Tiako P.F. (ed) *Competitive Tools, Techniques, and Methods*. Chronicle of Computing. OkIP. CAIF24#17
© 2024 Oklahoma International Publishing https://doi.org/10.55432/978-1-6692-0007-9_5

Using Artificial Intelligence (AI) and Machine Learning (ML) to Disrupt the Negative Impact of Disinformation on Digital Sovereignty and Social Stability Through Cognitive Security in Elections

Joseph Squillace, Justice Cappella

Penn State University, jms10943@psu.edu, Schuylkill Haven,17972, United States
Penn State University, jlc6927@psu.edu, Schuylkill Haven, 17972, United States

ABSTRACT

Artificial Intelligence (AI) and Machine Learning (ML) stand at the forefront of election security. However, the rapid ascension of AI and ML as future tenets of modern election integrity have required these resources be protected to safeguard democracy from disinformation, misinformation, and media manipulation; securing tomorrow by protecting technology today.

Keywords: Artificial Intelligence, Cybersecurity, Election Integrity, Data Protection

I. INTRODUCTION

The election of civic members to legislative positions is a cornerstone of democracy. This process is a crucial opportunity for voters to participate, at least indirectly, in the political process while helping shape the laws that affect their daily lives. The procedure leading up to elections, organization and conduct of elections, and the declaration and publication of results, are therefore extremely sensitive points in the democratic functioning of a state. Maintaining a high level of public confidence in these systems is essential in establishing legitimacy within the branches of power. Moreover, assurances of security in this mechanism helps to ensure the entire attribution of state power is beyond public reproach within a normal functioning society (Hariri, 2023). However, in the current geopolitical context of the information age, threats to election integrity and attempts to influence the resultant outcome have been greatly enhanced by threat actors.

It is equally important to maintain citizens' confidence in the fairness and integrity of elections; an essential component in ensuring sustainable security (McEvily, 1998). Over the past decade, social media platforms have been used to carry out significant media manipulation and disinformation campaigns related to elections. As a result, many nation states have introduced and implemented a strategic set of security measures to ensure the integrity of democratic elections. However, states are treading on thin ice; excessive interference in elections by government officials can also jeopardize the overall legitimacy of elections and threaten the right to freedom of expression.

II. PROPOSED INNOVATION

In many countries today, the electoral process, or certain elements of it, are being implemented digitally. In addition, the success of election campaigns is strongly linked to cyberspace, especially social media. This has led to a renewed focus of cyber threats in recent years to engage in the direct interference of elections in an attempt to manipulate the outcome by one party during the democratic processes. The unexpected ability by actors to change election results, on the other hand, has required a commitment towards more effective defenses against attempts to influence and delegitimization of election results combining more secure forms of cyber defenses (Roy et al., 2023), including *Artificial Intelligence* and *Machine Learning* (Bishop, 2006). Ensuring the sustainability of electoral legitimacy is an aspect that has a major impact on voters' faith and trust in democracy – a fact that is also highly vulnerable to misinformation, disinformation, and fake news from cyberspace.

In our presentation and paper, we will outline the methodology and theoretical framework necessary for election security combining the intersectionality of *Artificial Intelligence* and *Machine Learning* (Bishop, 2006) that integrates the requisite Cybersecurity defensive (Jajodia et al., 2018) measures needed to preserve voting integrity (Roy et al., 2023).

III. METHODS

In order to find the right balance of regulations, measures, and policies necessary to safeguard the election process, it is paramount that cooperation exists between states, political actors and social organizations. Using advanced *Artificial Intelligence* (AI) adaptation will allow the use of cutting-edge technologies and security measures (Jajodia et al., 2018) necessary to safeguard voting data and secure election integrity. The implementation of intelligent electioneering software combined with a secure *Machine Learning* (ML) (Bishop 2006) learning platform will enable the safe execution of the democratic voting process without fear of party interference. Working together will ensure measures taken by the government to provide oversite, intended to protect election security, will be accepted by the community as a positive, and not lead to a democratic deficit possessing the ability to ultimately fracture the populace and cause civil unrest.

In addition to the measures mentioned above, there will be direct analysis of the impact that (mis)Information and (dis)Information has on the outcome of voting and election outcomes. Using data from election polling and available from public, secondary data sources, we will assess information presented to end users (voters) through electronic mediums to determine if the data was able to manipulate the voter. This data includes, but is not limited to, online websites, social media platforms, social engagement applications, online gaming sites, etc. Moreover, we will attempt to determine, through both

Presented at the 2024 OkIP International Conference
on Artificial Intelligence Frontiers (CAIF)
in Oklahoma City, OK, USA, and Online, on April 3, 2024

qualitative and quantitative methodologies, whether the impact observed (if an impact was present) was *positive* (+), or *negative* (-), and how the extent of that impact had an overall effect on the end result of the election being investigated.

