International Journal of Applied Science and Engineering
Citation: *IJASE*: **13**(01): 75-89, June 2025
DOI: 10.30954/2322-0465.1.2025.8

REVIEW PAPER

INFORMATION SCIENCE

Emerging Digital Extremism: Analyzing Patterns, Evolving Threats, and Global Security Implications of Cyber Attacks by Extremist Groups

Nahid Reza Shatu[1], Prosannajid Sarkar[2*], Md Asaduzzaman[3] and Anima Barma[4]

[1]*Researcher, National University, Bangladesh*
[2]*Dr. Wazed International Research and Training Institute, Begum Rokeya University Rangpur, Bangladesh*
[3]*Researcher, National University, Bangladesh*
[4]*Government Begum Rokeya College, Rangpur, Bangladesh*

**Corresponding author: drpsarkarwri@gmail.com*

Received: 11 Apr., 2025 **Revised:** 19 May, 2025 **Accepted:** 01 June, 2025

ABSTRACT

The digital age has significantly transformed the operations of extremist groups, enabling them to utilize cyberspace for radicalization, propaganda, recruitment, and cyber warfare. This report analyses the increasing threat of digital extremism, investigating the evolving patterns of cyberattacks, exploited vulnerabilities, and their global consequences. The study utilizes a mixed-methods approach, combining qualitative techniques (thematic and discourse analysis) with quantitative methods (descriptive statistics). Data was obtained from primary sources, including interviews and dark web activity, as well as secondary sources, such as cybersecurity databases and international security periodicals. Ethical considerations, including data protection and bias prevention, were recognized, yet challenges such as data accessibility and the dynamic nature of cyber threats persist. Extremist organizations are increasingly utilizing advanced cyber tactics, including DDoS attacks, ransomware, phishing, website defacement, data breaches, and AI-driven disinformation campaigns. These strategies compromise critical infrastructure, skew public image, and fund illicit activities, posing significant risks to national security, economic stability, and social unity. Significant vulnerabilities, including insufficient cybersecurity protocols, encrypted communication platforms, the dark web, and the misuse of emerging technology such as artificial intelligence and deepfakes, exacerbate the threat. These tools enable radicals to operate with increased anonymity, scale, and influence, resulting in global consequences that extend beyond security to disrupt geopolitical dynamics and erode trust in digital systems. The paper emphasizes the imperative of proactive cybersecurity strategies, AI-enabled threat detection, global intelligence sharing, and cooperation among various stakeholders to mitigate this threat. It advocates for the integration of cybersecurity with counterterrorism efforts, offering practical

How to cite this article: Shatu, N.R., Sarkar, P., Asaduzzaman, Md. and Barma, A. (2025). Emerging Digital Extremism: Analyzing Patterns, Evolving Threats, and Global Security Implications of Cyber Attacks by Extremist Groups. *IJASE.,* **13**(01): 75-89.

Source of Support: None; **Conflict of Interest:** None

advice for legislators, law enforcement, and security professionals. The findings underscore the imperative for robust regulatory frameworks, technological innovation, and global cooperation to address cyber-enabled extremism and safeguard the digital future, thus assuring a secure and resilient digital landscape.

Keywords: Digital Extremism, cyber warfare, Cyber Threats, Radicalization Patterns, Global Security, Cyber Attacks, Dark web

The digital era has profoundly altered societal operations, introducing a novel array of problems to global security. One of the most concerning developments is the emergence of digital extremism—an emerging phenomena in which extremist groups exploit online for radicalisation, recruiting, promotion, and cyber warfare. The Internet, originally a medium for information dissemination, has transformed into a theatre for ideological conflict, with extreme groups increasingly leveraging its extensive reach and anonymity to advance their objectives. In recent years, the techniques utilised by these groups have evolved to be more complex and perilous. Cyber techniques, including Distributed Denial-of-Service (DDoS) attacks, ransomware, phishing schemes, website defacement, and data breaches, have become fundamental elements of their operations. These attacks not only target digital infrastructure but also penetrate the centre of society, compromising national security, destabilising economies, distorting public perception, and engendering turmoil across borders. A potent instrument in this arsenal is the propagation of disinformation and misinformation—either purposeful or inadvertent distribution of incorrect information that can distort public opinion, incite social unrest, and undermine democratic processes. The employment of advanced technologies, including artificial intelligence (AI), machine learning, and deepfakes, by extremists has intensified the threat, allowing them to function with enhanced anonymity, scalability, and efficiency. AI-driven disinformation operations can exacerbate radical ideas, destabilise political environments, and undermine institutional trust, rendering them a formidable instrument for those aiming to manipulate societies internally. These falsehoods, whether disseminated intentionally or inadvertently, exacerbate polarisation and conflict, complicating the differentiation between fact and fiction and eroding public trust in credible information sources.

This study investigates the escalating menace of digital extremism, emphasising the advancing strategies of cyberattacks, the susceptibilities that enable them, and the worldwide ramifications of these acts. It analyses how extremist organisations adjust to swiftly evolving technology, exploiting vulnerabilities in cybersecurity and communication infrastructures to fulfil their aims. The document emphasises the pressing necessity for improved cybersecurity protocols, global intelligence collaboration, and preemptive counterterrorism tactics to alleviate the extensive repercussions of cyber threats, especially with disinformation and misinformation. This study aims to analyse the interplay between digital extremism, disinformation, and cybersecurity to provide essential insights into the magnitude of the problem and suggest practical methods for mitigation. The results underscore the necessity of international collaboration, strong regulatory structures, and continuous technological progress in combating the escalating dangers of cyber-enabled extremism, thus guaranteeing a resilient and safe digital future.

