Paper ID: 125

Changing Threat Dimensions; Preventing Extremism in The Digital Age

CLCM Patabendige[1#]

[1]*Institute of National Security Studies*

[#]charani.patabendige@gmail.com

Abstract- *Extremism poses a persistent and significant threat to the stability of a nation. It is a complex psychological phenomenon that gradually leads to tangible actions, extending beyond its narrow military aspects. Countering extremism in the present digital era requires innovative strategies to effectively address and prevent it within the changing digital landscape. Therefore, this research aims to explore the intricate relationship between extremism and its implications for national security in the digital sphere. Sri Lanka's historical experiences with extremism, both before and after digitalization, add unique dimensions to this examination. Understanding how the digital age has become a fertile ground for disseminating and amplifying extremist ideologies is crucial for formulating effective countermeasures. Leveraging the digital space to counteract and prevent extremism warrants exploration. Using a qualitative methodology, this study will investigate the evolving threat landscape through various analysis techniques. By shedding light on these changes, it seeks to uncover the complexities associated with preventing extremism in the digital age. The findings will inform recommendations to reduce its impact.*

Keywords- Digital space, Extremism, Security, Sri Lanka

I. INTRODUCTION

The advent of the digital age has brought about significant transformations in societal structures and communication patterns. However, along with these advancements, new challenges have occurred in the realm of security. One pressing concern that necessitates immediate attention is the prevention of extremism in the digital age. The digital age refers to a time characterized by the widespread use of digital technologies like computers, the internet, and other digital communication tools. It has brought significant changes to how information is accessed, shared, and processed. Extremism, characterized by radical ideologies and the adoption of extreme measures to achieve ideological objectives, has found a fertile breeding ground in the digital environment. Online platforms have become instrumental in the dissemination of extremist content, recruitment of susceptible individuals, and the facilitation of extremist activities. As per, the Centre for Policy Alternatives (2021), the term "Violent Extremism" (VE) gained widespread recognition among analysts and development agencies worldwide following the events of 9/11. The reason behind its prominence was the realization that the approach of the United States and its allies, primarily focused on security concerns, proved ineffective in addressing the underlying causes of the issue. According to the Centre for Policy Alternatives (2021), the definition proposed by USAID, which is widely utilized, defines violent extremism as the endorsement, participation in, preparation for, or support of violence driven or justified by ideology to advance social, economic, or political objectives. Essentially, it pertains to violence that is justified through a rigid ideology as the exclusive means of attaining specific social, economic, and political aims. Nevertheless, establishing a clear understanding of extremism can be problematic due to varying interpretations among individuals.

Within this context, two essential characteristics of violent extremism have been identified. Firstly, it involves exalting one's group or faith while being deeply concerned with the challenges it confronts. Secondly, it encompasses the rejection of diversity and the concept of an inclusive society. These intrinsic attributes of violent extremism underscore its deviation from democratic principles, including the acceptance of diversity and the upholding of universal human rights. Addressing this issue requires a comprehensive understanding of the complexities surrounding extremism in the digital age and the development of effective strategies to counter its proliferation. This paper highlights the urgency of preventing extremism in the digital age. The digital revolution has provided extremists with unprecedented opportunities, necessitating a comprehensive understanding of the evolving threat landscape. By critically examining the challenges and opportunities associated with preventing extremism in the digital space, this research aims to contribute to the development of effective strategies that safeguard security interests while upholding individual rights in the digital era.

II. LITERATURE REVIEW

As mentioned by (Zeiger & Gyte), “The global reach of these online platforms has allowed terrorist networks to merge and spread across national boundaries, cultures, and languages. This has resulted in the formation of global coalitions among previously separate terrorist organizations, a phenomenon that the researcher fully agrees with the author on. A notable example is the pledging of allegiance (bayat) to Abu Bakr al-Baghdadi, the leader of ISIS. Due to geographic and security constraints, traditional methods of expressing loyalty in person were impractical, prompting the utilization of social media as an alternative approach. The Researcher concur that this shift towards online platforms has been particularly evident in Southeast Asia, where various terrorist groups in the Philippines and

Indonesia, such as Maute, Abu Sayyaf, Katibat Ansar al-Sharia, and Mujahidin Indonesian Timor, have pledged their allegiances via online videos. The acceptance and recognition of these pledges have also been released through online video platforms, reinforcing the researcher's agreement with the author's perspective on the role of social media in facilitating and documenting these alliances."

