

Research Vidyapith International Multidisciplinary Journal

(International Open Access, Peer-reviewed & Refereed Journal)

(Multidisciplinary, Monthly, Multilanguage)

* Vol-2* *Issue-4* *April 2025*

Examining the Threat of Digital Disinformation to National Security In The Modern Era

Hariom Kochar

Research Scholar, Centre For Kashmir Studies, School of Social Science, Central University of H.P, Dharmshala

Abstract-

The purpose of this study is to investigate the various aspects of digital deception, with a particular focus on the psychological, social, and political repercussions as they pertain to the Indian context. The research makes use of a mixed-methods approach, which blends qualitative analysis derived from literature reviews and case studies with statistical data obtained from a structured public survey. The key findings indicate that there is a significant shortage of public knowledge; a large number of individuals lack the confidence to recognise and combat incorrect information that can be found on the internet. The sections point that is brought up in the report is the role that social media websites play in the rapid dissemination of false information, as well as the deficiencies of the existing legal and institutional solutions. When compared with practices from around the world, comparative research highlights the urgent need for coordinated responses, which may include changes to regulations, initiatives to improve digital literacy, and efforts to collaborate internationally. At the end of the study, there are certain policy recommendations that are possible. These recommendations are intended to raise institutional resilience and improve public preparation against attacks of disinformation.

Keywords- Digital disinformation, National security, public awareness, social media, information warfare.

Introduction

Disinformation has evolved into a complex and pervasive threat in the contemporary digital world beyond individual false information or rumour (Sarts, 2020). Misinformation in the digital world is the intentional creation and dissemination of false or deceptive content through digital means intended to influence public opinion, impact political results, or erode society trust. In contrast to traditional forms of false information, online disinformation is often algorithmically amplified, personalized based on personal data, and disseminated at rapid velocities across social

media, websites, and messaging applications (Boban, 2022).

The growing use of social media platforms, where material virality often outweighs factual accuracy, has accelerated this trend. Disinformation campaigns have been far more impacted by the ability of adversarial actors—state and non-state alike—to employ echo chambers and filter bubbles. Additionally, the anonymity of the internet, the breakdown of traditional gatekeeping in journalism, and the commodification of attention have all played a part in creating a fertile ground for the dissemination of deceptive material (Slugocki & Sowa, 2021).

Disinformation is not only a threat to public perception but also to democratic institutions, national security, and social cohesion in our time. It erodes trust in truthful information sources, deforms reality, and appeals to emotions. Formulating effective countermeasures in this case demands a knowledge of the systems, tools, and incentives that fuel digital deception.

Historical Trajectory and Evolution in the Digital Era

For falsehoods as an influence weapon is nothing new; it has ancient roots in military, propagandistic, and political strategy. From bogus intelligence employed by ancient civilizations to psychological operations during the Cold War, misinformation has been used for centuries to manipulate public opinion and disrupt enemy systems. What distinguishes today, however, is the magnitude, velocity, and sophistication with which false information can be disseminated and digested (Zaloga, 2022).

The transition from traditional to online media has revolutionized the character of information warfare. Previous disinformation strategies relied primarily on written content, radio communications, or state-controlled media. The age of the internet, in contrast, allows millions to rapidly repost and reshare inaccurate information, often without fact-checking. Deepfakes, botnets, and artificial intelligence-generated content have all added to the innovation of disinformation tactics, so that it now becomes increasingly difficult for users to distinguish fact from fiction (Vasu et. al., 2018). Cornerstone historical moments have framed this development: the 2016 US presidential election, Brexit referendum, and global responses to the COVID-19 pandemic all illustrated the ways disinformation could inform public discourse, augment polarisation, and impact democratic processes. Nation-states, political strategists, ideologues, and even business players have since applied these tactics in order to achieve strategic objectives.

The growth of deception in the digital age therefore reflects a major paradigm change in the way information is weaponised. For knowing its historical background enables the public, academics, and politicians identify reoccurring trends and new dangers in the complicated information ecosystem of today (Moral, 2022).

