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

A Modern Perspective on the Impact of Artificial Intelligence on Cyber Diplomacy

Moses Joshua
Cybersecurity Education Initiative
E-mail: mosesjoshua72@gmail.com
Phone: +2348067017054

ABSTRACT

This paper is a critical review that examines the evolution and impact of cyber diplomacy, with a specific focus on the role of artificial intelligence (AI) in shaping international cybersecurity strategies. It explores how AI, driven by advances in data availability, computing power, and algorithms, is transforming cybersecurity by enhancing threat detection and response capabilities while also introducing new risks such as AI-driven cyberattacks. The review highlights the dual role of AI in both advancing and complicating cyber diplomacy and discusses various international frameworks aimed at addressing these challenges. It reinforces the need for a unified global approach to balance AI's benefits with its potential risks and advocates for integrated regional and global cybersecurity efforts to stimulate resilient international cyber diplomacy.

Keywords: Cyber Diplomacy, Artificial Intelligence, Cybersecurity, International Cooperation

Proceedings Citation Format
Moses Joshua (2024): A Modern Perspective on the Impact of Artificial Intelligence on Cyber Diplomacy 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 165-174. https://cybersecurenigeria.org/conference-proceedings/volume-1-2024/
dx.doi.org/10.22624/AIMS/CSEAN-SMART2024P15

1. INTRODUCTION

Diplomatic efforts in international relations have become a critical aspect of global security in today's interconnected world (Prantl & Goh, 2022). The emergence of cyber diplomacy can be traced back to 2007 (Kello, 2024), following a significant cyberattack on Estonia, one of Europe's most digitally advanced nations (CÎRNU et al., 2024). The attack severely disrupted computer networks, paralysing numerous government and corporate websites.

This event accelerated the urgency for governments to develop national cybersecurity strategies, recognising that cyberspace, much like the physical world, holds military and strategic importance, necessitating international cooperation to combat cyber threats (CÎRNU et al., 2024). Cyberattacks are increasingly characterised by sophisticated, strategic threats that extend beyond conventional physical terrorism (Colajanni & Marchetti, 2021). As global progress, democracy and peace are at risk, cyber diplomacy has become a viral component of foreign policy (Zamanli, 2022). Its interdisciplinary nature involves a range of factors, including policies, politics, sociology, digital science, diplomacy, multilateralism and historical context, making it essential for nations to address these issues collaboratively (Radanliev, 2024).

The rapid advancement of artificial intelligence (AI) is driven by key technological enablers and is already having a profound impact on daily life and work. As AI continues to evolve, it will likely bring significant economic and social changes. To fully harness AI's benefits while minimising its negative effects, coordinated efforts from diverse stakeholders are essential (Feijóo et al., 2020). National variations in political, economic, and cultural frameworks will shape how AI affects areas such as privacy, efficiency, and surveillance. Countries competing in AI development may face geopolitical tensions, as leading nations stand to gain considerable economic and political power. However, this rivalry could also risk global fragmentation, hindering technological progress (Egon et al., 2023).

While decentralisation in AI development could encourage innovation and balance power, international cooperation is vital to address the broader governance, ethical, and cultural challenges posed by AI. Stronger collaboration among governments, private sectors, and academic bodies is necessary to manage AI's far-reaching effects (Bremmer & Suleyman, 2023). Advancing the concept of technology diplomacy can promote global alignment in AI policy, ensuring its development benefits humanity while preventing malicious uses.

1.2 Objectives

1. **Examine the Role of Artificial Intelligence (AI) in Cyber Diplomacy** - Analyse how AI influences international cybersecurity strategies.
2. **Evaluate Opportunities and Benefits** - Identify the advantages AI offers in enhancing cybersecurity through cyber diplomacy.
3. **Assess Risks and Challenges** - Discuss the potential threats AI introduces, including AI-driven cyberattacks and ethical concerns.
4. **Explore International Cooperation** - Highlight the importance of global collaboration in managing AI-related cybersecurity risks.
5. **Provide Policy Recommendations** - Suggest strategies for balancing AI opportunities and risks in cyber diplomacy.