Literature Review

The emergence of digital extremism is intricately connected to the advancement of internet communication

tools that enable the swift propagation of extreme ideology. Extremist organisations utilise encrypted chat applications, social media networks, and the dark web to recruit individuals, spread propaganda, and orchestrate unlawful operations (Conway, 2017; Awan, 2016). Social media platforms' algorithmic amplification of extremist information has intensified the problem, fostering echo chambers that perpetuate radical ideologies (Berger & Morgan, 2015; Weimann, 2016). Radicalisation in the digital age is a multifaceted, multi-stage process shaped by socio-political grievances, psychological susceptibilities, and ideological indoctrination (Gill *et al.* 2017; Ingram, 2017). The availability of extremist content has revolutionised recruitment methods, allowing terrorist organisations to customise their outreach campaigns using user data and behavioural analytics (European Commission, 2021). Research underscores the increasing use of deepfake technology and AI-generated propaganda in extremist recruiting, complicating detection and intervention efforts (Johnson *et al.* 2016; Hussain, 2020). Academics underscore the pressing necessity for strong counter-narratives and digital literacy initiatives to alleviate the effects of online extremism (Braddock & Horgan, 2016; Ebner, 2020). The transition to decentralised platforms and encrypted networks has rendered conventional counterterrorism strategies less successful, requiring adaptive and multidisciplinary approaches to digital security (Perry & Scrivens, 2016; Post, 2019).

Cyber Threat Actors and Their Attack Procedures

Extremist groups have used the digital landscape to employ sophisticated cyber-attack techniques, including website defacement and AI-driven disinformation operations. Prominent cyber threat actors comprise terrorist organisations, ideological hacktivists, and state-sponsored extremist groups (RAND Corporation, 2019; FBI Cyber Division, 2021). These individuals exploit weaknesses in global cybersecurity frameworks, utilising encrypted communication channels and blockchain-based financial transactions to escape law enforcement (Arquilla & Ronfeldt, 2001; Clarke & Knake, 2019). Common cyber-attack methodologies encompass Distributed Denial of Service (DDoS) assaults, phishing tactics, ransomware implementation, and cyber espionage (Schmidt, 2016; NATO Strategic Communications Centre of Excellence, 2020). Recently, extremists have utilised AI-generated misinformation campaigns, employing deepfake videos and bot-driven social media manipulation to influence public opinion and radicalise individuals (Singer & Brooking, 2018; Wojcieszak, 2010). The growing amalgamation of cyber terrorism with conventional terrorist activities has heightened apprehensions regarding the likelihood of hybrid assaults, wherein physical and digital dangers intersect (Denning, 2001; Zech & Kelly, 2015). As cyber threats advance, global security agencies stress the necessity for cooperative threat intelligence-sharing systems to proactively detect and mitigate extremist cyber actions (Byman, 2020; National Counterterrorism Centre, 2022).

Objectives

This study seeks to analyse the swiftly changing domain of digital extremism and its considerable influence on global cybersecurity. The objectives of the study are:

- To discern and examine patterns of cyberattacks.
- To investigate the techniques, objectives, and reasons underlying extremist cyberattacks.

- To examine the function of sophisticated digital instruments and platforms utilised by extremist organisations.
- To analyse the progression of cyber risks presented by extremist organisations.
- To evaluate the impact of misinformation and disinformation on digital extremism.
- To investigate preventive strategies and policy suggestions.

Methodology

This study employs qualitative methodologies to provide a comprehensive understanding of cyber extremism and countermeasures. The research design consists of three key components:

Comparative Case Studies

A systematic analysis of real-world cyber extremist attacks was conducted using secondary data from government reports, cybersecurity threat assessments, intelligence briefings, and security agency publications. This method enabled the identification of patterns, tactics, and vulnerabilities that extremist groups exploit. Key cases were selected based on severity, impact, and relevance to modern cyber extremism trends.

Primary Data Collection

Thirty-five in-depth expert interviews were conducted with cybersecurity professionals, intelligence analysts, policymakers, and digital forensics experts. Participants were selected based on their experience in counterterrorism, digital security, and cybercrime investigations. The interviews provided first-hand insights into emerging cyber threats, response strategies, and policy gaps.

The expert (KII) interview demographics included:

- Cybersecurity Professionals
- Policymakers
- Intelligence Officials
- Digital Forensics Experts
- IT Professionals
- Banking Professionals
- Researchers
- Prosecutors
- Law Enforcement Authorities

To enhance the depth of qualitative findings, a Zoom conference was hosted on March 14, 2025, featuring a multidisciplinary panel of experts from the IT, security, policy, and banking sectors. Discussions centred on technological advancements in extremist activities, the evolving cyber threat landscape, and the role of financial institutions in mitigating risks associated with cyber extremism.