Digital Disinformation as a National Security Concern

Digital technology has made disinformation a major national security concern. Disinformation is intentionally incorrect or misleading information provided to sway public opinion and shape views. Unlike misinformation, which can be conveyed accidentally, disinformation is a deliberate tactic sometimes used by state and non-state actors to upset

populations, erode confidence in institutions, and sway political results (American Security Project, 2023).

Around the world, disinformation tactics have been used to disrupt political processes, provoke violence, and undermine public confidence. For example, foreign players used social media channels during the 2016 U.S. presidential election to disseminate fake stories meant to affect voter behaviour and create conflict. Likewise, in Myanmar, widespread false information on Facebook fuelled ethnic violence against the Rohingya minority (B. P. A., 2024).

With its vast and diverse population, India is particularly prone to the dangers of electronic disinformation. Misinformation has spread on fertile ground created by the rapid expansion of internet penetration and the extensive use of social media platforms. Disinformation in India typically targets specific groups to incite sectarian conflicts and disrupt social peace by playing on linguistic and cultural diversity.



Figure 1: Government of India Action Against Disinformation on YouTube under IT Rules, 2021

Source: Ministry of Information and Broadcasting, Government of India

One such important case is the April 2022 response of the government, which shut down 16 YouTube news channels operated by the Ministry of Information and Broadcasting for spreading fake news related to public order and national security. Six channels were operating from Pakistan and 10 from India, and they were found to be circulating content that could possibly put national security at risk and disrupt public order (Press Information Office, 2022). For Recognizing the threat posed by disinformation, the Indian government has moved in many ways to contain its dissemination. These include the enforcement of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, which mandate digital platforms to remove unlawful content promptly and establish grievance redressal mechanisms (Press Information Office, 2022).

In addition, initiatives like the National Digital Literacy Mission aim to educate individuals on how to use digital channels appropriately and the necessity of verifying information prior to spreading (Observer Research Foundation, 2023). The entire plans against disinformation are also being developed by government agencies, tech companies, and civil society actors in collaboration.

Digital disinformation is a multi-faceted threat to national security

that impacts political stability, social cohesion, and public trust. In India, it is compounded by the diversity of the country and the rapid digitalisation of information dissemination. By Addressing the issue requires an integrated approach encompassing legal regimes, public education campaigns, technology interventions, and international cooperation to safeguard the country's democratic fabric and social cohesion.

Aim

With particular focus on the Indian setting, the main goal of this paper is to critically investigate the rising impact of digital disinformation and its consequences for national security. The study aims to know the channels of disinformation dissemination, spot sensitive areas in the socio-political and digital ecosystems, and assess current governmental initiatives to reduce its influence.

Objectives

- To analyze the psychological, social, and political impact of digital disinformation on national security and public trust in India.
- To evaluate the effectiveness of government policies, institutional mechanisms, and media responses in countering digital disinformation.
- To assess public awareness and societal resilience toward fake news and disinformation across different digital platforms.

Scope of the study

This study is limited to the analysis of digital disinformation—specifically, information that is intentionally false or misleading and spread via the internet, social media, and digital news platforms. Though worldwide examples are included for comparison, the geographical focus is India. From the development of social media as a dominant information source—roughly 2010—to the present, the chronological emphasis covers. Touching on media studies, security studies, information technology, and political science, the work is multidisciplinary.

Research Questions

The study is guided by the following research questions:

1. How does digital disinformation affect national security and public perception in the Indian socio-political context?
2. What strategies and mechanisms have been implemented by Indian authorities and media platforms to combat disinformation?
3. To what extent are Indian citizens aware of digital disinformation, and how confident are they in identifying and resisting it?