2. THE EVOLUTION OF CYBER DIPLOMACY

2.1 Diplomacy

Diplomacy is commonly defined as the process of negotiating between state representatives (Nyakomitah, 2023). It is an interdisciplinary field that has attracted attention from various research areas, including social science (Oosthuizen, 2024), global affairs (Vasiloiu, 2023), and politics (Carrapico & Farrand, 2024). Diplomacy today faces numerous challenges.

One key issue is the "international responsibility to protect," alongside immigration and emigration, which are considered major diplomatic concerns worldwide (Vasiloiu, 2023). The COVID-19 pandemic has significantly tested governments around the globe (Rocco et al., 2024).

Nations must recognise that their economies, global competitiveness, and cybersecurity heavily depend on a secure and stable cyberspace. Internet access and the integration of emerging technologies have become priorities on political agendas globally, whether the countries in question are cyber powers (e.g., the United States, China, Russia, France, Israel, the United Kingdom) or simply consumers of internet-based technologies (Sutter, 2020).

In modern diplomacy, issues such as sustainable development, environmental concerns, global pandemics, economic challenges, and the growth of international law are key priorities (Vasiloiu, 2023). Over the past two decades, cyber diplomacy has emerged as an important addition to these existing challenges (Chiriatti, 2023).

2.2 Cyber Diplomacy

Cyberspace offers digital tools that enhance the effectiveness of diplomatic strategies, while also enabling the development of various government-led initiatives that benefit from the diplomat's traditional techniques and mindset (Glluccio, 2021). The distinction between traditional diplomacy and cyber diplomacy is clear: when cyberspace issues are central to diplomatic efforts, it is classified as cyber diplomacy. Cyber diplomacy applies diplomatic tools and approaches to address challenges stemming from the international use of cyberspace (Alethawy, 2022). It involves both the use of cyber tools to advance broader diplomatic objectives and the application of diplomatic strategies to analyse and manage cyberspace-related problems—activities that are distinct yet interconnected.

Another related term is digital diplomacy, also known as "e-Diplomacy" or "Diplomacy 2.0" (Randaliev, 2024), which can also be referred to as contemporary diplomacy. This involves the use of social media, online platforms, and digital technologies by governments and diplomats to engage with global audiences, encourage communication, and conduct diplomatic outreach (Randaliev, 2024, p. 4). Randaliev (2024) explains that digital diplomacy is a broader concept focused on the use of technology for achieving diplomatic goals, whereas cyber diplomacy specifically deals with cyberspace issues and security.

2.3 The Paris Call

The Paris Call for Cyber Peace is a cyber diplomacy initiative launched by France (Lété, 2022), announced by President Emmanuel Macron during a speech at the "Internet of Trust" event on November 12, 2018, at UNESCO in Paris. UN Secretary-General António Guterres was present during the event.

This initiative followed the 2017 efforts of the UN Group of Governmental Experts (GGE), which failed to reach a consensus (Lété, 2022). The Paris Call is a significant cyber diplomacy effort positioning France as a leading advocate of soft power (Novanto et al., 2021) in international cyber relations, a concept introduced by Joseph Nye (2022). It emphasises the importance of cybersecurity in global diplomatic relations, as reflected in the EU-NATO collective Cyber Defence strategies, which prioritise national cybersecurity (Pijpers, 2021).

3. THE IMPACT OF ARTIFICIAL INTELLIGENCE (AI) ON CYBER DIPLOMACY

3.1 A Short Story on AI

Feijóo et al. (2020) highlight that several key factors drive the rapid advancement of artificial intelligence (AI): (i) the vast increase in data available for training machine learning models; (ii) enhanced computing power that supports deep neural networks and various learning methodologies; (iii) improvements in algorithms that significantly boost machines' ability to tackle diverse problems across different sectors; (iv) the long-term accumulation of software as a cultural and technological asset; and (v) the swift decline in costs, which has made complementary technologies—such as ubiquitous connectivity, pervasive computing, and the Internet of Things (IoT)—more accessible.

