI develops, more sophisticated internet disinformation may become possible. Terrorist organizations might manipulate public opinion and the chain of command by using AI-generated movies to fabricate messages from authorities. This would give them excessive power and emphasize the risks to national security posed by deep fake technology [28].

4.5. Involvement in 3D Printing

Technology development, especially in automated weapons, is changing high-skill tasks from the conflict into more mundane routines. The U.S. Army recognizes the availability of AI software and instructions that can be used with current weaponry systems online, which has resulted in developments like automated gun turrets that are put together using Raspberry Pi processors and 3D printed components. These AI-guided tools can identify and interact with targets on their own, greatly reducing the obstacles that non-state actors must overcome to improve their combat capabilities and creating new difficulties for national security.

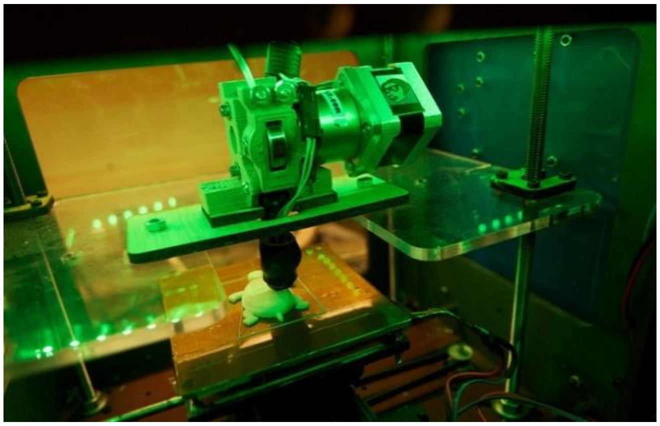

Figure 8: *Plastic Terrorism: 3D printing transformation in the security world [28]*

The contribution of 3D printing to terrorism is especially problematic because of its capacity to create weapons with advanced components quickly as shown in Figure 8. Malicious organizations can now acquire weapons without using conventional means thanks to this technology, which makes regulation and government tracking more difficult. These capabilities aren't just available to state actors; with 3D printing becoming more widely available and affordable, terrorist organizations and private citizens may also be able to use it, confounding security protocols even more. Thus, it's imperative to strike a balance between encouraging technology innovation and limiting its exploitation, necessitating the adoption of both modern technological remedies and 3-D printing regulations [29].

4.6. Could Computing

The effectiveness, availability, and data storage advantages of Cloud storage are offset by distinct difficulties in counterterrorism. Terrorist organizations may use its robust encryption, which is essential for security and privacy, to conceal communications and planning documents from law enforcement, making it difficult to track and access their data. Terrorist organizations use cloud tools to quickly share information spread disinformation and communicate across networks, dodging constant observation and necessitating a significant investment in technology and counterterrorism resources. Terrorist organizations have adapted to the digital sphere in response to stepped-up counterterrorism measures, according to Weimann and Vellante [30], who point out that these groups use anonymous content-sharing services such as Sendvid.com, and Dump. to, and JustPaste.it. These platforms provide a means of eluding conventional surveillance, enabling organizations such as ISIS to continue operating online despite social media shutdowns. The strategic redundancy in content hosting highlights how difficult it is to combat terrorism in the digital era.

4.7. DRONES

Over the past ten years, the use of weaponized drones for assault and combat missions has expanded dramatically as a result of the US successfully deploying unpiloted planes for counterterrorism missions to places like Yemen, Somalia, and Pakistan, demonstrating the advantages of lower mortality and labour costs These benefits have drawn the attention of terrorist organizations in addition to increasing the acceptance of drone technology in combat. These groups are shifting away from more conventional techniques like suicide bombs and towards the use of drones for more effective, low-risk bombing attacks. With this change, they can cause significant harm with less danger to themselves. Drone technology has advanced significantly in recent years, particularly with the addition of artificial intelligence. Because AI-driven drones are capable of performing tasks autonomously, terrorists will be able to carry out intricate, large-scale strikes effectively and quietly [31].

5. Social Context and Hyper Attacks

Terrorists can thrive on social media platforms because of their widespread accessibility and worldwide reach to groups and rebel factions to disseminate their beliefs. Ineffective content filtering guidelines and a lack of transparency, which let dangerous content stay online, are partially to blame for this spread. Large social media firms have difficulty identifying and limiting "terrorist content," as demonstrated by Facebook's difficulties moderating content based on language and cultural context differences. This problem was particularly noticeable in Myanmar, where inadequate Facebook monitoring allowed violent content to proliferate.