IV. Limitations

Limitations in this research include reduced access to official voting data from associated countries identified for exploration, including the United States and Hungry. Through reduced access to actual voting data we will be projecting extrapolated results from secondary data and user information.

- Reduced and limited access to official voting data
- Different voting regulations and procedural guidelines between the countries being examined will introduce limitations and challenges to guaranteeing data integrity during data collection.

V. Future Work

Future work will incorporate the introduction of a new regulatory framework, institutional powers, practices and public awareness programs in the United States and the European Union to combat (electoral) disinformation. Direct comparison of the United States and Hungarian regimes will allow us to introduce a theoretical construct of best practices for cognitive security (Roy et al., 2023) in civic elections.

VI. About the Authors

Joseph Squillace, Ph.D., is an Assistant Teaching Professor of Cybersecurity at Penn State University. Joseph received his Ph.D. in Information Systems (DISS) with a concentration in Information Security from the College of Engineering and Computing at Nova Southeastern University (NSU). Joseph's research interests include Cyberbullying, Cybersecurity, Privacy, Cybersecurity in Artificial Intelligence (AI), Secure Supply Chain, Data Integrity, and Economics of Information Security and Privacy Breaches. Joseph has previously published scholarly research in Cybersecurity, Artificial Intelligence, Privacy, Information Systems, Computer Science, the Internet of Things (IoT), and Climate Change domains.

Justice Cappella is a Senior Research Assistant attending Penn State University. Justice is graduating in May 2024 with a Bachelor of Science degree in Business Management and Marketing and a minor in Project Supply Chain Management. Justice's research interests include Business, (Secure) Supply Chain Management, Marketing, Cyberbullying, Cybercrime, and Climate Change, and she is currently collaborating on multiple research studies at Penn State Schuylkill.

References

Alawida, M., Shawar, B. A., Abiodun, O. I., Mehmood, A., & Omolara, A. E. (2023). "Unveiling the Dark Side of ChatGPT: Exploring Cyberattacks and Enhancing User Awareness." *Preprint* (non-peer reviewed version)

Bishop, M. (2006) "Pattern recognition and machine learning," *Springer*, 2006.

Chatzoglou, E., Karopoulos, G., Kambourakis, G., & Tsiatsikas, Z. (2023). "Bypassing antivirus detection: old-school malware, new tricks." *Preprint* (non-peer reviewed version)

Hariri, W. (2023). "Unlocking the Potential of ChatGPT: A Comprehensive Exploration of its Applications, Advantages, Limitations, and Future Directions in Natural Language Processing." *Preprint* (non-peer reviewed version)

Jain, A.K., Ross, A., Prabhakar, S. (2004). "An introduction to biometric recognition," *IEEE Transactions on Circuits and Systems for Video Technology, Vol. 14, No.* (1), pp. 4-20.

Jajodia, S., Liu, P., Swarup, V., Wang, C., and Wang, X. (2018). "Cybersecurity and supply chain management: Challenges and research opportunities," *IEEE Security & Privacy, Vol. 16, No.* (4), pp. 38-47.

Keromytis, A. D., and Stolfo, S. J. (2003). "Securing the supply chain," *IEEE Security & Privacy, Vol. 1, No.* 4, pp. 15-24.

Kanhere, S.S. and Zaveri, M. J. (2020). "A survey of security issues in machine learning," *IEEE Communications Surveys & Tutorials, Vol. 22, No.* 4, pp. 2751-2771.

McEvily, A. K. (1998). "The dark side of trust: When trust becomes a liability," *Academy of Management Review, Vol. 23, No.* 3, pp. 459-472.

Narayanan, A. and Shmatikov, V. (2008). "How to break anonymity of the Netflix prize dataset," *ACM Conference on Computer and Communications Security*, pp. 167-178.

Narayanan, A. and V. Shmatikov, V. (2009). "De-anonymizing social networks," *ACM Conference on Computer and Communications Security*, pp. 173-182.

Narayanan, A. and Shmatikov, V. (2010). "Myths and fallacies of "personally identifiable Information," *Communications of the ACM, vol.* 53, no. 6, pp. 24-26.

Roy, S. S., Naragam, K. V., & Nilizadeh, S. (2023). "Generating Phishing Attacks using ChatGPT." *Preprint* (non-peer reviewed version).