While technology has not yet achieved "strong" AI that matches human cognitive abilities (Korteling et al., 2021), the emergence of increasingly advanced "weak" AI systems designed for specific tasks has gained considerable strength. As a result, AI is becoming deeply integrated into business and everyday life, fundamentally altering operations, markets, and entire industries (Loureiro et al., 2021). Experts and analysts liken this transformation to a new industrial revolution, emphasising its potential to reshape economies and societies (Rymarczyk, 2020). AI is set to redefine our understanding of productivity, our interactions with the environment, and aspects of national power. Historically, nations that have harnessed technology effectively during previous industrial revolutions gained significant power and influence; similarly, AI could emerge as a pivotal factor on the global stage.

A competitive race for AI technological breakthroughs is already underway, particularly among the United States, China, and, more recently, the European Union, along with countries like South Korea, Japan, Russia, and India (Brattberg et al., 2020). The prevailing expectation is that the nations that lead in AI will dominate economically and geopolitically in the coming decades (Grochmalski, 2020). A comprehensive evaluation indicates that while the United States and, to a lesser degree, the EU hold advantageous positions in research and innovation, China is leveraging its early lead in practical applications and consumer use cases (Lundavall & Rikap, 2022).

3.2 AI in Cyber Diplomacy

Artificial intelligence (AI) is set to profoundly influence the cyber domain, shaping the offensive and defensive capabilities of both state and non-state actors (De Azambuja et al., 2023). On one hand, AI can enhance cybersecurity through predictive models that anticipate attacks and sophisticated encryption methods that protect data even during breaches. Conversely, it also introduces risks, as it may be used to execute sophisticated cyberattacks or develop autonomous cyber weapons that can cause physical harm.

In cybersecurity, AI's capacity to process large volumes of data and identify threats positions it as a transformative force. By analysing technical events and human behaviours, AI can uncover vulnerabilities, predict phishing targets, and create profiles that help detect deviations from normal patterns. This enables AI to identify weaknesses in networks and systems, offering significant advantages in both offensive and defensive strategies (Nair et al., 2024).

AI's importance in predictive cybersecurity is particularly notable in countering complex threats like botnets, which may also use AI technologies. It can differentiate between legitimate and malicious bots (Nair et al., 2024), allowing for more effective responses than traditional methods. Moreover, by establishing behaviour baselines and continuously learning from them, AI can detect subtle anomalies that might indicate malware or ransomware activity. This proactive approach significantly enhances threat detection and response capabilities, making AI an essential tool for staying ahead of cybercriminals and improving automated threat mitigation. Incorporating all this into cyber diplomacy, AI presents a dual challenge: while it improves defences, it also calls for international collaboration to regulate its application and prevent AI-driven cyber warfare, ensuring responsible and secure use.

3.3 Opportunities and Benefits

AI presents substantial potential for advancing cyber diplomacy, particularly in areas like threat intelligence, negotiation, disarmament, and conflict resolution (Randaliev, 2023). Its ability to analyse vast datasets enhances decision-making and drives innovative solutions to global cybersecurity challenges. In threat intelligence, AI processes data in real time, automating threat detection and enabling timely defensive strategies for governments and diplomats. In negotiations, AI identifies mutual interests and proposes balanced compromises, making treaty discussions more efficient. For disarmament, AI automates compliance monitoring, facilitating trust and ensuring adherence to disarmament agreements. AI also supports conflict resolution by mediating cyber disputes, assessing resolutions, and proposing long-term peace strategies, addressing both technical and political aspects.

3.4 Challenges and Ethical Concerns

AI can amplify cyber threats as criminal groups, ideological factions, and state-sponsored hackers may exploit it to spread misinformation, bypass security, and evade detection. Despite its cybersecurity advantages, AI is vulnerable to manipulation, leading to erroneous outcomes (Carrol et al., 2023; Tarsney, 2024). This dual-use nature serves both offensive and defensive purposes.

In 2021, the U.S. invested over $6 billion in AI research (Harper, 2021), while China's AI spending is estimated in the tens of billions, with some regional governments committing approximately USD 14.7 billion each (Allen, 2019), but hastily implementing AI systems without proper validation poses risks. In unstable environments, AI may make harmful decisions. Data poisoning attacks can distort AI algorithms, disrupting military operations and escalating conflicts if decisions are left to AI systems (Cotroneo et al., 2024; Ferrara, 2023). AI's logical decision-making lacks human intuition, making it risky in complex scenarios like warfare. Moreover, integrating AI across military coalitions with varying technologies presents significant challenges, potentially leading to operational failures.

