Cyber Security Experts Association of Nigeria (CSEAN)
Society for Multidisciplinary & Advanced Research Techniques (SMART)
West Midlands Open University
SMART Scientific Projects & Research Consortium (SMART SPaRC)
Sekinah-Hope Foundation for Female STEM Education
ICT University Foundations USA
Academic Innovations City University Foundations

Proceedings of the Cyber Secure Nigeria Conference – 2024

AI in Cyberwarfare: Impact of AI Automation and Data Weaponisation

[1]Hamzat Lateef (CISM), [2]Birma Markus Yakubu & [3]Abdulqadri Afolabi
[1&2]CyberPlural MSSP,
[3]Whitehat.NG Project, Abuja, FCT, Nigeria.
E-mails: [1]lateef.h@cyberplural.com; [2]b.markus@cyberplural.com; aa@projectwhitehat.ng
Phone: +234 815 454 4647; +234 706 660 2852; +234 811 815 0524.

ABSTRACT

This research focuses on the transformative power of Artificial Intelligence in modern cyberwarfare, in particular, its effects on AI automation and data weaponisation throughout the 2023 Nigerian presidential election. We have analysed the ways by which AI is redefining cyberspace operations and found both the potential benefits of the use of AI in such operations and the very serious security and ethical challenges brought forth. Using a four-step methodology, we identified current trends in AI and cyberwarfare, harvested and analysed over six million tweets relevant to the Nigerian election, and set the foundation for building an AI model whose objective is to mimic Nigerian communication styles to generate fake content. Our findings indicate that the potential of AI-generated disinformation to manipulate election results is downright terrifying. This means that policymakers must understand and regulate the use of AI in cyber warfare for national security protection.

Keywords: AI, Cyberwarfare, AI Automation, Data Weaponisation

Proceedings Citation Format
Hamzat Lateef (CISM), Birma Markus Yakubu & Abdulqadri Afolabi (2024): AI in Cyberwarfare: Impact of AI Automation and Data Weaponisation. Proceedings of the Cyber Secure Nigeria Conference held at The Ballroom Center, Central Business District, Federal Capital Territory, Abuja, Nigeria - 25th - 26th September, 2024. Pp 71-82.
https://cybersecurenigeria.org/conference-proceedings/volume-1-2024/ dx.doi.org/10.22624/AIMS/CSEAN-SMART2024P7

1. INTRODUCTION

In recent years, modern warfare has transformed significantly, driven by the rapid integration of Artificial Intelligence (AI) into military operations, particularly cyberwarfare (Hartmann & Giles, 2020). AI's capabilities have revolutionised strategies in cyber operations, affecting both offensive and defensive tactics.

AI-driven automation enables routine tasks, like monitoring network traffic, identifying vulnerabilities, and responding to threats, to be executed with unprecedented speed and efficiency. This not only frees human operators from more complex tasks but also reduces response times, crucial for countering evolving cyber threats. AI's adaptive nature amplifies its impact. Machine learning algorithms enable systems to learn from previous attacks and adjust tactics in real time, enhancing both offensive and defensive strategies. AI improves situational awareness in cyber warfare by analysing vast amounts of data in real time, aiding in proactive defence strategies and dynamic adjustments of cybersecurity measures.

However, integrating AI into cyberwarfare poses challenges and ethical considerations. Autonomous AI decision-making raises questions about accountability and unintended consequences. Balancing AI's security benefits with responsible use is crucial (Cristiano et al., 2023). A study by Cristiano et al. (2023) highlights the nuanced state of cyberspace, existing in a perpetual state of unpeace, marked by espionage, sabotage, and subversion. AI-driven automation and data weaponisation are pivotal in this transformation. AI-driven automation involves advanced algorithms and machine learning to streamline tasks like monitoring network traffic and identifying vulnerabilities (Malik, 2023). This enhances efficiency and allows human operators to focus on complex challenges (Masriadi et al., 2023). The collaboration between humans and AI strengthens cybersecurity frameworks, with AI enabling proactive defence mechanisms.

Data weaponisation, another key aspect, involves AI systematically analysing vast datasets to identify and exploit individual vulnerabilities. AI's analytical capabilities allow attackers to discern intricate patterns, making personalised, highly effective threats. AI continuously learns from past attacks, evolving its strategies, and challenging traditional cybersecurity measures. The personalised and adaptive nature of data weaponisation necessitates a reassessment of current cybersecurity strategies. Traditional defences often fail against these sophisticated threats, as evidenced by Ukraine's use of AI to identify Russian operatives and deploy autonomous drones (Bergengruen, 2024; Hambling, 2023). Generative AI introduces new threats, enabling cybercriminals to generate malware, create synthetic identities, and fabricate data for fraud, as seen with the OnlyFake platform (Lemonnier, 2024).