KII Interviews

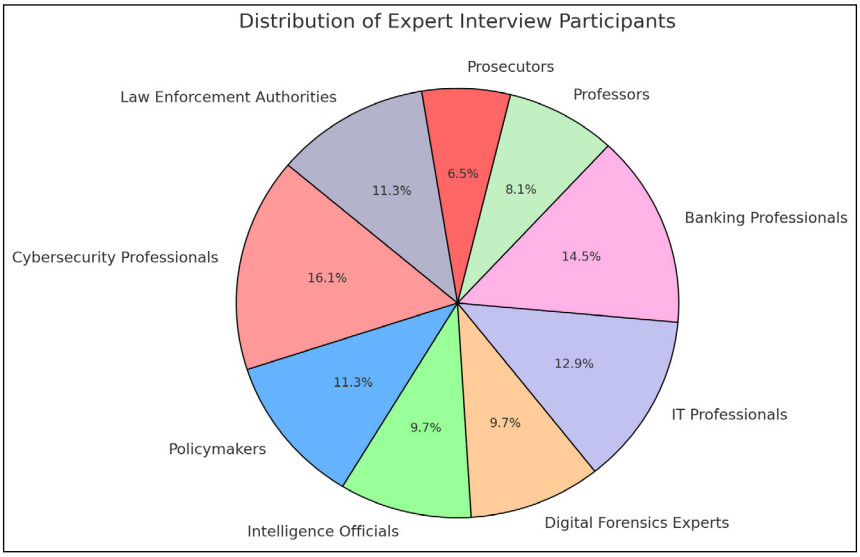

Fig. 1: The diverse professional backgrounds of the interview participants

From fig. 1 was used to represent the diverse Key Informant Interview personal participants, ensuring a well-rounded perspective on cyber extremism and countermeasures. The combination of qualitative insights, quantitative analysis, and visual data representation strengthens the methodological framework, providing a holistic perspective on the evolving landscape of digital extremism and cybersecurity policies.

Data Analysis

Thematic and discourse analysis was applied to expert interviews and conference discussions, identifying recurring themes, emerging cyber threats, and gaps in current cybersecurity frameworks. To ensure data validity and reliability, rigorous triangulation methods were applied, cross-referencing primary interview data with secondary sources. Furthermore, reaching data saturation, where no new insights emerged. Validated the robustness of the qualitative findings. The integration of expert knowledge, real-world case studies, and empirical data analysis enhances the credibility and applicability of the research outcomes.

Research Gap

While previous studies have examined the spread of misinformation and extremist propaganda online, significant gaps remain in understanding the evolving role of AI-driven disinformation, particularly about deepfake technology and algorithmic exploitation. This research identifies the following key gaps:

- Our research has found that digital misinformation (the spread of false information online) and disinformation (deliberately misleading or false information) are among the most common tools employed in digital extremism.
- One key finding of our study is the growing use of AI to spread false information. For example, deepfakes AI-generated videos or images that mimic people are used to mislead and manipulate public opinion.
- In addition to these advanced technologies, extremist groups are also using social media platforms to spread propaganda.

RESULTS AND DISCUSSION

Evolution of Cyber Attacks by Extremist Groups

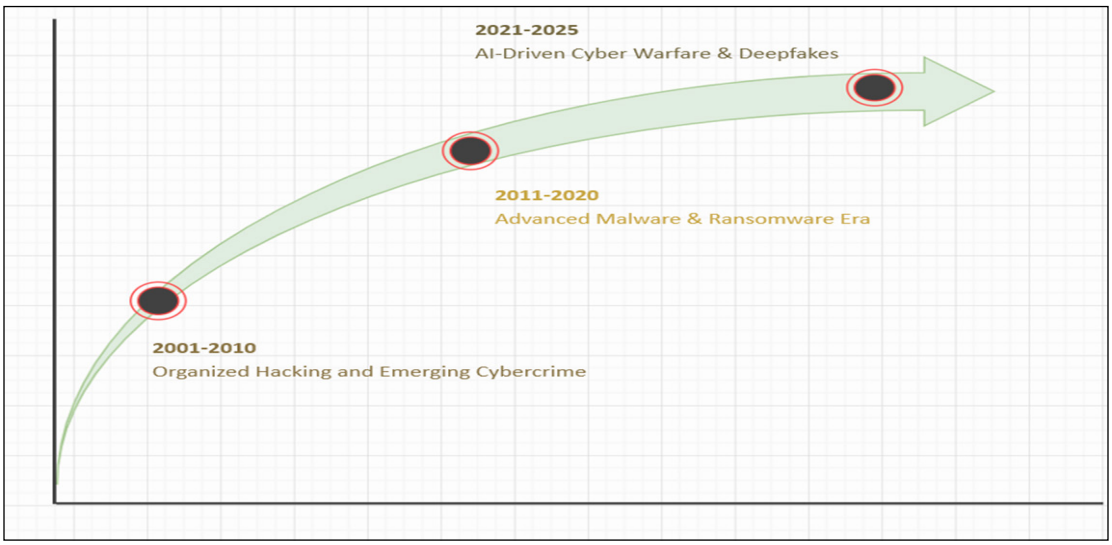

Fig. 2: Cyber Attacks by Extremist Groups

The landscape of cyber threats has drastically evolved over the years, especially about extremist groups. The following sections present an overview of the evolution of these cyber threats across three distinct periods, highlighting the technological advancements and strategic shifts that have characterized their methods.

2001-2010: Emergence of Organized Hacking and Cybercrime

In the early 2000s, the rise of organized cybercrime and hacking groups laid the foundation for the exploitation of digital vulnerabilities. Extremist groups initially employed basic hacking techniques for attacks, including website defacement, data breaches, and the dissemination of propaganda. This period marked the beginning of cyber threats as a tool for ideological warfare and criminal activity.

2011-2020: The Rise of Advanced Malware and Ransomware

From 2011 to 2020, cyber threats underwent a significant evolution, marked by the rise of advanced persistent threats (APTs), sophisticated malware, and ransomware. Extremist groups began leveraging these tools not only to disrupt digital systems but also as a means of financing operations through ransomware attacks and state-sponsored cyber warfare.