Research Methodology

In order to fully comprehend the threat that digital disinformation poses to national security, this study uses a mixed-methods research design that combines qualitative and quantitative techniques. The research begins with a thorough literature review, analyzing scholarly articles, government publications, iimc publication, policy briefs, and reports from international organizations and National organizations. This provides a

conceptual foundation and contextual background for the study

To gather empirical data, a structured survey questionnaire was developed and administered to assess public awareness, perceptions, and levels of resilience toward disinformation. The results of this survey are presented and analyzed in Section 3. Additionally, a series of case studies were examined, focusing on notable instances where disinformation campaigns had a significant impact on electoral processes, communal harmony, or international relations. These case studies offer grounded insights into the real-world implications of disinformation.

A comparative study is also conducted, assessing India's existing counter-disinformation strategies and comparing them with the ones used by nations like the United States, Estonia, and the European Union member states. This serves to point out both good practices and gaps in current policy. Additionally, content analysis was used to study media reports, fact-checking websites, and social media trends with the goal of tracking the way disinformation is produced, shared, and consumed online.

Lastly, the data gathered—most especially from the survey—are treated with descriptive statistics such as frequency distributions and percentages, and interpretative methods are employed to determine commonly recurring themes and patterns of public sentiments. The end-result of the combined methodology is a strong and multi-dimensional analysis of the research issue.

THE STRATEGIC ROLE OF THE STATE IN ADDRESSING DIGITAL DISINFORMATION

Information warfare, strategic communication, information operations, psychological operations, and disinformation must be defined in the changing cyber world. For national and social security, information warfare involves offensive and defensive methods to gain an informational edge (Arcos, 2024). Though definitions vary, many now consider information a strategic resource.

NATO and the National Security Bureau define strategic communication as coordinated public diplomacy, media, and psychological operations to alter views and achieve long-term goals (NATO, 2022). It borders marketing and organisational behaviour academically (Wilbur, 2017). Information operations use numerous methods to influence adversary decisions while protecting one's own systems (NATO, 2022). Psychological operations are conducted by military and civilian agencies to influence behaviour. While often avoided due to its negative connotation, propaganda has historically been defined as intentional persuasive message (MLIGO, 2023; Nikitenko et al., 2024).

The EU and NATO prioritise strategic communication to address hybrid threats from Russia and terrorist groups. EU Global Strategy (2016) and Common Framework for Countering Hybrid Threats emphasise collaboration to counter disinformation. Media saturation, psychological manipulation, and globalisation fuel incorrect information, especially in digital and sensationalist media.

Since cyberattacks sometimes use mass media to spread misinformation, media cyberspace is a major vector. Media algorithms unwittingly amplify these attacks, requiring closer collaboration between media and

governments to ensure accurate communication and public confidence.

Security is a widespread social issue. Security, from the Latin **securitas** ("without worry"), is a procedure (protection) and a condition (feeling safe) that must adapt to new threats (Caramancion, 2020). Independent from risk to basic values is the typical concept (Wambua et al., 2020). Social sciences define a danger as an actual or prospective risk to life, property, or social order, sometimes impacted by human perspectives (Tenove, 2020). Globalisation has blurred civilian and military divides, creating unanticipated complications. False information threatens democracy, national security, and social stability. Though interpretations vary, disinformation is increasingly recognised as harmful and intentional.

To combat adversarial narratives, the EU's Hybrid Fusion Cell and Strategic Communication Task Forces develop counterstrategies. The 2017 Freedom on the Net survey showed governments increasingly use social media for political gain (Balogun et al., 2025). In 2015, the EU identified the threat of fake news (Europejska, 2015), establishing Task Force South, Western Balkans Task Force, and East StratCom. During the 2019 European Parliament elections, major publications defended democratic integrity due to rising concerns (Joint Communication, 2018; Dezinformacja, 2021).

The fight against lies requires continual research, public education, and institutional cooperation. Awareness helps people spot manipulation and protect themselves and others. Strategic communication initiatives, including embassies and cultural institutions, are crucial given Russian disinformation and hybrid assault during the Ukraine conflict. The EU Anti-Disinformation Action Plan (2018) defines disinformation as intentionally false material affecting the public. Security is complex, context-dependent, and dynamic (Koziej, 2022). Today, information security is crucial among modern security methods. Piotr Potejko defines it as "a set of activities, methods, and procedures by authorised entities to ensure the integrity of stored and processed information resources by securing them against unauthorised disclosure, modification, or destruction" (Potéjko et al., 2009). Other definitions emphasise information availability, secrecy, and protection from unintended or intentional destruction.