Generative AI's applications extend to creating realistic identification documents and facilitating financial fraud and unauthorised access. Nation-state actors exploit AI capabilities for malicious activities, as revealed by Microsoft Threat Intelligence and OpenAI, involving actors from China, Iran, North Korea, and Russia (Microsoft Threat Intelligence, 2024) and (Coker, 2024). AI automation and data weaponisation also influence geopolitical processes through disinformation. CrowdStrike predicts a significant AI impact on 2024 elections in various countries, including the U.S., Russia, India, and others, highlighting the manipulation potential for strategic gains. In summary, AI's integration into cyberwarfare brings transformative changes and ethical challenges. Understanding its implications is crucial for policymakers, military strategists, and cybersecurity experts navigating the evolving digital battleground.

1.1 Problem Statement

The evolving landscape of cyberspace, marked by a state of "unpeace" and grey zone conflicts, presents distinct challenges (Cristiano et al., 2023). The integration of AI into cyberwarfare reshapes conflicts, raising security and ethical concerns. AI-driven automation enhances response times and operational efficiency but raises ethical issues about accountability and unintended consequences. Data weaponisation, powered by AI, poses significant threats (Bergengruen, 2024). Personalised, adaptive attacks, as seen in the Russian/Ukraine conflict with Ukraine's use of Clearview AI and autonomous drones, challenge traditional cybersecurity measures (Hambling, 2023).

Generative AI enables cybercriminals to quickly generate sophisticated malware, create synthetic identities, and fabricate data for fraud (Lemonnier, 2024). Nation-state actors misuse AI services for malicious activities (Coker, 2024; Microsoft Threat Intelligence, 2024). The multifaceted impact of AI in cyberwarfare, from defensive enhancements to offensive threats, necessitates a comprehensive understanding. The challenge lies in balancing AI's benefits with responsible use, addressing ethical concerns, and formulating robust defence strategies to safeguard national security against evolving digital threats.

1.2 Aim and Objectives

This study aims to thoroughly investigate the implications of Artificial Intelligence (AI) capabilities in the domain of cyber warfare, specifically focusing on how AI automation and data weaponisation can impact Nigeria by analysing the trends on the global stage.
To achieve this, the following are the objectives

1. Analyse the global use of AI in cyberwarfare
2. Create an AI model and train it to act like a Nigerian to spread fake news on social media
3. Analyse the accuracy and possible impact on Nigeria's national security
4. Provide recommendations for Nigeria on how to utilise AI for national security

1.3 Scope of the Study

This study's scope includes a thorough investigation of the consequences of Artificial Intelligence (AI) capabilities in the field of cyber warfare, with a particular emphasis on how Nigeria is impacted by AI automation and data weaponisation. The study will examine how AI is transforming cyber operations' offensive and defensive strategies.

2. RELATED STUDIES

To understand cyberwarfare, we first define cyberspace and warfare. The North Atlantic Treaty Organization (NATO) describes cyberspace as "the global domain within the information environment, consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers" (Shea, 2018). The United Nations (UN) defines it as "the complex environment resulting from the interaction of people, software, and services on the Internet using technology devices and networks connected to it" (UNIDIR, 2014). Ivanova et al. (2022) add that cyberspace encompasses interconnected computer networks, information systems, and digital infrastructure, characterised by its global distribution, unique online behaviour rules, and potential for various harms.

Warfare, according to Britannica (2024), is the lawful use of force between countries, distinct from civil war, and governed by international laws such as the United Nations Charter and the Geneva Conventions. It must be conducted by lawful combatants with limited methods and means, avoiding civilian and neutral targets. The Cambridge Dictionary further defines warfare as the activity of fighting a war, including the weapons and methods used (Cambridge Dictionary, n.d.). Cyberwarfare, a concept without a single, universally accepted definition, involves using digital technology to carry out hostile actions against a country, group, or individual to cause harm.

This includes misinformation campaigns, disabling critical infrastructure, spreading malware, hacking, and electronic espionage. It can target various sectors, such as banking, military networks, government organisations, and essential utilities like communication and electricity grids. Cyberwarfare often combines offensive and defensive tactics and significantly impacts privacy, the economy, and national security. Some experts debate whether cyber warfare exists, as no single cyber-attack has been officially termed war (NATO, 2013).