2021-2025: AI-Driven Cyber Warfare and Deepfake Disinformation

The most recent phase (2021-2025) has seen a dramatic shift towards AI-powered cyber threats and deepfake disinformation campaigns. Extremist groups, along with nation-states, have increasingly turned to artificial intelligence to conduct cyber warfare, create manipulated digital content, and spread misinformation. This phase has introduced new challenges in both offensive and defensive cybersecurity tactics.

Cyber Attack Trends (2015-2025)

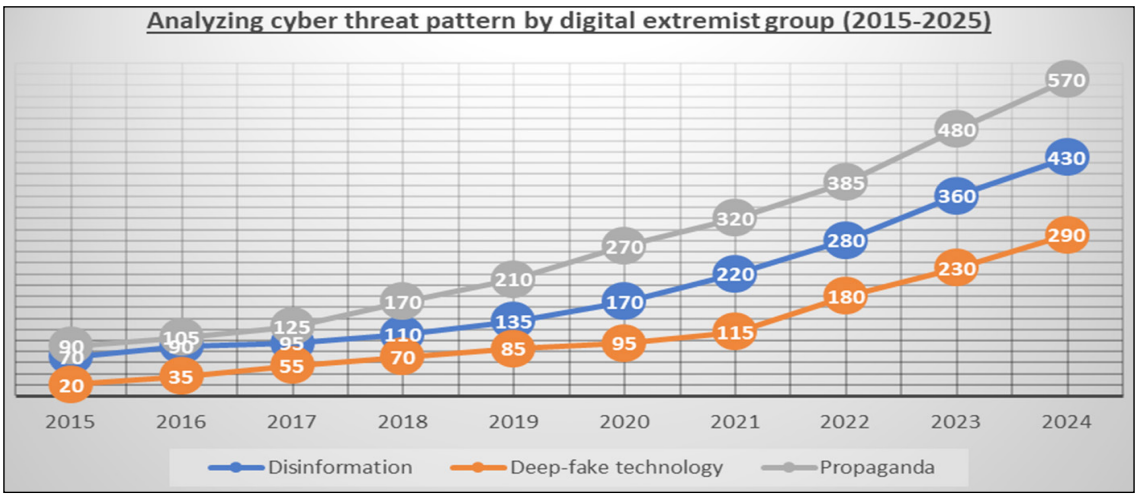

Fig. 3: Cyber threat pattern by digital extremist groups

Fig. 3 showed that misinformation, AI-powered fake content, and extremist propaganda are becoming bigger threats each year. As these numbers rise, it becomes increasingly important to develop robust cybersecurity and fact-checking measures. Over the past decade, the digital threat landscape has evolved dramatically, with extremist groups leveraging technology to spread disinformation, manipulate narratives, and radicalize individuals. Data from the Global Terrorism Index 2025 highlights three major cyber threats—Disinformation, Deep-Fake Technology, and Propaganda—all of which have shown alarming growth.

- Reported incidents (blue line) increased from 70 in 2015 to an estimated 430 by 2025.
- This surge reflects how extremist groups exploit social media and online platforms to spread false narratives, manipulate public opinion, and fuel division.

- Initially a minor concern (orange line) with 20 reported cases in 2015, deep-fake threats have escalated sharply, reaching 290 by 2025.
- Advances in artificial intelligence (AI) have enabled extremists to create hyper-realistic fake content, making it increasingly difficult to distinguish between authentic and manipulated media.
- The most pervasive digital threat (grey line), propaganda, grew from 90 reported cases in 2015 to 570 by 2025.
- Digital extremist groups continue to exploit online platforms to disseminate radical ideologies, recruit members, and influence vulnerable populations.

Evolution of Cyber Attacks by Extremist Groups

This section presents a comprehensive analysis of the evolution of cyber-attacks by extremist groups, the role of artificial intelligence (AI) and deepfake technologies, and the challenges faced in regulating digital extremism. It examines the technological advancements, strategic shifts, and regulatory challenges that must be addressed in combating digital extremism.

The evolution of cyber-attacks by extremist groups reveals a troubling shift from simple hacking attempts to sophisticated AI-driven misinformation campaigns. In the early stages, extremist groups utilized basic hacking techniques for activities such as website defacement, propaganda dissemination, and data breaches. Over time, these attacks have become increasingly sophisticated, incorporating advanced persistent threats (APTs) and ransomware attacks, which have targeted critical infrastructure and disrupted global systems.