(Evans & Williams, 2022) state that the internet's unique characteristics contribute to individual radicalization, a point supported by the researcher. Virtual echo chambers immerse users in inhomogeneous media environments, reinforcing the tendency to seek like-minded individuals and affirming information. Algorithmic systems, as identified by the researcher, customize information presentation based on user preferences. Within these echo chambers, interaction plays a significant role in radicalization. Users engage with extremist content and like-minded peers, fostering an environment conducive to radicalization. The researcher's analysis highlights the importance of understanding these dynamics for effective counter-radicalization strategies. The internet's influence on individual beliefs and behaviour, as explored by the researcher, is a topic of concern.

The same authors go on to mention that Efforts to disrupt online extremism and prevent the indoctrination of individuals have been undertaken by various governmental, educational, and civil sector entities. These initiatives involve the use of automated tools to identify and remove violent, hateful, or harmful content, aiming to inhibit its spread online. The researcher agrees with the author's viewpoint and emphasizes the significance of these measures. Tech companies have implemented advanced algorithms and collaborations with law enforcement agencies to swiftly remove extremist content from their platforms. Governments have also introduced regulatory frameworks to ensure accountability and responsible content moderation. Educational initiatives promote digital literacy and critical thinking skills, while civil society organizations foster dialogue and peace-building efforts. Collectively, these actions demonstrate a commitment to combatting online extremism. While challenges persist, stakeholders are dedicated to creating a safer online environment. The literature reflects consensus on the importance of collaborative approaches, automated content moderation, educational programs, and civil society engagement in countering radicalization online. The researcher supports these strategies and emphasizes their role in curbing the spread of extremist ideologies in the digital realm.

III. METHODOLOGY

The research methodology employed in this paper aims to effectively address and prevent extremism in the dynamic digital age. It utilizes a qualitative approach, focusing on non-numerical data and avoiding statistical conclusions. Both primary and secondary sources are utilized for data collection and analysis. Secondary data sources, such as scholarly articles, books, reports, and literature, are analyzed to support the research objectives. This analysis helps identify patterns and gaps in knowledge related to extremism in the digital age. Throughout the research, various examples and case studies are incorporated to illustrate and validate the findings. These examples substantiate statements and arguments, providing practicality and relevance to the analysis. Real-world instances are examined to shed light on effective strategies and approaches for countering and preventing extremism in the digital landscape.

IV. ANALYSIS AND DISCUSSION

A. Extremism and National Security

Scholars have presented various interpretations and definitions of the term "extremism," influenced by societal norms, cultural values, religious beliefs, and gender perspectives. Consequently, the understanding of extremism may differ among individuals, posing inherent challenges in addressing this phenomenon. It is crucial, therefore, to examine existing definitions of extremism, including its association with violent extremism, to develop a comprehensive understanding. As stated by the Danish government, "Extremism refers to individuals or groups that commit or seek to legitimize violence or other illegal acts, based on societal conditions they disagree with. This term encompasses various forms such as left-wing extremism, right-wing extremism, and Islamist extremism" (Schmid, n.d.). Likewise, J.M. Berge describes extremism as the belief that an in-group's success or survival necessitates hostile actions against an out-group, which can range from verbal attacks and discrimination to violence and even genocide (Schmid, n.d.). The notion of violent extremism, according to Berge, involves the belief that violent action is indispensable for an in-group's success or survival, whether defensive, offensive, or pre-emptive. In line with the Federal Bureau of Investigation's definition, violent extremism is characterized as "encouraging, condoning, justifying, or supporting the commission of a violent act to achieve political, ideological, religious, social, or economic goals" (LaFree and Freilich, 2019). These definitions highlight the diverse motivations behind individuals' engagement in extremist activities, often resorting to violence, which is considered illegitimate.