Major international organisations, including the UN and NATO, acknowledge cyberspace's complexities and the potential for conflict within it. The UN focuses on promoting responsible state behaviour in cyberspace and developing norms for its peaceful use (UNIDIR, 2014), while NATO emphasises collective defence in cyberspace, recognising it as a potential conflict domain (NATO, 2023). Researchers, governments, and militaries often articulate cyberwarfare involving state and state-sponsored actors (Hodges & Creese, 2015). Wilcox (2018) suggests that the distinction between cyber warfare and other cyberattacks is contextual, with cyber warfare defined as cyberattacks within overt military engagements, like the Syrian war against the Islamic State or Russia's actions in the Russo-Georgian war and the annexation of Crimea. He contrasts this with clandestine nation-state cyber-attacks, such as alleged Russian operations in Eastern Ukraine, emphasising anonymity and non-attribution. Wilcox also highlights that Russia and China view cyber warfare as part of information warfare, using it in conjunction with or as a precursor to conventional military actions. To summarise it all, cyberwarfare involves using digital technology to conduct hostile actions, blending offensive and defensive tactics, significantly affecting privacy, the economy, and national security, and posing unique challenges to international law and governance.

2.1 History and Real-World Impact of Cyberwarfare

Cyberwarfare has evolved from theoretical discussions to a daily reality, impacting various sectors, including finance, education, health, and private businesses. The first recorded cyber-attack dates back to 1834 when two thieves hacked the French telegraph system to steal financial information (Monroe College, n.d.). In 1962, MIT student Allan Scherr exploited a punch card to print and share stored passwords, increasing computer access time (Monroe College, n.d.). In 1971, Bob Thomas created "Creeper," the first computer virus, as a security test (Kaspersky, n.d.). In 2007, Russia allegedly launched cyberattacks against Estonia, responding to perceived anti-Russian behaviour (KIRICHENKO, 2024). The discovery of Stuxnet in 2010 marked a significant milestone, as it targeted Iran's nuclear centrifuges, showcasing the destructive potential of cyberwarfare (Greenberg, 2019; Kushner, 2013). In 2012, the Shamoon malware attack on Saudi Aramco, allegedly by Iran, crippled its operations (James & Lee, 2015).

By 2014, nations had developed significant cyber capabilities. North Korea was accused of hacking Sony Pictures in retaliation for a film depicting an assassination plot against its leader (James & Lee, 2015). The Russia-Ukraine conflict has revealed multiple cyberattacks since 2015, including a historic blackout in 2015 and the deployment of Industroyer malware in 2016, highlighting the evolving cyber threat landscape (Greenberg, 2019). Ukraine War (2022-Present): This conflict has become a major battleground for cyberwarfare. Both sides have been accused of launching attacks. Ukraine has received significant cyber defence support from Western nations, while Russia has been accused of targeting critical infrastructure in Ukraine, such as power grids and communication networks (Duguin & Pavlova, 2023). Nagorno-Karabakh Conflict (2020):

During this renewed conflict between Armenia and Azerbaijan, both sides used cyberattacks to disrupt communication and military operations. For instance, Armenia reported denial-of-service attacks targeting government websites, while Azerbaijan faced attacks on its energy infrastructure (Chernobrov, 2022). Middle East Tensions: Cyberwarfare is increasingly used in proxy conflicts. For example, in 2019, Saudi Arabia's Aramco oil facilities were targeted by a sophisticated cyberattack, with some attributing it to Iran as part of ongoing regional tensions (Al-Rawi, 2021).

Africa is becoming a target for nation-state cyberattacks, potentially as a testing ground or to disrupt regional stability. April 2024 A report by cybersecurity firm Performanta highlighted a rise in financial trojan attacks targeting Kenyan and Nigerian banks, potentially linked to broader geopolitical aims (Golan, 2024). Evolving Tactics: Cyberattacks are becoming more sophisticated, targeting critical infrastructure and financial systems. In early 2023, Reports emerged of a potential cyberattack disrupting operations at a major port in an undisclosed African nation. The attack's origin and targets remain unclear, but it highlights the growing risk to African infrastructure (PTSecurity, 2023).

2.2 The Impact of AI on Cyberwarfare

The integration of artificial intelligence (AI) into cyberwarfare has transformed modern conflict and defence strategies. AI algorithms analyse vast datasets, detect patterns, and make real-time decisions, enhancing both offensive and defensive capabilities. AI-powered systems improve cyber defences through predictive analytics, anomaly detection, and automated incident response, helping to pre-emptively mitigate threats (TAHIR, 2024). However, the rise of AI in cyberwarfare also introduces challenges and ethical concerns. AI's potential misuse by malicious actors necessitates robust safeguards and regulations. The anonymity and global reach of cyberspace allow sophisticated attacks with minimal risk of attribution, complicating defence efforts. International collaboration and investment in AI research are essential for building resilient cyber defences (Yu, 2023).