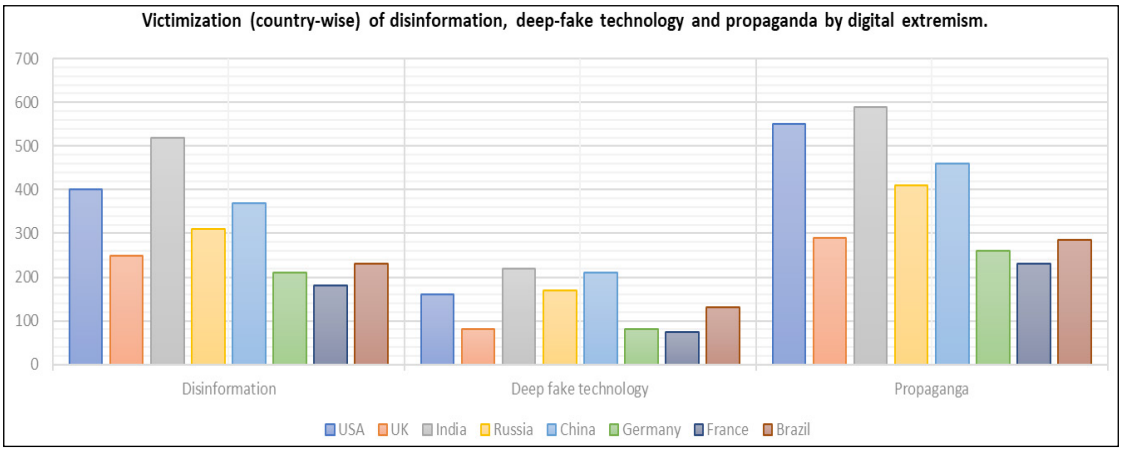

Fig. 4: Impact of digital extremism on various countries

One of the most concerning trends is the increasing use of cryptocurrencies for funding terrorist activities. Cryptocurrencies provide a high degree of anonymity, making it difficult for law enforcement agencies to trace financial transactions related to terrorism. This shift poses significant challenges to global counterterrorism efforts as extremists exploit these digital currencies to fund their operations without detection. The nations most frequently targeted by these cyber-attacks are those with significant political influence, including the USA, Russia, and India. These countries are often at the centre of geopolitical

conflicts, making them prime targets for cyber warfare and propaganda campaigns. As extremist groups become more adept at exploiting cyber vulnerabilities, these nations must enhance their cybersecurity strategies to defend against future attacks.

Fig. 4 illustrated that the impact of digital extremism on various countries, including the effects of disinformation, deepfake technology, and propaganda. India is the most impacted across all three areas, especially in propaganda and disinformation. The USA, China, and Russia also face significant challenges, particularly in disinformation and propaganda. Meanwhile, countries like the UK, Germany, France, and Brazil experience moderate impacts but are less affected compared to India and the USA. Overall, the graph highlights that digital threats are a global issue, with some countries being more heavily targeted than others.

Common Platforms Used by Digital Extremist groups for Spreading propaganda

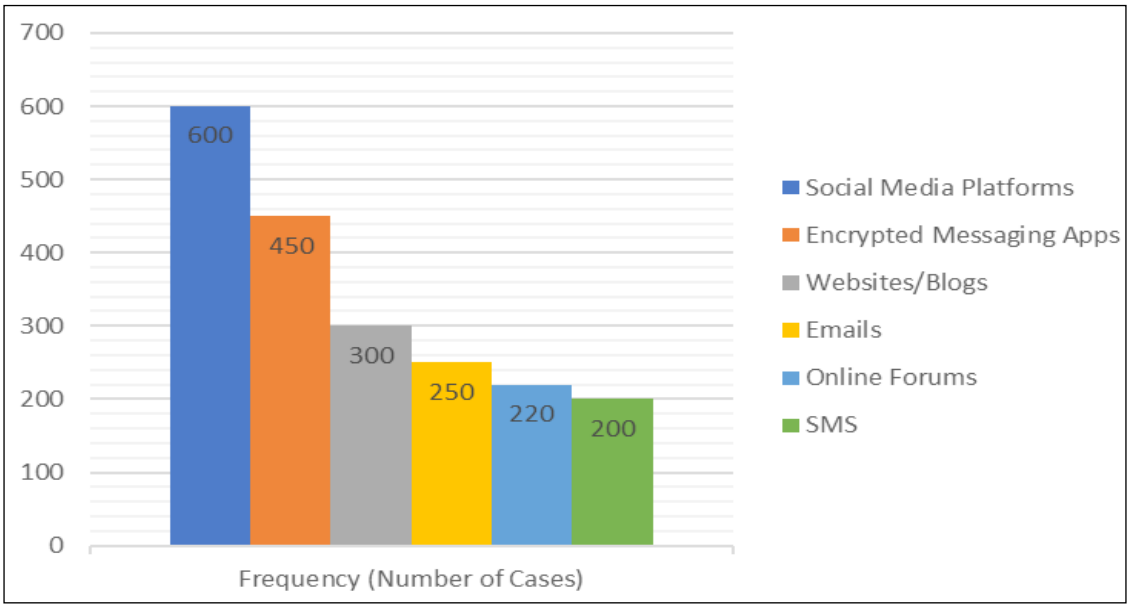

Fig. 5: Common Platforms Used by Digital Extremist Groups for Spreading Propaganda

Fig. 5 illustrated that the frequency of various digital platforms leveraged by extremist groups to disseminate their propaganda. The data reveals that Social Media Platforms are the most commonly used medium, with 600 reported cases, highlighting their vast reach and ease of access. Encrypted Messaging Apps follow as the second most preferred channel with 450 cases, likely due to the privacy and anonymity they provide. Websites and blogs rank third, being used 300 times and serving as detailed content hubs for extremist narratives. Emails account for 250 cases, indicating their use in direct, targeted communication. Online Forums are used 220 times, often acting as breeding grounds for discussions and radicalization. Lastly, SMS is the least-used medium, with 200 cases, possibly due to its limited reach and traceability compared to other digital platforms. This distribution clearly emphasizes the dominance of modern, interactive, and private digital communication channels in extremist propaganda efforts.