Extremism, including violent extremism, poses a significant threat to national security for several reasons. It disrupts social order, harmony, tranquillity, social cohesion, community engagement, and stability. It undermines the rule of law and freedom of expression. Extremist ideologies can lead to the radicalization of individuals, making them vulnerable to recruitment by terrorist organizations. These organizations exploit the isolation and exclusivity

experienced by extremists, offering them a sense of belonging and purpose in exchange. Consequently, extremist acts give rise to terrorism, impacting both individuals and the state, with military and non-military implications. Moreover, extremism fosters discrimination within society, contributing to polarization along ethnic, religious, or political lines. Violent extremists advocate for separatism, which poses a threat to the territorial integrity of nations. Additionally, the transnational nature of extremism, violent extremism, and terrorism involving multiple actors creates complex international networks and funding mechanisms, straining diplomatic relationships between nations. Furthermore, extremism violates both the human rights and fundamental rights of individuals.

B. Digital age as a platform for extremism

To comprehend the facilitation of extremism and violent extremism in the digital age, it is essential to grasp the nature of the present world. According to Digital Sociology (n.d.), the Digital Age, also known as the Information Age or the Computer Age, characterizes the contemporary era in which the pervasive use of the Internet has become integral to various dimensions of society. This era emerged in the 1970s and encompasses the widespread adoption of personal computers and communication technologies, significantly impacting social, political, and business domains. In the fully digitalized landscape of today, the propagation and promotion of extremism have become effortless undertakings. As a result, individuals and societies face a formidable challenge in combatting extremism amidst the opportunities and challenges presented by the digital age. The ramifications of extremism manifest both online and in tangible forms, posing threats to national security.

In line with the research by Ganesh and Bright (2020), drawing upon the insights of Gill et al. (2017), it is evident that extremists skillfully exploit social media platforms and the broader realm of the Internet to serve their purposes. These purposes encompass the dissemination of hateful narratives, propaganda, financial transactions, recruitment activities, and the exchange of operational information. An example of hate speech as stated in (Al Jazeera, 2019) is, “hate propaganda targeting Muslim communities” in Sri Lanka aftermath of the Easter Sunday Bombings 2019 which were by National Thawheed Jamath inspired by ISIS. Furthermore, social media platforms have become conduits for inciting violence, as extremists share provocative content and venerate terrorist leaders. According to Digital Watch Observatory, “Terrorist entities employ online propaganda as a strategic tool to effectively radicalize individuals, recruit supporters and new members, and even instigate "lone wolf attacks" (as evidenced by the case of the Christchurch gunman [who live telecasted], who is believed to have undergone online radicalization). The dissemination of online propaganda also serves the central aim of terrorist activities, which is to propagate fear and apprehension within society.” The digital landscape also exposes vulnerabilities to cyber terrorism, as governmental and private entities face the risk of system disruptions and compromised information security. Influential figures on social media pose an additional challenge, as they attract susceptible youth by projecting glamorous lifestyles that obscure their underlying terror connections. Moreover, contemporary trends indicate an increasing utilization of disinformation by violent extremists and terrorist groups, particularly targeting vulnerable populations residing in conflict-affected regions, as underscored by the International Centre for Counter-Terrorism - ICCT (n.d.). Additionally, the dark web, a clandestine segment of the internet that evades search engine indexing, serves as a breeding ground for extremist activities, encompassing the illicit trade of goods, coordination of attacks, and the dissemination of hard-to-access extremist content. Easy accessibility to extremist and terrorist networks for the exchange of information further exacerbates the challenges associated with extremism in the digital age. Further, it is important to draw attention that the process of radicalization and recruitment predominantly occurs within the online domain, facilitated by extremist groups leveraging various means such as propaganda outlets, front organizations, cover identities, and sympathetic networks.

a. Sri Lankan situation

Before the widespread usage of the term "Violent Extremism," Sri Lanka had already experienced various instances of such phenomena. In 1971, the Janatha Vimukthi Peramuna (JVP) uprising served as the country's first encounter with organized violent extremism following its independence. As highlighted by the Center for Policy Alternatives (2021), the subsequent LTTE uprising in the 1980s predominantly involved Tamil youth from the northern and eastern regions of Sri Lanka. This uprising can be categorized as a form of violent extremism, as Tamil youth were trained, armed, and indoctrinated with an ideology focused on the pursuit of a separate Tamil Eelam. Extremist Buddhist nationalism also poses a threat, exemplified by groups like Bodu Bala Sena.