The National Cyber Power Index 2022 identifies over 30 countries with developed cyber power, with the United States, China, Russia, the UK, Australia, the Netherlands, South Korea, Vietnam, France, and Iran being the top 10 (Voo et al., 2022). Nations are increasingly collaborating to enhance their cyber capabilities using AI. For instance, France and Singapore's ministries are jointly developing AI capabilities for cyber defence (Yu, 2023). Nation-state actors leverage AI to enhance cyber capabilities.

For example, Russia's Forest Blizzard uses AI for open-source research on sensitive technologies, while North Korea's Emerald Sleet employs AI for reconnaissance and phishing campaigns. Iran's Crimson Sandstorm utilizes AI for malware development and phishing, and Chinese groups Charcoal Typhoon and Salmon Typhoon use AI for vulnerability research and attack orchestration (digiALERT, 2024; Microsoft Threat Intelligence, 2024). These trends underscore AI's significant role in modern cyberwarfare, facilitating sophisticated and automated cyber operations.

3. METHODOLOGY

For this study, we use a 4-step methodology.

1. Current Trends Review: We checked out current trends of AI and cyberwarfare, and how AI is using data to change the norm in the cyberwarfare domain.
2. Data Collection: The data was collected from Twitter (now X) using their API. This data collection exercise was focused on tweets emanating from Nigeria on the subject of the 2023 presidential election. This was a data collection exercise to determine what effect this collection of datasets, if weaponised, would have on election results.
3. Data Analysis: Very good data analysis was done on the data that was collected to derive the most valuable information out of it. We used analytical methods that helped ensure the data was not only accurate and relevant but also related specifically to the Nigerian 2023 presidential election.
4. Model Development Roadmap: A futuristic road map to use this data to help train a model that will help mimic a Nigerian. This model is oriented toward generating content for social media posting, with the output closely resembling genuine Nigerian communication styles.

4. RESULTS DISCUSSION

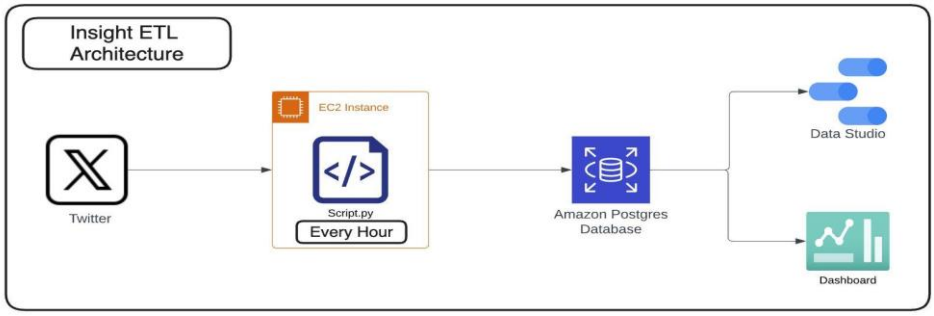

Figure 1. Insight ETL Architecture

We built an ETL architecture to collect tweets relating to conversations on Twitter (now X) focused on the Nigerian 2023 General Elections. The collection was between September 2022 and January 2023, and a total of over 600K user data points were collected that contributed to almost 6 million Tweets across 16 query tags, which were used for the collection.

	table_name [PK] text	row_count integer	latest_record_time timestamp without time zone	last_loaded_time timestamp without time zone
1	user_data	612847	2023-03-03 17:14:46.559502	2023-03-03 17:14:52.216719
2	tweet_data	5945400	2023-03-03 17:14:17	2023-03-03 17:14:54.579444

Figure 2. Collected Data Summary

As shown in the hit map below, activities of tweet data collected for those periods, aligning that to the various candidates on the presidential ballot for the major parties contesting the election

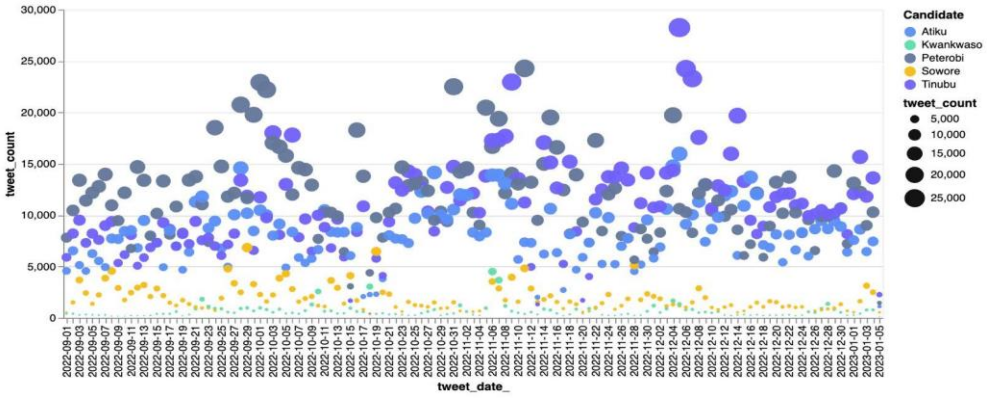

Figure 3. Tweet Data Activities Collected over a Period.