3.5 International Cooperation

AI advancements are intensifying the competition between offensive cyberattacks and defensive cybersecurity measures, heightening the risk of global cyber conflicts. Both state and non-state actors are using AI, raising concerns about the potential militarisation of cyberspace and threats to critical infrastructures like nuclear facilities and satellite communications. AI's offensive capabilities could escalate conflicts beyond state control, and its defensive use could skew government priorities away from collective human interests.

On a macroeconomic level, AI will shape industries and national competitiveness, with countries that fail to adopt AI falling behind. This shift may worsen global inequalities, leading to "data colonialism" (Harari, 2019) and threatening low-cost labour economies as automation increases. The race for AI talent could fuel political fragmentation and economic displacement, further intensified by fragmented policies on skilled labour mobility. The possibility of an AI arms race (Waizel, 2024; Sarkin & Sotoudehfar, 2024; Blumenthal, 2023) is concerning due to the absence of global AI regulations (Guha et al., 2023), making the development and deployment of malicious AI easier. Beyond cybersecurity, AI poses risks in surveillance, social manipulation, and lethal autonomous weapons, threatening global stability and undermining democratic institutions (Coeckelbergh, 2023; Kreps & Kriner, 2023).

4. POLICY RECOMMENDATIONS

4.1 Balancing Opportunities and Risks

Feijóo et al. (2020) argue that the differing political, strategic, and ethical views on AI across major nations, such as China, the U.S., the EU, India, Japan, South Korea, and Russia, risk limiting AI's global potential. Initiatives by organisations like the UN, IEEE, OpenAI, and Data Pop Alliance aim to address AI's challenges but often remain confined within specific regions or sectors (Butcher & Beridze, 2019). For example, the EU focuses on ethical AI within its borders, seeking to balance surveillance with democratic values. While these efforts are important, a unified international dialogue is needed to create a comprehensive framework that integrates human rights, ethics, legal, economic, and social considerations.

"New technology diplomacy" (Feijóo et al., 2020; Adler-Nissen, 2022) could merge fragmented initiatives, promote collaboration, mutual learning, and harmonisation, while still recognising competition and varying policy approaches. International collaboration models, such as internet governance (Pigatto et al., 2021), offer benefits by reducing adversarial costs and stimulating synergy to mitigate AI risks. However, AI's global impact demands a more adaptable international framework (Radu, 2021). This diplomacy should involve a broad range of stakeholders—including governments, industry, academia, and civil society—to build trust and establish leadership, possibly starting with informal initiatives and progressing to a global conference or organisation. This diplomatic effort must address both overarching AI issues and sector-specific applications, balancing civil liberties with security concerns.

4.2 Frameworks for Global Cooperation

Integrating regional and global cybersecurity frameworks is vital for effective cyber diplomacy. ASEAN CERT highlights Southeast Asia's commitment to cybersecurity through collaboration, while ENISA strengthens EU cybersecurity but could benefit from a broader perspective (Rui, 2023; Dunn Cavelty & Smeets, 2023). The OAS aids cybersecurity in the Americas by promoting best practices (ASSEMBLY, 2020). Globally, the GFCE and GCI facilitate international cooperation and improve national strategies (Ruhl et al., 2022; ITU, 2024). Aligning these frameworks to address AI challenges can establish unified standards and strengthen global responses to AI-driven cyber threats.

5. CONCLUSION

Cyber diplomacy is not just a technical issue. While technical experts have shaped cyberspace, relying on them alone may leave governments unprepared for broader security and power challenges. AI offers significant potential for transforming work and daily life but also presents risks of misuse. This paper emphasises three key points: the critical role of cyber diplomacy in global relations, AI's impact on cybersecurity, and the need for international cooperation to manage AI risks. As AI evolves, its influence on cyber diplomacy will grow, potentially reshaping power dynamics. Continued collaboration and research are essential for developing policies that ensure global stability and cybersecurity.