Country-Specific Impact Assessment of Disinformation, Deepfakes, and Propaganda

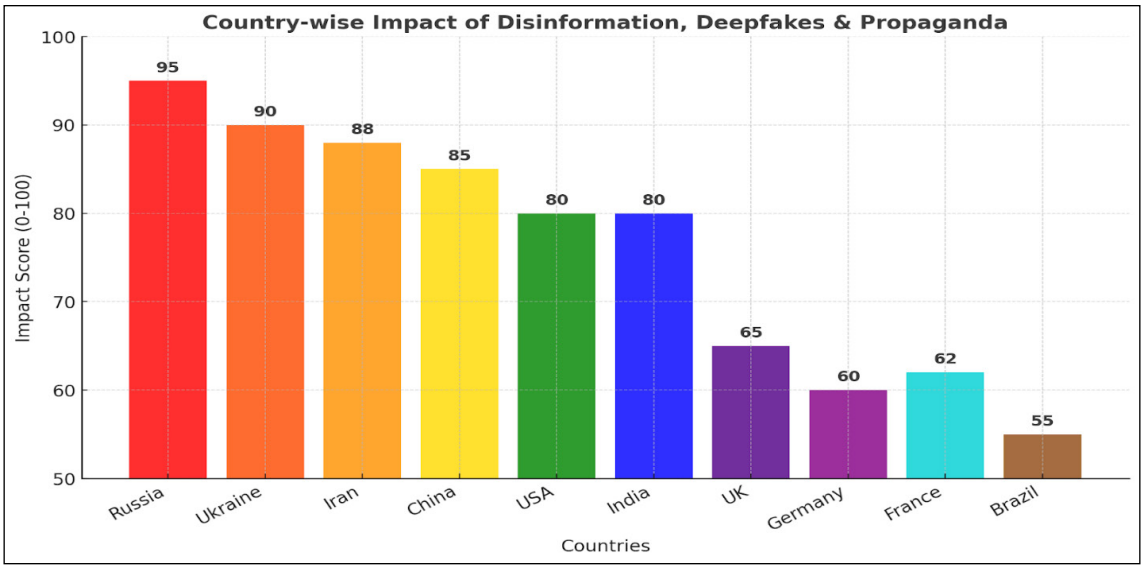

Fig. 6: Disinformation, deepfakes, and propaganda

Fig. 6 illustrated that the country-specific impact of disinformation, deepfakes, and propaganda, measured on a scale of 0 to 100. Russia tops the list with the highest impact score of 95, followed by Ukraine (90), Iran (88), and China (85), indicating that these countries are most affected or involved in such activities. The USA and India share a moderate impact score of 80, while the UK (65), France (62), and Germany (60) experience comparatively lower impacts. Brazil, with the lowest score of 55, is the least impacted among the countries listed. Overall, the graph indicates that countries such as Russia, Ukraine, Iran, and China are more susceptible to the influence or threat of disinformation and propaganda. In contrast, others, including Brazil and Germany, are relatively less affected.

In the digital age, the merging of cyber extremism and cyber warfare, alongside the psychological manipulation of vulnerable individuals, is transforming the landscape of conflict and radicalization. The fusion of advanced technology, psychological manipulation, and state-sponsored support for extremist groups is creating new challenges for both national security and digital governance. This section analyzes the intersection of these two phenomena and explores how AI-driven technologies and social media play a central role in shaping the future of digital extremism. As the global cybersecurity landscape evolves, the distinction between cyber extremism and cyber warfare has become increasingly blurred. Cyber extremism, historically associated with non-state actors and terrorist groups, has matured into a tool for state-sponsored agendas, blurring the roles of nation-states and extremist factions. These groups are no longer isolated in their activities but are often supported by powerful governments to further geopolitical goals through digital means. In cyber extremism, the focus has traditionally been on disruption, propaganda, and data breaches to instil fear and manipulate public perception. However, the rise of state-sponsored cyber warfare has led to more advanced and coordinated cyberattacks aimed at destabilizing entire nations or interfering in the domestic affairs of foreign states. Governments are increasingly accused of using proxy extremist groups to carry out covert cyber operations in situations where direct state involvement would

be politically unacceptable or too risky. This phenomenon has raised the stakes of cyber conflicts, with countries no longer only defending against terrorism but also dealing with the covert manipulations of nation-states. As cyber warfare continues to evolve, it is essential to rethink the traditional distinctions between non-state terrorism and state-backed cyber aggression, primarily as the latter increasingly relies on extremist groups to carry out operations that would otherwise be difficult to attribute or prosecute. This evolving relationship demands international cooperation to address the security gaps that such hybrid attacks exploit.

Challenges and Limitations

This research provides significant insights into the evolution and repercussions of cyber extremism; nevertheless, certain limitations must be recognised that may impact the comprehensiveness and accuracy of the findings. The constraints arise from issues related to data accessibility, the swift progression of cyber dangers, legal and ethical considerations, and regional variations in the occurrence of cyber extremism. These aspects provide substantial obstacles to the ongoing surveillance and comprehension of digital extremism. A significant constraint in the study of cyber extremism is the scarcity of accessible data, particularly when extremist activities transpire on encrypted platforms or dark web forums. Numerous extremist organisations and cybercriminals have progressively utilised secure communication platforms, such as encrypted messaging applications (e.g., Telegram, Signal), to orchestrate assaults and propagate propaganda. These platforms safeguard users' identities, complicating access to crucial information for researchers, law enforcement, and cybersecurity experts. Although certain security services can penetrate these networks, the restricted access into these encrypted environments obstructs a thorough comprehension of the methodologies, ideas, and strategies utilised by extremists in the digital realm.