The lack of clarity surrounding policy enforcement on these platforms exacerbates the situation. For example, Meta Platforms, the company that owns Instagram and Facebook During the Russia-Ukraine war, the platform briefly changed its hate speech policy, permitting some posts that would typically be considered violent and in violation of established guidelines. This choice emphasizes the subjectivity of enforcing policies and the possibility of prejudice when it comes to content moderation that supports particular agendas or viewpoints Using DarkSide, Anonymity assaulted companies and religious organizations, causing instability. The group's ransomware attack on the Colonial Pipeline in 2021, which stopped the oil supply on the American East Coast, serves as an example of the numerous and serious effects of these kinds of cyberattacks. These incidents highlight the variety and sophistication with which terrorist organizations use cyberspace and digital platforms, underscoring the need for strong defences and global collaboration in the fight against terrorism in the digital age [32]. Terrorism in the digital era is a new kind of danger that goes beyond direct physical assaults to make use of the interconnection of cyberspace and have a significant socioeconomic impact. The effects of this contemporary terrorism on international relations, public opinion, and stock markets have a major impact on people, groups, and countries.

6. Conclusion

The current study was limited to the review of existing literature; this review of literature clarifies the complex and quickly changing context of violence in the digital era. The shift in violence tactics from conventional methods to more intricate, technology-driven schemes necessitates a multifaceted, intelligent response that incorporates social, technological, and international measures. In light of the study's findings, the public needs to be made aware of the dangers of violence in the digital era. This entails instructing on how to identify and report internet extremist material, recognizing disinformation and deepfakes, and encouraging critical thinking in the digital sphere. Governments, academic institutions, and internet platforms must work together to enable people to recognize and reject extremist messages, therefore lowering the danger of radicalization. International cooperation is also essential because cyberterrorism is a worldwide threat; it covers information exchange, best practices, and technical resources, working together to take down cyberterrorist networks, and creating common guidelines for controlling online areas. Collaborations with digital service providers and IT firms are crucial for controlling and keeping an eye on online content while striking a balance between speech freedom and privacy. Combating the growing threat of digital-age terrorism will require focusing counterterrorism efforts on promoting international cooperation, improving digital literacy, and utilizing cutting-edge technology.

Competing Interests: The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.
Ethical Issues: There are no ethical issues. All data in this paper is publicly available.
Author Contribution Statement: J.A, C.Y, A.F and A.N conceived the idea and designed the research; Analyzed and interpreted the data and wrote the paper.
Funding Statement: This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.
Acknowledgement: The authors are thankful to the editor and reviewers for their valuable suggestions to improve the quality and presentation of the paper. The authors are also thankful to Mian Muhammad Afzal Advocate Lahore High Court, Lahore Pakistan.