Currently, we have processed the tweet data to extract sentiment analysis, user data such as username, account description, and account creation date and informed when participating users' accounts were created, stipulating months and years, devices from which most tweets came, helping identify bots' participations. Below is the tweet sentiment graph for each of the leading candidates, indicating the volume of tweets in each category of sentiments: positive, negative and neutral. Over 25% of the tweet data across the board for all leading candidates falls into the negative sentiment, showcasing a high level of cyberbullying present online during this period.

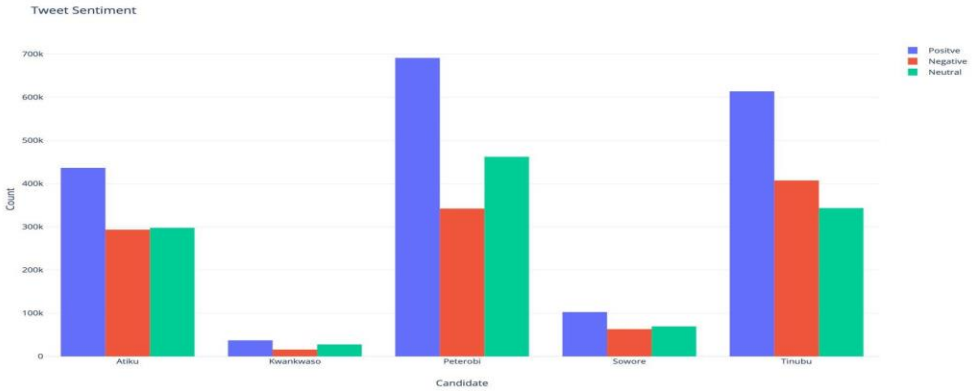

Figure 4. Tweet Sentiment Graph

Another great observation is information that can be grabbed from the user data collected during this period, where some part of the information suggests that the majority of the user accounts that participated were heavily registered during the year 2022 and fewer contributions from users from 2009.