The anonymity and privacy safeguards provided by these platforms provide ethical challenges for researchers and authorities. The evolving nature of cyber threats poses a considerable problem in sustaining current research approaches. The domain of cyber extremism and cyber warfare is ever advancing, with novel assault channels, strategies, and instruments routinely arising. As cyber attackers evolve and exploit weaknesses in digital systems, research approaches must consistently adapt to these developments. Moreover, the examination of cyber extremism poses considerable legal and ethical dilemmas that restrict the breadth of research. A fundamental concern is the equilibrium between surveillance and privacy. Gathering information about extremist activities frequently necessitates surveillance of persons and digital platforms, potentially resulting in infringements on data privacy and civil liberties. In many nations, legal statutes restrict particular investigative techniques, including hacking back and the surveillance of encrypted communications, owing to apprehensions of governmental overreach and personal liberties.

Furthermore, ethical dilemmas emerge when the scrutiny of extremist organisations possibly violates the privacy rights of innocent individuals who may be ensnared in the digital crossfire. These constraints necessitate meticulous navigation to guarantee that the research is both legally compliant and ethically robust.

Recommendations

Technology firms must consistently improve AI algorithms to identify extremist content in real-time across digital platforms. These algorithms must not only recognise textual content but also

contextualise photos, videos, and metadata to properly identify propaganda. Artificial intelligence must advance to comprehend nascent languages, colloquialisms, and cryptographic techniques employed by extremist organisations. Furthermore, the use of AI alongside human supervision will enhance decision-making, particularly in intricate situations where material may be ambiguous. Global collaboration in cybersecurity is essential for effectively addressing cyber terrorism. Governments ought to develop international legal frameworks that set uniform standards for the prosecution of cybercrime, data privacy, and the obligations of digital platforms. These statutes need to promote the formation of specialised divisions within law enforcement agencies focused on the investigation of cyber extremism. Moreover, educational systems must emphasise digital literacy to enable students to comprehend the risks of online radicalisation. Courses focused on critical thinking, media literacy, and cyber safety ought to be incorporated into educational curricula globally. Furthermore, governments and civil society organisations ought to endorse grassroots programs that offer training in identifying extremist narratives and comprehending the psychology of radicalisation.

Expanding international cyber intelligence-sharing mechanisms is essential for mitigating cross-border cyber threats posed by terrorist organisations. Through collaboration with entities like NATO, INTERPOL, and national cybersecurity agencies, nations can exchange real-time intelligence regarding developing threats and the tactics employed by extremist groups. Collaborative initiatives must encompass the development of collective cyber defensive capabilities, including AI-driven technologies capable of identifying trends of radicalisation. Governments, technology firms, and financial institutions must cooperate to create tools and policies that combat online extremism. Public-private collaborations can significantly contribute to the development of common databases, artificial intelligence models, and early warning systems that monitor terrorist activities across several platforms.

Investment in the research and development (R&D) of innovative technology is crucial to maintain an advantage over extremist groups. Research and Development should concentrate on creating creative counter-radicalization instruments, encompassing sophisticated AI systems that scrutinise user behaviour patterns, digital forensics tools that facilitate the tracing of cyberattacks, and privacy-enhancing technologies that reconcile security with civil liberties. The public and business sectors must to engage in financing academic research to investigate novel approaches for online deradicalisation.

CONCLUSION

Digital extremism is a swiftly advancing menace that persistently capitalises on emerging technologies to disseminate extreme ideology and execute highly sophisticated cyberattacks. As technological developments like quantum computing, AI-driven cyber weaponry, and deepfake-generated misinformation campaigns proliferate, the realm of digital extremism is expected to grow increasingly intricate and difficult to regulate. These technologies not only expand the dissemination and influence of extremist content but also create new vulnerabilities, necessitating proactive measures to counter these developing dangers. This study highlights the urgent want for robust cybersecurity frameworks that can adeptly respond to current technological breakthroughs. The future of countering digital extremism depends on leveraging artificial intelligence, machine learning, and other advanced technologies to detect, neutralise, and avert extremist operations in real time.

A coordinated global strategy is needed; nations must cooperate to create unified standards, regulations, and regulatory frameworks that can successfully tackle the transnational nature of cyber threats. The importance of education and public awareness in combating digital extremism is equally significant. Providing individuals with digital literacy skills and instilling critical thinking from an early age will be crucial in curbing the dissemination of extremist ideology. Governments, educational institutions, and technology corporations must invest in public awareness initiatives that instruct individuals on how to recognise, report, and address radicalisation in the digital era. The future of cybersecurity in addressing extremism will necessitate a comprehensive strategy involving technological advancement, international cooperation, and proactive education. By amalgamating these components, we can establish a more secure and robust digital landscape that mitigates the risks associated with extremist activity while enhancing the possibility for positive and secure online interactions. Only through these collaborative endeavours can we ensure a tranquil and safeguarded digital future for everyone.

ACKNOWLEDGMENTS

All authors express gratitude to the digital platform for providing essential data and support, as well as for their assistance and prompt responses, which made the study feasible.

REFERENCES

1. Awan, I. 2016. Cyber-extremism: ISIS and the power of social media. *Social Science & Public Policy,* **53**(3): 138–147.

2. Benkler, Y., Faris, R. and Roberts, H. 2018. *Network propaganda: Manipulation, disinformation, and radicalization in American politics.* Oxford University Press.

3. Berger, J.M. and Morgan, J. 2015. The ISIS Twitter census: Defining and describing the population of ISIS supporters on Twitter. *Brookings Institution Report.*

4. Braddock, K. and Horgan, J. 2016. Towards a guide for constructing and disseminating counter-narratives to reduce support for terrorism. *Studies in Conflict & Terrorism,* **39**(5): 381–404.

