International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Examining the Role of Information and Artificial Intelligence in National Security: A Comparative Analysis

Kavya. S. M[a]. , *Dr. Keerthi Kumar H M*[b]

Research Scholar [a], Malnad Collge of Engineering, Hassan, Karnataka-573201, India
Associate Professor[b], Malnad Collge of Engineering, Hassan, Karnataka-573201, India

ABSTRACT :

Information plays a very important role in national security, with the potential to both strengthen defenses against threats and expose vulnerabilities to cyber-attacks. The information revolution has brought about significant advancements, but it also introduces complex challenges that must be addressed to maintain stable national security. Social media, in particular, has emerged as a powerful source of information that can be manipulated, leading to potential destabilization of security measures. Artificial Intelligence (AI) is a key tool in this landscape, intelligently analyzing public information from social media to mitigate risks and combat cyber-attacks. This research focuses on key areas such as public information access, its impact on national security, the risks posed by cyber-attacks, and the vital role of AI in enhancing national security efforts.

Keywords: Artificial intelligence, cyber attacks, information role, information security, national security, social media information.

1. Introduction :

The role of information and advanced artificial intelligence (AI) in shaping national security has become increasingly of significance in this digital age. While the revolutionary information offers immense potential to enhance national security measures, it also introduces complexities and challenges that need to be addressed properly. Particularly, the proliferation of endless information on various social media platforms has raised considerable concerns about its manipulation and the potential to destabilize national security! . This particular document delves deeply into the impactful consequences of social media information, the risks associated with cyber-attacks, and the pivotal role that AI could possibly play in identifying and mitigating potential threats to national security. Notably, the authors propose an innovative model and functional algorithm to continuously monitor and consequently limit social media information that poses risks.

2. Literature Survey

By conducting a Systematic Literature Review (SLR) to gather credible and authentic arguments related to the impact of information on national security, the evolution of information, and the risks of cyber-attacks.

[2] The author's analyzed and underlined contradictions in knowledge with the opacity of many AIs versus transparency sought by progressive political, social, and economic leader for good governance. [3}. The writers jump into the fastly changing scenery of fake intelligence (AI) and machine studying (ML) as they relate to national safety, with a particular accent on their merging into military implementations.

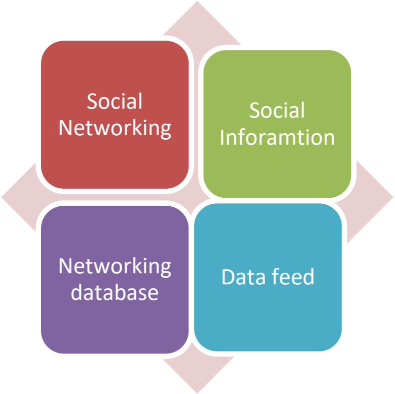


Fig. 1 : Cycle Of cyberspace with social media

Fig a in the paper represents the information cycle on cyberspace and its integration with social media. It illustrates how social networking databases contribute to future data predictions, activity tracking, market trends, and users' response rates in response to national threats. The figure highlights the role of social media in spreading information and the potential impact it can have on national security. It emphasizes the need for monitoring and analyzing social media information to identify and address potential threats effectively .

3. Methodology

The methodology used here is a Systematic Literature Review (SLR) process, which involves a thorough, transparent, and replicable process for literature search and critical analysis . The authors followed the recommendations provided by Kitchenham for conducting the SLR, which includes scoping, search and analysis, and selection of peer-reviewed papers guided by research questions . The search and analysis process involved searching relevant peer-reviewed literature on credible search engines such as Google Scholar, Scopus, and Web of Knowledge . The criteria for inclusion in the study involved papers that clearly addressed the combined use of 'Information' and 'National Security' and aligned with the research purpose .

The research question that may be raised be:

RQ1 : What kind of information are available to the public corresponding to the national security through social media?

RQ2 : How Informations are affecting the national security over time.

RQ3 : What are all the current and future risks of cyber-attacks, and Cyber-wars resulting from information driven media?

R4 : How Artificial Intelligence is playing important role in national security for accomplishing competent information role and acting as a saviour for national security?

In recognizing the significance of national security in the digital age, a series of inquiries are warranted to explore the impact of information dissemination and technological advancements on safeguarding a nation's well-being. Through the lens of social media, the public's access to security-related content is a pressing concern. Additionally, understanding the evolution of information's influence on national security is crucial for addressing ongoing and potential risks of cyber warfare. Moreover, the pivotal role of Artificial Intelligence in enhancing national security capabilities cannot be overlooked, as it serves as a guardian of vital information in today's complex landscape.

Tools and strategies can be used to limit the spread of information and ensure national security:

To limit the spread of information and ensure national security, several tools and strategies can be employed:

1. Establishing Information Control Laws: Instead of imposing bans on social media, national security agencies can implement laws that restrict and filter information sharing capabilities of social media platforms .