References

1. Berners-Lee, T., *Long live the web.* Scientific American, 2010. **303**(6): p. 80-85.
2. Weis, A.H., *Commercialization of the Internet.* Internet Research, 1992. **2**(3): p. 7-16.
3. Jardine, E., S. Cruz, and H. Kissel, *Media coverage of darknet market closures: assessing the impact of coverage on US search and Tor use activity.* Crime, Law and Social Change, 2023. **79**(3): p. 263-289.
4. Yongmei, C. and J. Afzal, *Impact of enactment of ‘the prevention of electronic crimes act, 2016’as legal support in Pakistan.* Academy of Education and Social Sciences Review, 2023. **3**(2): p. 203-212.
5. Popoola, S.I., et al. *Ransomware: Current trend, challenges, and research directions*. in *Proceedings of the World Congress on Engineering and Computer Science*. 2017.
6. Cabaj, K., M. Gregorczyk, and W. Mazurczyk, *Software-defined networking-based crypto ransomware detection using HTTP traffic characteristics.* Computers & Electrical Engineering, 2018. **66**: p. 353-368.
7. Indu, R. and A. Sharma, *Ransomware: A New Era of Digital Terrorism.* Computer, 2018. **1**(02).
8. You, I. and K. Yim. *Malware obfuscation techniques: A brief survey*. in *2010 International conference on broadband, wireless computing, communication and applications*. 2010. IEEE.
9. Pathak, P. and Y.M. Nanded, *A dangerous trend of cybercrime: ransomware growing challenge.* International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), 2016. **5**(2): p. 371-373.
10. Liska, A. and T. Gallo, *Ransomware: Defending against digital extortion*. 2016: " O'Reilly Media, Inc.".
11. Kim, S., et al., *A Brief Survey on Rootkit Techniques in Malicious Codes.* J. Internet Serv. Inf. Secur., 2012. **2**(3/4): p. 134-147.
12. Milošević, N., *History of malware.* arXiv preprint arXiv:1302.5392, 2013.
13. Savage, K., P. Coogan, and H. Lau, *The evolution of ransomware, symantec security response.* Symantec Corporation, Mountain View, CA, 2015.
14. Rajesh, B., Y. Reddy, and B.D.K. Reddy, *A survey paper on malicious computer worms.* International Journal of Advanced Research in Computer Science and Technology, 2015. **3**(2): p. 161-167.
15. Kerr, P.K., J. Rollins, and C.A. Theohary, *The stuxnet computer worm: Harbinger of an emerging warfare capability*. 2010: Congressional Research Service Washington, DC.
16. Zhioua, S. *The middle east under malware attack dissecting cyber weapons*. in *2013 IEEE 33rd International Conference on Distributed Computing Systems Workshops*. 2013. IEEE.
17. Yong Wong, M., et al. *An inside look into the practice of malware analysis*. in *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security*. 2021.
18. Adigwe, C.S., et al., *The evolution of terrorism in the digital age: Investigating the adaptation of terrorist groups to cyber technologies for recruitment, propaganda, and cyberattacks.* Propaganda, and Cyberattacks (February 20, 2024), 2024.
19. Buresh, D.L., *Does digital terrorism really exist.* Journal of Advanced Forensic Sciences, 2020. **1**(1): p. 18.
20. Smith, K.T., et al., *Cyber terrorism cases and stock market valuation effects.* Information & Computer Security, 2023. **31**(4): p. 385-403.
21. Abalaka, A., O. Olaniyi, and O.O. Adebiyi, *Understanding and overcoming the limitations to strategy execution in hotels within the small and medium enterprises sector.* Available at SSRN 4614043, 2023.
22. Oladoyinbo, T.O., et al., *Evaluating and establishing baseline security requirements in cloud computing: an enterprise risk management approach.* Available at SSRN 4612909, 2023.
23. Olaniyi, O., et al., *Harnessing predictive analytics for strategic foresight: a comprehensive review of techniques and applications in transforming raw data to actionable insights.* Available at SSRN 4635189, 2023.
24. Khan, F.A., et al., *AI-Driven Counter-Terrorism: Enhancing Global Security Through Advanced Predictive Analytics.* IEEE Access, 2023. **11**: p. 135864-135879.
25. Giantas, D. and D. Stergiou, *From Terrorism to Cyber-Terrorism: the case of ISIS.* Available at SSRN 3135927, 2018.
26. Afzal, J. and C. Yongmei, *Federal and provincial legislation regarding ‘Right to Information’for good governance in Pakistan.* Discover Global Society, 2023. **1**(1): p. 12.
27. Trifunović, D., *Cybersecurity–virtual space as an area for covert terrorist activities of radical islamists.* Teme-Časopis za Društvene Nauke, 2021. **45**(1): p. 95-109.
28. Olabanji, S.O., et al., *AI for Identity and Access Management (IAM) in the cloud: Exploring the potential of artificial intelligence to improve user authentication, authorization, and access control within cloud-based systems.* Authorization, and Access Control within Cloud-Based Systems (January 25, 2024), 2024.
29. Olaniyi, O., O.O. Olaoye, and O.J. Okunleye, *Effects of Information Governance (IG) on profitability in the Nigerian banking sector.* Asian Journal of Economics, Business and Accounting, 2023. **23**(18): p. 22-35.
30. Weimann, G. and A. Vellante, *The Dead Drops of Online Terrorism.* Perspectives on Terrorism, 2021. **15**(4): p. 39-53.
31. Adigwe, C.S., et al., *Critical analysis of innovative leadership through effective data analytics: Exploring trends in business analysis, finance, marketing, and information technology.* Asian Journal of Economics, Business and Accounting, 2023. **23**(22).
32. Milmo, D., *Google Engineer Warns It Could Lose out to Open-Source Technology in AI Race*. 2023.