This study emphasises the growing danger digital disinformation poses to India's national security, democratic integrity, and social cohesion. Encrypted platforms like WhatsApp have seen especially notable growth in false information; according to the Digital India Report (2023) from the Ministry of Electronics and Information Technology (MeitY), WhatsApp accounts for 64% of false information spread in the nation, followed by Facebook (18%) and Twitter (12%). With India seeing a 214% increase in fake news incidents in 2020, the COVID-19 epidemic made this problem even worse, according to the National Crime Records Bureau (NCRB) (Vishwanath et al., 2021).

Disinformation has far-reaching consequences that influence electoral processes, fuel communal strife, and erode institutional public confidence. For example, disinformation operations have been used to disseminate polarising stories during the Indian elections, hence affecting voter

behaviour and maybe causing long-term social effects. Furthermore, the employment of deepfakes in political campaigns has become a new difficulty as phoney videos affect public perception and skew the election scene. The Indian government has therefore started actions including the shutdown of 16 YouTube channels spreading false information about public order and national security. These initiatives, therefore, have to be included into a larger, multi-pronged approach. Among the policy suggestions:

- Updating legislation to cover the subtleties of digital deception guarantees responsibility for offenders and protects free speech.
- Establishing countrywide initiatives to teach people how to spot and combat false information helps to improve media literacy.
- Working closely with social media businesses to track and reduce the spread of misleading information is part of cooperation with technology platforms.
- Encouraging government organisations to aggressively exchange correct information helps to close the gap for false information to flourish.

Notwithstanding these efforts, difficulties remain. Some platforms' encrypted character makes tracking difficult; the fast changing of disinformation strategies, notably those involving artificial intelligence-generated material, calls for constant adjustment. Future studies should emphasise creating sophisticated detection systems, knowing the psychological elements that render people vulnerable to false information, and assessing the efficacy of present counter-disinformation techniques. Ultimately, fighting digital disinformation in India calls for coordinated action by the public, government agencies, civil society, and technology companies. India can protect its democratic principles and national security against the widespread danger of false information by promoting a knowledgeable and resilient citizenry.

The national security scene has been greatly enlarged by media growth and technological development. New developments—like disinformation—now call for information security to be seen as a vital component of national defence policy.

PUBLIC AWARENESS AND SOCIETAL RESILIENCE TO DIGITAL DISINFORMATION

Because cyberspace allows both good and evil behaviour, the Internet has revolutionised political engagement. E-mobilization, which allows widespread political participation through affordable and accessible media, is the key idea (Benkler et al., 2018). However, hostile states, criminals, terrorists, and other evil people utilise the Internet for illicit operations including cyberattacks and spreading false information (Wasiuta et al., 2018).

Disinformation is not new, but the Internet and social media have amplified it, allowing vast public opinion manipulation. False information producers leverage psychological deficiencies for political, commercial, or ideological gain (Zannettou et al., 2018). Disinformation tactics, especially those that use emotional manipulation and terror, can change public

opinion (Wasiuta et al., 2018).

The definition of "security" now encompasses political, technical, economic, and social challenges. In this expanded security context, misinformation is a huge threat, generally unnoticed and capable of great damage through psychological manipulation and modern technology (Wambua et al., 2020). To combat deception, states are protecting their citizens. The media may spread incorrect information but also educate the public on how to recognise and reject false narratives. Strategic communication strategies are vital in this struggle to increase public knowledge and resilience to disinformation (Benkler et al., 2018).

Even though the Internet has democratised political activity, it also created new vulnerabilities. Governments, media, and civil society must work together to promote media literacy, openness, and responsibility in information distribution to combat disinformation.