2. Utilizing AI-Based Tools: AI-based tools can help in monitoring and analyzing social media activities to identify potential threats and malicious activities. These tools can also help in locating anonymous actors and taking corrective actions

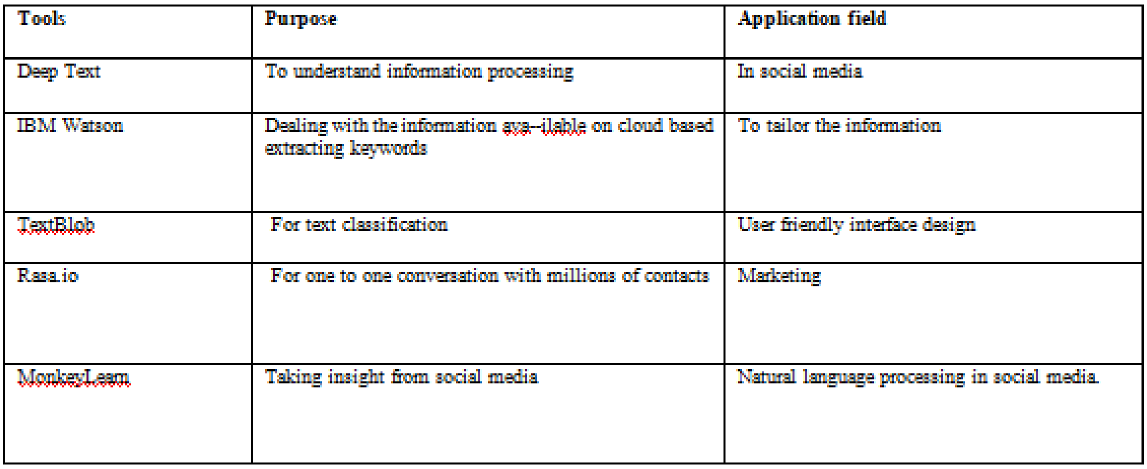
3. Creating a Model for Information Filtering: Developing a model to control and filter social media information that targets and destabilizes national security can be an effective strategy. This model can include functional algorithms for tracking and stopping harmful information from spreading

4. Implementing Strategic Measures: Planning strategic national action plans based on objectives and agenda can contribute to predicting future threats and weaknesses of attackers . Ensuring that implementing thse strategies are kept confidential can enhance security measures

5. Utilizing AI for Information Investigation and Analysis: AI can be used for investigating and analyzing information circulating through social media to identify potential risks and threats to national security .By utilizing a combination of these tools and strategies, authorities can work towards limiting the spread of harmful information and safeguarding national security in an era where information poses significant challenges..

4. Related Work

These AI-based tools are essential for monitoring activities, identifying threats, and ensuring the success of national security plans . The tools mentioned in the document are designed to automate tasks, manage social media, and analyze information to better understand national preferences . They also play a crucial role in combating cyber-attacks and safeguarding against anti-national factors . Overall, these AI tools are instrumental in enhancing national security measures and protecting against potential threats.



Tools	Purpose	Application field
Deep Text	To understand information processing	In social media
IBM Watson	Dealing with the information ava--ilable on cloud based extracting keywords	To tailor the information
TextBlob	For text classification	User friendly interface design
Rasa.io	For one to one conversation with millions of contacts	Marketing
MonkeyLearn	Taking insight from social media	Natural language processing in social media.

TABLE 2. AI tools for information assistance on social media.

Represents social networking databases contribution toward future data predictions, activity tracking, market trends, and users response rates in response to any national threats. Data feed features extend national compromises.

How does the information revolution impact national security?

The information revolution has a significant impact on national security as it poses both opportunities and challenges. The rapid diffusion of information, especially through social media platforms, has the potential to strengthen national security by providing valuable insights and intelligence . However, the accessibility and manipulation of information on social media can also pose threats to national security by spreading false information, destabilizing relationships, and exposing sensitive data to cyber-attacks .

The availability of information on social media can influence public perception, impact decision-making processes, and even lead to economic losses . Cyber-attacks, such as hacking into email accounts of government officials, releasing false news, or leaking sensitive information, can have severe consequences on national security . As social media becomes more integrated into daily life and reaches a vast number of users worldwide, the risks of cyber-attacks and manipulation through information-driven media increase .

To address these challenges, it is essential for national security agencies to utilize information technology and artificial intelligence (AI) to identify potential threats, secure information sharing, and protect national security mechanisms . AI can intelligently analyze public information from social media to detect and combat threats to national security . Implementing measures to control and filter information sharing capabilities of social media through AI tools can help prevent cyber-attacks and safeguard national interests .

5 Conclusion

The document highlights the significant role of information and artificial intelligence (AI) in national security. It emphasizes the potential of the information revolution to strengthen national security measures but also raises concerns about the complications it presents, especially in the context of social media manipulation and cybersecurity threats.

In future discussions, researchers are encouraged to focus on establishing all-purpose multi-functional information handling tools that can enhance national security measures. This includes developing parameters to meet security standards and catch national threats before they can harm security plansFuture discussions should center around leveraging AI tools, establishing proactive national security strategies, and implementing secure measures to combat cyber threats and protect national security. By continuously refining and enhancing information handling processes, researchers can contribute to strengthening national security in the face of evolving cyber challenges.