Additionally, the 2019 Easter Sunday attacks, alleged to be carried out by an ISIS-inspired group called National Thawheed Jamath, shook the country. It can be regarded as a prominent incident where online extremism happened afterwards. Following the attacks, Sri Lanka temporarily blocked certain social media networks and messaging apps, including Facebook and WhatsApp, as reported by Al Jazeera (2019). This action was taken in response to an inflammatory post that incited anti-Muslim riots across multiple towns. In one such town, Chilaw, predominantly inhabited by Christians, there were instances of stone-throwing at mosques and Muslim-owned shops in response to the Facebook post made by a shopkeeper,

according to the police. The aftermath of these events witnessed communal violence, including the boycott of Muslim businesses. Sri Lanka faced a significant rise in online extremism following the Easter Sunday bombings, targeting the Muslim community. On one hand, there was understandable fear among non-Muslims in the wake of the unprecedented brutal bombings. On the other hand, innocent Muslims who had no association with the extremist group NTJ were unfairly affected.

C. Prevention of extremism in the digital age

The digital age, despite its inherent challenges and role as a platform for online extremism, can also be effectively harnessed for positive purposes. The essence lies in utilizing the digital age efficiently to contribute to the well-being of humanity. Although individuals who are radicalized, extremists, and terrorists may exploit the online realm for their hidden motives, it is imperative to acknowledge that the opposing party can employ the digital age as a means to counter and eliminate such attacks. Ultimately, the crux of the matter lies in strategically utilizing the digital age as a potent tool to combat and eradicate the threats posed by online extremism.

Starting from individuals, tech companies, and private entities to governments all over the world are utilizing precautionary measures to prevent online extremism. These measures can be by way of websites, laws, resolutions or policies. Social media platforms have community standards where if they detect extremist activities they take it down, it also provides the opportunity to report such content. For example, YouTube uses enhanced Content Moderation, where machine learning algorithms and human moderators are employed as moderators to identify and remove extremist content from its platform. In Sri Lanka, Section 3 of the International Covenant On Civil and Political Rights Act No.56 of 2007 (ICCPR Act) is a significant legal framework to address hate crimes. The Educate Against Hate website, established by the Home Office and Department of Education of the United Kingdom is another example. the website serves as an information hub catering to students, teachers, and parents. Its primary objective is to provide a comprehensive range of resources and support materials aimed at countering extremist ideologies and promoting education focused on tolerance and inclusivity. Another example is the Global Internet Forum to Counter Terrorism (GIFT), which is an initiative that facilitates the collaboration and exchange of information among the technology industry, government bodies, civil society organizations, and academic institutions. Its primary objective is to collectively address and mitigate the impact of terrorist and violent extremist activities on the internet. Another example is the Toronto Declaration which addresses the protection of human rights in the context of artificial intelligence. Led by Amnesty International and Access Now, it has received widespread support from the global human rights community.

V. CONCLUSION

In conclusion, the prevention of extremism in the digital age is a pressing concern that demands immediate attention and this applies to Sri Lanka as well. The digital revolution has transformed societal structures and communication patterns, presenting both opportunities and challenges in the realm of security. Extremism thrives in the digital environment, where online platforms have become instrumental in disseminating extremist content, recruiting susceptible individuals, and facilitating extremist activities. Understanding extremism requires examining diverse definitions influenced by societal norms, cultural values, religious beliefs, and gender perspectives. Extremism, including violent extremism, poses significant threats to national security, social order, and human rights, while also fostering discrimination and straining diplomatic relationships. Online platforms, including social media and the dark web, serve as powerful tools for the dissemination of hate speech, recruitment, and incitement of violence. Prevention efforts necessitate a collaborative approach involving individuals, tech companies, private entities, and governments, with measures such as community standards, legislation addressing hate crimes, and collaborative initiatives for information sharing. Promoting digital literacy and education focused on tolerance are crucial components. International cooperation, exemplified by initiatives like the Global Internet Forum to Counter Terrorism, is essential in mitigating the impact of online extremism. By comprehensively understanding the threat landscape and strategically utilizing digital tools, societies can counter extremism and create a safer and more inclusive digital environment.