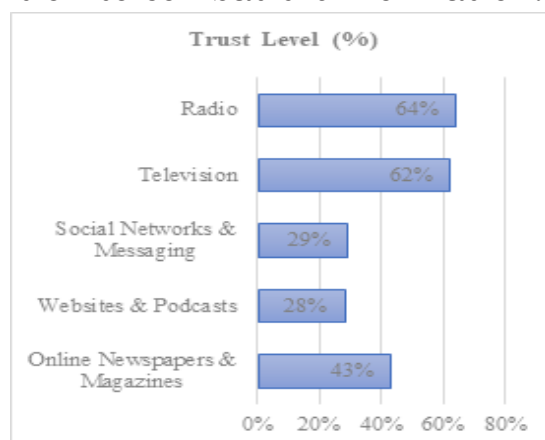


Figure 2: Trust in Information Channels

Figure 2 indicates that the Information and news from online sources (online periodicals and newspapers) are less likely to be trusted by respondents (43%), followed by websites and podcasts (28%), social media, and instant messaging (29%). The vast majority of respondents (64%), however, fully trust or inclined to fully trust news and information obtained from television networks. 62%.

Table 3: Frequency of Encountering False Information

Frequency of Encounter	Percentage (%)
Daily or Almost Daily	41%
At Least Once a Week	38%

Table 4: Confidence in Identifying Fake News

Confidence Level	Percentage (%)
Confident (Completely/Somewhat)	65%
Unsure or Unable	32%

Table 4 indicates the Public trust in spotting false or misleading news

or information—65% of those polled claim they are totally or somewhat confident in their ability to discern news or information distorting reality. Conversely, 32% of those polled cannot or do not know news or information to recognise it.

Table 5: Perceived Threat of Disinformation

Statement	Agreement (%)
Disinformation affects citizen mood	88%
Disinformation threatens security and democracy	86%

Table 5 shows the great deal of respondents—up to 88% when considering the scope of the problem of disinformation in cyberspace—think that citizens' moods are undoubtedly impacted by the phenomenon of disinformation on the Internet. According to 86% of those surveyed, it also jeopardises the country's democracy and security.

Table 6: Suggested Actors to Combat Fake News

Actor	Responsibility (%)
Journalists	51%
State Institutions	42%
Social Networks	34%
EU Institutions	29%
NGOs	31%

Table 6 shows the respondents said journalists - 51%, state institutions and offices - 42%, social networks - 34%, EU institutions - 29%, and NGOs - 31% in relation to their opinion and view of what media actors and institutions should do to stop the spread of false information and news.

Case Studies: Evaluating the Impact of Public Awareness Initiatives

• Alt News— Community-Based Media Literacy Fact-Checking

-Background

It is Co-founded in 2017; Alt News has become one of the most well-known independent fact-checking portals in India. It was created in reaction to the increasing amount of false information, particularly in social and political contexts.

- Action:

The group created a powerful mechanism for dispelling false information in real time, particularly that which spreads via social media and WhatsApp. In order to give people the ability to check information, Alt News also started digital literacy initiatives in rural and university settings.

- Impact:

When it comes to preventing disinformation during election seasons and public events, alt news has been essential. For their journalistic work, the co-founders were recognised internationally and nominated for a Nobel Peace Prize in 2022 (Valiyamattam, 2024). Their efforts have enhanced media consumers' fact-checking habits and raised public awareness of

fake news.

•Interactive Public Engagement with WebQoof by The Quint

-Background:

The Quint's WebQoof was introduced to combat viral fake news using an open and transparent paradigm, with a particular emphasis on false information disseminated via WhatsApp.

-Action:

The WebQoof encouraged the public to submit questionable items to its tipline, where journalists would then verify it. Additionally, it worked with the BBC on the "Swachh Digital India" campaign, creating videos that demonstrated how fake news propagates and how to spot it.

-Impact:

The WebQoof has grown into a user-driven real-time verification platform that is particularly well-liked by young, urban consumers (Posetti et al., 2019). The program became a reliable digital literacy tool and increased public participation in the battle against false information.