REFERENCES :

[1] D. C. Rowe, B. M. Lunt, and J. J. Ekstrom, ‘‘The role of cybersecurity in information technology education,’’ in Proc. Conf. Inf. Technol. Educ. (SIGITE), New York, NY, USA, 2011, pp. 113–122, doi: 10.1145/2047594.2047628.

[2] MPilar, Cousido-González., Daniel, Palacios-Alonso. (2022). Artificial Intelligence serving National Security: the Spanish case. doi: 10.1109/MECO55406.2022.9797172

[3] A., M., Al-Dousari. (2023). Optimizing National Security Strategies through LLM-Driven Artificial Intelligence Integration. doi: 10.36227/techrxiv.22787327

[4] Tomasz, Guta. (2022). The applicability of the gdpr to artificial intelligence and the resulting threats to national information security. Studia Bezpieczeństwa Narodowego, doi: 10.37055/sbn/151151

[5] (2021). S. E. Institute. CERT Coordination Center. [Online]. Available: https://sei.cmu.edu/about/divisions/cert/index.cfm

[6] D. C. Mowery, ‘‘National security and national innovation systems,’’ J. Technol. Transf., vol. 34, no. 5, p. 455, 2009

[7] A. Dutta and K. McCrohan, ‘‘Management’s role in information security in a cyber ecoomy,’’ California Manage. Rev., vol. 45, no. 1, pp. 67–87, Oct. 2002, doi: 10.2307/41166154.

[8] T. E. Copeland, ‘‘The information revolution and national security,’’ Army War College, Carlisle Barracks PA, Strategic Stud. Inst., USA, Tech. Rep., 2000. [Online]. Available: https://apps.dtic.mil/sti/ pdfs/ADA382498.pdf

[9] S. L. Jarvenpaa and A. Majchrzak, ‘‘Knowledge collaboration among professionals protecting national security: Role of transactive memories in ego-centered knowledge networks,’’ Org. Sci., vol. 19, no. 2, pp. 260–276, Apr. 2008.

[10] E. C. Tandoc, D. Lim, and R. Ling, ‘‘Diffusion of disinformation: How social media users respond to fake news and why,’’ Journalism, vol. 21, no. 3, pp. 381–398, Mar. 2020.

[11] S. J. Schwartzstein and W. A. Owens, The Information Revolution and National Security: Dimensions and Directions. Washington, DC, USA: Center for Strategic & International Studies, 1996. [Online]. Available: https://www.ojp.gov/ncjrs/virtual-library/abstracts/informationrevolution-and-national-security-dimensions-a

[12] V. V. Novikov, ‘‘Digitalization of economy and education: Path to business leadership and national security,’’ Bus. Ethics Leadership, vol. 5, no. 2, pp. 147–155, 2021.

[13] J. Der Derian, ‘‘Global events, national security, and virtual theory,’’ Millennium, J. Int. Stud., vol. 30, no. 3, pp. 669–690, Dec. 2001, doi: 10.1177/03058298010300030301.

[14] K. A. Oluwadamilola, ‘‘The role of information technology in national security: ‘A case study of Nigeria,’’’ Global J. Comput. Sci. Technol., vol. 16, no. 3, pp. 1–7, 2016. [Online]. Available: https://computerresearch.org/index.php/computer/article/view/1443

[15] J. Norbekov, ‘‘Ensuring information security as an ideological problem,’’ Mental Enlightenment Sci. Methodol. J., vol. 2020, no. 1, pp. 56–65, 2020.

[16] Z. D. Clopton, ‘‘Territoriality, technology, and national security,’’ Univ. Chicago Law Rev., vol. 83, no. 1, p. 45, 2016. [Online]. Available: https://heinonline.org/HOL/P?h=hein.journals/uclr83&i=47

[17] S. Fischer and A. Wenger, ‘‘Artificial intelligence, forward-looking governance and the future of security,’’ Swiss Political Sci. Rev., vol. 27, no. 1, pp. 170–179, Mar. 2021.

[18] G. Mani, ‘‘Data processing and analytics for national security intelligence: An overview,’’ in Data Management, Analytics and Innovation. Singapore: Springer, 2022, pp. 293–315, doi: 10.1007/ 978-981-16-2937-2. [16] A. Bratko, A. Datskov, D. Oleshko, V. Vychavka, and O. Olytskyi, ‘‘Some aspects of capability-based planning in the field of national security,’’ Turkish J. Comput. Math. Educ., vol. 12, no. 6, pp. 2219–2225, Apr. 2021, doi: 10.17762/turcomat.v12i6.4827

[19] M. N. Al-Suqri and M. Gillani, "A Comparative Analysis of Information and Artificial Intelligence Toward National Security," in IEEE Access, vol. 10, pp. 64420-64434, 2022, doi: 10.1S109