VI. RECOMMENDATIONS

To further advance the endeavours aimed at countering extremist activities within the digital realm, a range of supplementary actions can be deployed. Of paramount importance is the cultivation of digital literacy among individuals, equipping them with the capacity to identify terrorist or extremist content and comprehend the potential ramifications, thereby fortifying their resilience against falling prey to such material. Moreover, fostering collaboration with technology companies assumes pivotal significance as it engenders cooperation among governments, law enforcement agencies, and technology enterprises, ultimately yielding the development and implementation of policies specifically designed to counteract extremist activities. In this context, technology companies can allocate resources towards the deployment of cutting-edge algorithms and artificial intelligence systems that expedite the identification and removal of extremist content. Additionally, the establishment of a robust reporting mechanism, congruent with principles of victim

and witness protection, assumes indispensable importance. Concurrently, forging alliances with civil society actors constitutes a potent strategy, providing a platform for civil society organizations, community leaders, and religious institutions to engender online dialogues, cultivate mutual understanding, and promote initiatives aimed at fostering peace. Lastly, the augmentation of international cooperation assumes paramount significance, as it facilitates the exchange of information among governments, law enforcement agencies, and technology companies, thereby bolstering efforts to combat extremist activities transcending national boundaries. The sharing of best practices, intelligence, and expertise serves to fortify preventive measures and response capabilities, amplifying the efficacy of counter-extremism endeavours.

REFERENCES

1. Ai and violent extremism - trends in 2023 (no date) Digital Watch Observatory. Available at: https://dig.watch/topics/violent-extremism (Accessed: 18 June 2023).
2. Al Jazeera (2019) *Sri Lanka blocks social media again after attacks on Muslims, Sri Lanka Bombing News | Al Jazeera*. Available at: https://www.aljazeera.com/news/2019/5/13/sri-lanka-blocks-social-media-again-after-attacks-on-muslims (Accessed: 19 June 2023).
3. Al Jazeera (2019) Sri Lanka urged to tackle 'hate propaganda' against Muslims, Human Rights News | Al Jazeera. Available at: https://www.aljazeera.com/news/2019/8/26/sri-lanka-urged-to-tackle-hate-propaganda-against-muslims (Accessed: 18 June 2023).
4. Digital Sociology. (n.d.). The Digital Age | The Challenges And Effects To Humanity. [online] Available at: https://digitalsociology.org.uk/.
5. Educate against hate (no date) Campaign Toolkit. Available at: https://www.campaigntoolkit.org/casestudies/educate-against-hate-uk-government/ (Accessed: 18 June 2023).
6. Ganesh, B. and Bright, J. (2020). Countering Extremists on Social Media: Challenges for Strategic Communication and Content Moderation. Policy & Internet, 12(1), pp.6–19. doi:https://doi.org/10.1002/poi3.236.
7. International Centre for Counter-Terrorism - ICCT. (n.d.). Strategic Communications, Disinformation and Violent Extremism. [online] Available at: https://www.icct.nl/project/strategic-communications-disinformation-and-violent-extremism [Accessed 18 Jun. 2023].
8. LaFree, G. and Freilich, J.D. (2019). Government Policies for Counteracting Violent Extremism. Annual Review of Criminology, 2(1), pp.383–404. doi:https://doi.org/10.1146/annurev-criminol-011518-024542.
9. *Policy recommendations on preventing violent extremism in Sri Lanka*. Available at: https://www.cpalanka.org/wp-content/uploads/2021/12/PVE-Eng_webfile.pdf (Accessed: 19 June 2023).
10. Schmid, A. (n.d.). Chapter 2 Terrorism Prevention: Conceptual Issues (Definitions, Typologies and Theories). [online] Available at: https://www.icct.nl/sites/default/files/2023-01/Chapter-2-Handbook-.pdf
11. von Behr, I., Reding, A., Edwards, C. and Gribbon, L. (2013). Radicalisation in the Digital Era. [online] Available at https://www.rand.org/content/dam/rand/pubs/research_reports/RR400/RR453/RAND_RR453.pdf.

AUTHOR BIOGRAPHY

Charani Patabendige is an Acting Research Analyst and Research Assistant at the Institute of National Security Studies in Sri Lanka. She is a NESA alumna and currently a postgraduate student pursuing an MPhil/PhD in Law. She holds a Bachelor of Laws degree from General Sir John Kotelawala Defence University with a second class. In addition, she has a distinction pass in Advanced Diploma in Transitional Justice. Charani also served as a member of the committee for reviewing Sri Lanka's Defence Policy. Currently, she is actively involved in the National Authority for Preventing Violent Extremism in Sri Lanka. In addition, she has represented Sri Lanka numerous times.