CONCLUSION AND STRATEGIC OUTLOOK

This study shows that digital disinformation is threatening public confidence, democratic government, and national security. The study found that modern disinformation strategies use psychological manipulation, emotional appeal, and algorithmic amplification to influence public opinion. The poll results' frightening public exposure to fake news and many people's lack of trust in their ability to recognise disinformation were concerning. Despite changes, Indian institutional initiatives struggle with regulatory enforcement, inter-agency cooperation, and public communication. Beyond political instability, disinformation undermines state sovereignty, social cohesion, election procedures, and public trust in honest institutions. Uncontrolled disinformation can generate community turmoil, diplomatic issues, and long-term governance issues in unstable sociopolitical environments. This study proposes a multifaceted approach for governments and societies. Policymakers must reform digital material laws, increase interagency coordination, and invest in cybersecurity infrastructure. Media literacy programmes must be entrenched in education and community-level digital awareness campaigns promoted quickly. Technology platforms should monitor misinformation and work with fact-checking groups.

Reference-

1. American Security Project. (2023, June 27). Disinformation and the threat to national security. American Security Project. <https://www.americansecurityproject.org/public-diplomacy-and-strategic-communication/disinformation>
2. Arcos, R., Chiru, I., & Ivan, C. (Eds.). (2024). Routledge handbook of disinformation and national security. Routledge.
3. B, P. A. (2024, January 18). The threat of disinformation to national security in the digital age.
4. Balogun, A. Y., Alao, A. I., & Olaniyi, O. O. (2025). Disinformation in the digital era: The role of deepfakes, artificial intelligence, and open-source intelligence in shaping public trust and policy responses. In O. Oladeji (Ed.), Disinformation in

- the digital era (pp. xx–xx). [Publisher].
5. Benkler, Y., Faris, R., & Roberts, H. (2018). *Network propaganda: Manipulation, disinformation, and radicalization in American politics*. Oxford University Press.
 6. Boban, M. (2022). Information and disinformation: Impact on national security in the digital age. *Economic and Social Development: Book of Proceedings*, 1(January), 309–317.
 7. Caramancion, K. M. (2020, March). An exploration of disinformation as a cybersecurity threat. In *2020 3rd International Conference on Information and Computer Technologies (ICICT)* (pp. 440–444). IEEE. <https://doi.org/10.1109/ICICT50521.2020.00081>
 8. CyberPolicy.pl. (n.d.). Dezinformacja. Retrieved May 14, 2021, from <https://www.cyberpolicy.pl/>
 9. European Commission & High Representative of the Union for Foreign Affairs and Security Policy. (2018). Joint communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions: Action Plan against Disinformation. Brussels.
 10. European External Action Service. (2015–2017). Strategic Communication Task Forces and EU Hybrid Fusion Cell. East StratCom Task Force (June 2015), Western Balkans Task Force (December 2015), Task Force South (June 2017). Brussels: European External Action Service.
 11. Koziej, S. (2011). *Security: Essence, basic categories, and historical evolution*. Warsaw.
 12. Ministry of Information & Broadcasting. (n.d.). Ministry of I&B blocks 16 YouTube news channels for spreading disinformation related to India's national security, foreign relations and public order. Retrieved [Date], from <https://pib.gov.in>
 13. Mligo, A. (2023). *Assessing threats caused by social media on national security* (Doctoral dissertation, International Academy of Arts).
 14. Moral, P. (2022). The challenge of disinformation for national security. In *Security and defence: Ethical and legal challenges in the face of current conflicts* (pp. 103–119). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-031-08271-4_8
 15. NATO. (n.d.). Strategic Communications Policy. Public Intelligence. Retrieved April 12, 2022, from <https://publicintelligence.net/nato-stratcom-policy>
 16. Nikitenko, L., Sharmar, O., Marusiak, O., Honcharuk, V., & Yanivskyi, V. (2024). Social media as an emerging threat to national security. *Amazonia Investiga*, 13(82), 100–111.
 17. Observer Research Foundation. (n.d.). India's two-front information war. ORF. Retrieved [Date], from <https://www.orfonline.org>
 18. Posetti, J., Simon, F., & Shabbir, N. (2019). What if scale breaks community? Rebooting audience engagement when journalism is under fire. Reuters Institute for the Study of Journalism.
 19. Potejko, P. (2009). Information security. In K. A. Wojtaszczyk & A. Materska-Sosnowska (Eds.), *State security* (p. 193). Warsaw: Oficyna Wydawnicza ASPRA-JR.
 20. Rada Europejska, Sekretariat Generalny Rady. (2015, March 19–20). Posiedzenie Rady Europejskiej – Konkluzje (p. 5). Brussels.
 21. Sarts, J. (2020). Disinformation as a threat to national security. In *Disinformation and fake news* (pp. 23–33). Singapore: Springer Singapore. <https://doi.org/10.1007/>