5. Conway, M. 2017. Determining the role of the Internet in violent extremism and terrorism. *Studies in Conflict & Terrorism,* **40**(1): 77–110.

6. Ebner, J. 2020. *Going dark: The secret social lives of extremists.* Bloomsbury Publishing.

7. Gill, P., Corner, E., Conway, M., Thornton, A., Bloom, M. and Horgan, J. 2017. Terrorist use of the Internet by the numbers: Quantifying behaviours, patterns, and processes. *Criminology & Public Policy,* **16**(1): 99–117.

8. Ingram, H.J. 2017. Deciphering the siren call of militant Islamist propaganda. *International Centre for Counterterrorism (ICCT).*

9. Johnson, N.F. *et al.* 2016. New online ecology of adversarial aggregates: ISIS and beyond. *Science,* **352**(6292): 1459-1463.

10. Weimann, G. 2016. *Terrorism in cyberspace: The next generation.* Columbia University Press.

11. Nacos, B.L. 2019. *Terrorism and counterterrorism.* Routledge.

12. Arquilla, J. and Ronfeldt, D. 2001. *Networks and netwars: The future of terror, crime, and militancy.* RAND Corporation.

13. Hussain, G. 2020. Cyber Jihad: How online extremism is transforming global security. *Cybersecurity Review,* **12**(4): 25–40.

14. Koehler, D. 2016. Understanding deradicalization: Methods, tools, and programs for countering violent extremism. *Routledge.*

15. Perry, B. and Scrivens, R. 2016. Right-wing extremism online: A thematic analysis of violent forums. *Studies in Conflict & Terrorism,* **39**(11): 871-892.

16. Holt, T.J. 2012. Examining the role of technology in the formation of deviant subcultures. *Social Science Computer Review,* **30**(1): 74–88.

17. European Commission, 2021. The role of AI in detecting extremist content. *European Security Journal, 18(2), 55–78.*

18. Rand Corporation, 2019. The future of cyber terrorism: Emerging threats and countermeasures. *RAND Research Report.*

19. McCauley, C. and Moskalenko, S. 2017. *Frictions: How radicalization happens to them and us.* Oxford University Press.

20. Koehler, D. 2019. Preventing violent radicalization in America. *National Security Review,* **25**(3): 32–47.

21. Papacharissi, Z. 2015. Affective publics and their role in political extremism. *Communication Theory,* **29**(4): 289–306.

22. Byman, D. 2020. *Road warriors: Foreign fighters in the armies of jihad.* Oxford University Press.

23. Singer, P.W. and Brooking, E.T. 2018. *LikeWar: The weaponization of social media.* Houghton Mifflin Harcourt.

24. Abrahms, M. 2008. What Terrorists Want: Terrorist Motives and Counterterrorism Strategy. *International Security,* **32**(4): 78–105.

25. Clarke, R.A. and Knake, R. 2019. *The Fifth Domain: Defending our country, our companies, and ourselves in the age of cyber threats.* Penguin.

26. National Counterterrorism Center, 2022. Online radicalization: Trends and mitigation strategies. *US Government Publication.*

27. FBI Cyber Division, 2021. Emerging cyber threats in extremist networks. *FBI Cybersecurity Report.*

28. European Parliament, 2020. Online radicalization and disinformation campaigns. *EU Policy Brief.*

29. UK Home Office, 2021. Countering online extremism: A policy approach. *Home Office Research Report.*

30. NATO Strategic Communications Centre of Excellence, 2020. Influence operations in cyberspace. *NATO Research Paper.*

31. Schmidt, A.P. 2016. The Role of Propaganda in Terrorist Recruitment. *Perspectives on Terrorism,* **10**(6): 25–45.

32. Dawson, L.L. 2018. The study of new religious movements and violent extremism. *Terrorism and Political Violence,* **30**(1), 98–115.

33. Wojcieszak, M. 2010. Effects of Online Radicalisation on Political Polarisation. *Journal of Political Communication,* **27**(3): 218-239.

34. Zech, S.T. and Kelly, M. 2015. Social media and terrorism: The case of ISIS. *Defense & Security Analysis,* **31**(2): 140–153.

35. Post, J.M. 2019. *The mind of the terrorist: The psychology of terrorism from the IRA to al-Qaeda.* Palgrave Macmillan.

36. Weimann, G. 2015. *Terror on the Internet: The new arena, the new challenges.* US Institute of Peace Press.

37. Denning, D. 2001. Activism, hacktivism, and cyberterrorism: The Internet as a tool for influencing foreign policy. *Harvard International Review,* **23**(2): 78–92.

38. Sageman, M. 2017. *Turning to political violence: The emergence of terrorism.* University of Pennsylvania Press.

39. Von Behr, I. *et al.* 2013. Radicalization in the digital era. *RAND Research Paper.*

40. Gartenstein-Ross, D. 2018. *Bin Laden's legacy: Why we are still losing the war on terror.* Wiley.

41. Bruce Schneier - "Data and Goliath"

42. Richard A. Clarke - "Cyber War"

43. P.W. Singer - "LikeWar: The Weaponization of Social Media"

44. Benjamin Wittes - "The Future of Violence"

45. David Sanger - "The Perfect Weapon"

46. Thomas Rid - "Rise of the Machines"

47. Nicole Perlroth - "This Is How They Tell Me the World Ends"

48. Christopher Hadnagy - "Social Engineering: The Art of Human Hacking"

49. Paul Rosenzweig - "Cyber Warfare: How Conflicts in Cyberspace Are Challenging America"

50. Alexander Klimburg - "The Darkening Web"