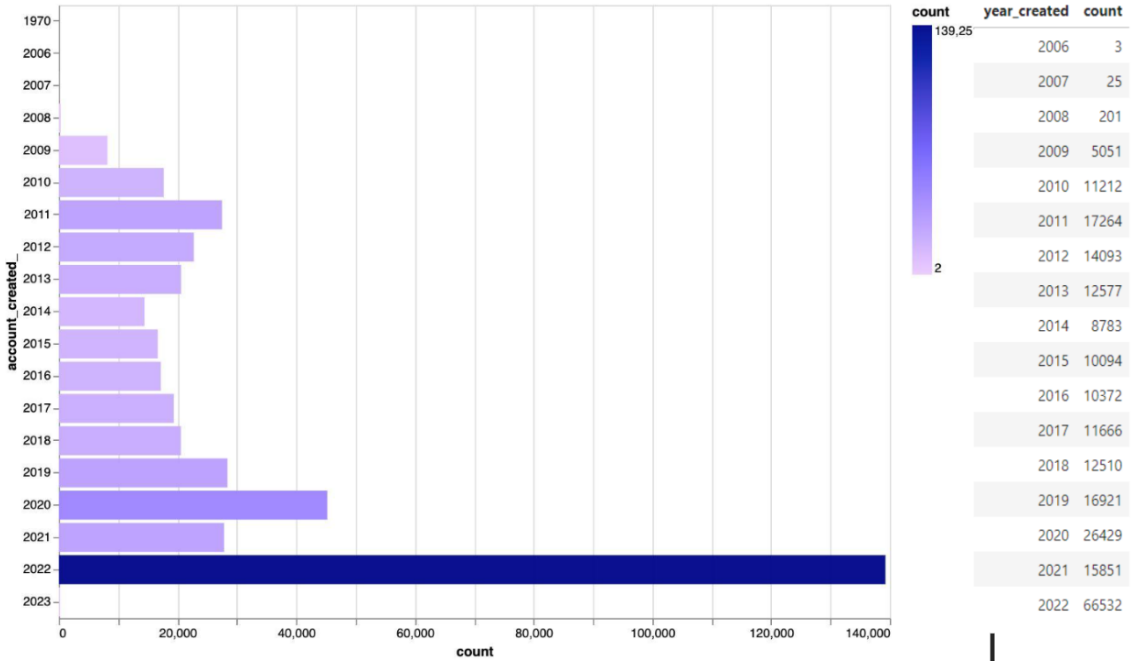

Figure 5. Registration Timeline for Participating Accounts

User Data – 2022 Creation Month

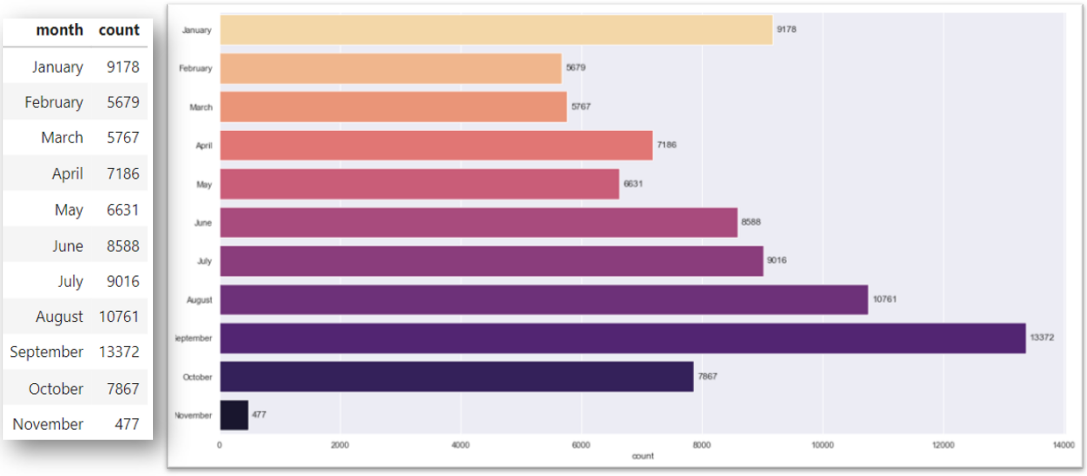

Figure 6. 2022 Monthly Registration Spread.

We took a deeper dive into the user data and matched contributions to monthly for users, based on the tweet volumes collected and we have the following top users across the conversations for the selected period. This indicated how much tweet data was being created by top-rated users, as Android devices contributed more within that period (an average of 30 tweets on a daily basis), just imagine AAI-powered capability is available to these users, we believe them to be able to generate 5X of any number that was currently generated.

Figure 7. Top Contributing Users on Monthly Breakdown

Figure 8. Tweets Emanating from Devices Summary

We currently have this dataset, and as part of future research, we are building a model (algorithm) that will be AI-powered to generate tweet data for upcoming elections based on the training with the current data set that is no longer available in the public as they were collected in real-time (only available with X, and coupled with the fact that some tweets and user data might have been deleted). Our team believes that this can be weaponised in future elections. Imagine focusing on extracting tweet data with only negative sentiments and using it to train a model, enabling auto-generations and responses. We hope to see our model generate some of the sample tweets in the future when fed and trained with a negative sentiment tweets block.