978-981-15-5097-0_3

22. Slugocki, W. L., & Sowa, B. (2021). Disinformation as a threat to national security on the example of the COVID-19 pandemic. *Security and Defence Quarterly*, 35(3). <https://doi.org/10.35467/sdq/142533>
23. Tenove, C. (2020). Protecting democracy from disinformation: Normative threats and policy responses. *The International Journal of Press/Politics*, 25(3), 517–537. <https://doi.org/10.1177/1940161220918740>
24. Valiyamattam, R. J. (2024). Exploring the Alt News phenomenon: A case study of one of India's most prominent fact-checking campaigns. *Rupkatha Journal on Interdisciplinary Studies in Humanities*, 16(4).
25. Vasu, N., Ang, B., Teo, T. A., Jayakumar, S., Raizal, M., & Ahuja, J. (2018). Fake news: National security in the post-truth era. S. Rajaratnam School of International Studies. <https://www.rsis.edu.sg/research/icpvtr/>
26. Vemuri, A. (2016). After Nirbhaya: Anti-sexual violence activism and the politics of transnational social media campaigns (Doctoral dissertation, McGill University, Canada).
27. Vishwanath, A. (2021, September 16). NCRB data: 214% rise in cases relating to fake news, rumours. *The Indian Express*. <https://indianexpress.com/article/india/214-rise-in-cases-relating-to-fake-news-rumours-7511534/>
28. Wambua, I. M. (2020). Impact of social media on national security in Africa: Case study Kenya (Doctoral dissertation, University of Nairobi). <http://erepository.uonbi.ac.ke/handle/11295/154021>
29. Wasiuta, O., & Wasiuta, S. (2017). *Wojna hybrydowa Rosji przeciwko Ukrainie*. Kraków: Arcana.
30. Wasiuta, O., & Wasiuta, S. (2018). Medialna manipulacja informacja w wojnie hybrydowej Rosji przeciwko Ukrainie. In R. Klepka (Ed.), *Medialne obrazy swiata. Wybrane problemy spoleczno-polityczne w mediach* (pp. 162–163). Kraków: Wydawnictwo Naukowe Uniwersytetu Pedagogicznego.
31. Wilbur, D. (2017). Propaganda's place in strategic communication: The case of ISIL's Dabiq magazine. *International Journal of Strategic Communication*, 11(3), 209–223. <https://doi.org/10.1080/1553118X.2017.1328613>
32. Zaloga, W. (2022). Disinformation in the age of the digital revolution in the aspect of state security. *Wiedza Obronna*, 280(3), 43–62.

Cite this Article-

'Hariom Kochar, 'Examining the Threat of Digital Disinformation to National Security In The Modern Era', Research Vidyapith International Multidisciplinary Journal (RVIMJ), ISSN: 3048-7331 (Online), Volume:2, Issue:04, April 2025.

Journal URL- <https://www.researchvidyapith.com/>

DOI- 10.70650/rvimj.2025v2i40011

Published Date- 16 April 2025