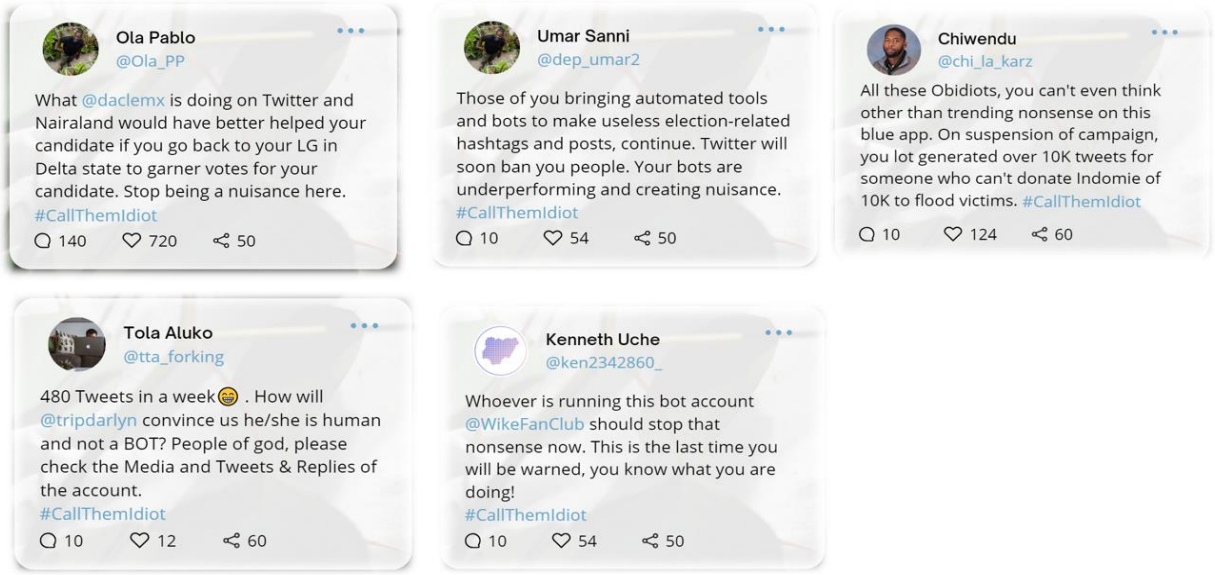

Figure 9. Sample Tweets that can be generated from Model

5. FUTURE WORK

Future research will be aimed at developing an AI-enabled model that can help to illustrate the potential ways in which social media data may be weaponised in elections, using insights from the 2023 Nigerian presidential election. This will include the generation of synthetic content driven by sentiments that stimulate AI-driven disinformation campaigns. We will also inform policymakers of the potential of these AI technologies and guide them in implementing effective regulations to keep national security safe and maintain the integrity of democratic processes.

REFERENCES

Al-Rawi, A. (2021). Cyberwars in the Middle East. *Cyberwars in the Middle East*, *January*. https://doi.org/10.36019/9781978810143

Bergengruen, V. (2024). *How Tech Giants Turned Ukraine Into an AI War Lab*. https://time.com/6691662/ai-ukraine-war-palantir/

Britannica. (2024). *Legally defining war*. https://www.britannica.com/topic/law-of-war/Legally-defining-war

Cambridge Dictionary. (n.d.). *warfare*. https://dictionary.cambridge.org/dictionary/english/warfare

Chernobrov, D. (2022). Diasporas as cyberwarriors: Infopolitics, participatory warfare and the 2020 Karabakh war. *International Affairs*, *98*(2), 631–651. https://doi.org/10.1093/ia/iiac015

Coker, J. (2024). *Microsoft, OpenAI Confirm Nation-States are Weaponizing Generative AI in Cyber-Attacks*. https://www.infosecurity-magazine.com/news/microsoft-nation-states-gen-ai/

Cristiano, F., Broeders, D., Delerue, F., Douzet, F., & Géry, A. (2023). Artificial intelligence and international conflict in cyberspace. *Artificial Intelligence and International Conflict in Cyberspace*, 1–15. https://doi.org/10.4324/9781003284093-1

digiALERT. (2024). *The Rise of Nation-State Actors: Exploring the Intersection of AI and Cyber Warfare*. https://www.linkedin.com/pulse/rise-nation-state-actors-exploring-intersection-ai-cyber-warfare-woarc/

Duguin, S., & Pavlova, P. (2023). The role of cyber in the Russian war against Ukraine: Its impact and the consequences for the future of armed conflict. *EU Directorate General For External Polices*, *September*.

Golan, G. (2024). *CYBER WARFARE CY RFARE CYBER WARFA Expert analysis on nation*. https://www.performanta.com/_files//ugd/4c1ac7_8c1bf90e7cff4ab39e9ad4defacb5e0b.pdf?utm_medium=email&_hsenc=p2ANqtz-9SSjnNk2uWXx2CI06i7Ssh0oz7_oDV2vOtXrNBrQV2XtzNAU00MfBFrCO_aqImrEZJ7_DcAU29XN87cULp4RDR4c-DuSjB1ve5vi2V0IQtFGn_GB8&_hsmi=86579699&utm_content=86579699&utm_source=hs_automation

Greenberg, A. (2019). *The WIRED Guide to Cyberwar*. https://www.wired.com/story/cyberwar-guide/

Hambling, D. (2023). *Ukraine's AI Drones Seek and Attack Russian Forces Without Human Oversight*. https://www.forbes.com/sites/davidhambling/2023/10/17/ukraines-ai-drones-seek-and-attack-russian-forces-without-human-oversight/?sh=60b9e00e66da

Hartmann, K., & Giles, K. (2020). The Next Generation of Cyber-Enabled Information Warfare. *2020 12th International Conference on Cyber Conflict (CyCon)*, *1300*, 233–250. https://doi.org/10.23919/CyCon49761.2020.9131716

Hodges, D., & Creese, S. (2015). *Cyber Warfare: A Multidisciplinary Analysis*.

Ivanova, K. A., Myltykbaev, M. Z., & Shtodina, D. D. (2022). The concept of cyberspace in international law. *Law Enforcement Review*, *6*(4), 32–44. https://doi.org/10.52468/2542-1514.2022.6(4).32-44

James, E. St., & Lee, T. B. (2015). *The 2014 Sony hacks, explained*. https://www.vox.com/2015/1/20/18089084/sony-hack-north-korea

Kaspersky. (n.d.). *A Brief History of Computer Viruses & What the Future Holds*. Retrieved March 29, 2024, from https://www.kaspersky.com/resource-center/threats/a-brief-history-of-computer-viruses-and-what-the-future-holds

KIRICHENKO, D. (2024). *Lessons and warnings from world's first all-out cyberwar*. https://asiatimes.com/2024/02/lessons-and-warnings-from-worlds-first-all-out-cyberwar/#:~:text=Starting in Estonia in 2007,out cyberwar against the country.

Kushner, D. (2013). The real story of stuxnet. *IEEE Spectrum*, *50*(3), 48–53. https://doi.org/10.1109/MSPEC.2013.6471059

Lemonnier, J. (2024). *The truth about OnlyFake and generative AI fraud*. https://resistant.ai/blog/onlyfake-generative-ai-fraud?utm_campaign=newsletter_feb_2024&utm_medium=email&_hsmi=295867715&_hsenc=p2ANqtz--IufnC78stwRkKj_TIuXNNG5CK3k1FJQObpOPVBnCbYCtI3t82J150B2oMjk72QIkaxTm3O0DN6-_2R7C0LFR1j91KwQ&utm_source=newsletter

Malik, M. (2023). *AI IN WARFARE : THE AUTOMATION OF KILL CYCLE*. *October*.

Masriadi, Dasmadi, Ekaningrum, N. E., Hidayat, M. S., & Yuliaty, F. (2023). Exploring the Future of Work: Impact of Automation and Artificial Intelligence on Employment. *Endless: International Journal of Future Studies*, *6*(1), 125–136. https://doi.org/10.54783/endlessjournal.v6i1.131

Microsoft Threat Intelligence. (2024). *Staying ahead of threat actors in the age of AI*. https://www.microsoft.com/en-us/security/blog/2024/02/14/staying-ahead-of-threat-actors-in-the-age-of-ai/

Monroe College. (n.d.). *CYBERSECURITY HISTORY: HACKING & DATA BREACHES*. Retrieved March 29, 2024, from https://www.monroecollege.edu/news/cybersecurity-history-hacking-data-breaches#:~:text=Technically%2C the very first cyberattack,that things got really interesting.

NATO. (2013). *Cyberwar - does it exist?* https://www.nato.int/docu/review/articles/2013/06/13/cyberwar-does-it-exist/index.html

NATO, N. A. T. O. (2023). *Cyber Defence - блог об информационной безопасности*. https://www.nato.int/cps/en/natohq/topics_78170.htm#:~:text=NATO's focus in cyber defence,political consultation and collective action.

PTSecurity. (2023). *Cybersecurity threatscape of African countries 2022–2023*. https://www.ptsecurity.com/ww-en/analytics/africa-cybersecurity-threatscape-2022-2023/

Shea, J. (2018). Cyberspace as a Domain of Operations: What Is NATO's Vision and Strategy? *MCU Journal*, *9*(2), 133–150. https://doi.org/10.21140/mcuj.2018090208

TAHIR, F. (2024). *5 Countries with Cyber Warfare Capabilities*. https://www.insidermonkey.com/blog/5-countries-with-cyber-warfare-capabilities-1265658/

UNIDIR. (2014). The United Nations, Cyberspace and International Peace and Security Responding to Complexity in the 21st Century. *Towards Mutual Security*, 351–356. https://doi.org/10.13109/9783666300547.351

Voo, J., Hemani, I., & Cassidy, D. (2022). *National Cyber Power Index 2022*. *September*, 1–66. www.belfercenter.org/project/cyber-project%0Ahttps://www.belfercenter.org/sites/default/files/files/publication/Cyber Project_National Cyber Power Index 2022_v3_220922.pdf

Wilcox, P. (2018). *Drawing the line for cyber warfare*. https://www.computerweekly.com/opinion/Drawing-the-line-for-cyber-warfare?_gl=1*1s8sxvs*_ga*MTY5MTIxMTI2OS4xNzEwMjgwOTEw*_ga_TQKE4GS5P9*MTcxMDI4MDkwOC4xLjEuMTcxMDI4MDkxMC4wLjAuMA..

Yu, E. (2023). *These two countries are teaming up to develop AI for cybersecurity*. https://www.zdnet.com/article/these-two-countries-are-teaming-up-to-develop-ai-for-cybersecurity/