REFERENCES

1. Adler-Nissen, R., & Eggeling, K. A. (2022). Blended diplomacy: the entanglement and contestation of digital technologies in everyday diplomatic practice. European Journal of International Relations, 28(3), 640-666.
2. Alethawy, M. (2022). Digital Diplomacy and Cybersecurity. Ahi Evran Akademi, 3(1), 82-90.
3. Allen, G. C. (2019). Understanding China's AI strategy. Centre for a New American Security. https://www.cnas.org/publications/reports/understanding-chinas-ai-strategy
4. ASSEMBLY, G. (2020). Organisation of American States—OAS. Organisation.
5. Blumenthal, R. (2023). What Pausing the AI Arms Race is and isn't: the Right Side of History or Wishful Thinking. ACM SIGCAS Computers and Society, 52(1), 23-26.
6. Brattberg, E., Rugova, V., & Csernatoni, R. (2020). Europe and AI: Leading, lagging behind, or carving its own way? (Vol. 9). Washington, DC, USA: Carnegie endowment for international peace.
7. Bremmer, I., & Suleyman, M. (2023). The AI power paradox: Can states learn to govern artificial intelligence-before it's too late? Foreign Aff., 102, 26.
8. Butcher, J., & Beridze, I. (2019). What is the state of artificial intelligence governance globally? The RUSI Journal, 164(5-6), 88-96.
9. Carrapico, H., & Farrand, B. (2024). Cybersecurity Trends in the European Union: Regulatory Mercantilism and the Digitalisation of Geopolitics. JCMS: Journal of Common Market Studies.
10. Carroll, M., Chan, A., Ashton, H., & Krueger, D. (2023, October). Characterising manipulation from AI systems. In Proceedings of the 3rd ACM Conference on Equity and Access in Algorithms, Mechanisms, and Optimization (pp. 1-13).
11. Chiriatti, A. (2023). Virtual Diplomacy as a New Frontier of International Dialogue. In Diplomacy, Society and the COVID-19 Challenge (pp. 39-46). Routledge.
12. CÎRNU, C. E., Rotuna, C. I., & Vasiloiu, I. C. (2023). Comparative Analysis on Cyber Diplomacy in EU and US. ROCYS, 5(1), 77-86.
13. Coeckelbergh, M. (2023). Democracy, epistemic agency, and AI: political epistemology in times of artificial intelligence. AI and Ethics, 3(4), 1341-1350.

14. Colajanni, M., & Marchetti, M. (2021). Cyber-attacks and defences: current capabilities and future trends. In Technology and International Relations (pp. 132-151). Edward Elgar Publishing.
15. Cotroneo, D., Improta, C., Liguori, P., & Natella, R. (2024, April). Vulnerabilities in ai code generators: Exploring targeted data poisoning attacks. In Proceedings of the 32nd IEEE/ACM International Conference on Program Comprehension (pp. 280-292).
16. De Azambuja, A. J. G., Plesker, C., Schützer, K., Anderl, R., Schleich, B., & Almeida, V. R. (2023). Artificial intelligence-based cybersecurity in the context of Industry 4.0—a survey. Electronics, 12(8), 1920.
17. Dunn Cavelty, M., & Smeets, M. (2023). Regulatory cybersecurity governance in the making: The formation of ENISA and its struggle for epistemic authority. Journal of European Public Policy, 30(7), 1330-1352.
18. Egon, K., ROSINSKI, J., KARL, L., & EUGENE, R. (2023). AI and national security: The geopolitical implications of autonomous weapons and cyber Security.
19. Feijóo, C., Kwon, Y., Bauer, J. M., Bohlin, E., Howell, B., Jain, R., ... & Xia, J. (2020). Harnessing artificial intelligence (AI) to increase wellbeing for all: The case for a new technology diplomacy. Telecommunications Policy, 44(6), 101988.
20. Ferrara, E. (2023). Fairness and bias in artificial intelligence: A brief survey of sources, impacts, and mitigation strategies. Sci, 6(1), 3.
21. Galluccio, M. (2021). Science and diplomacy: Negotiating essential alliances. Springer Nature.
22. Grochmalski, P. (2020). US-China rivalry for strategic domination in the area of artificial intelligence and the new AI geopolitics. The Bellona Quarterly, 701(2), 5-25.
23. Guha, N., Lawrence, C., Gailmard, L. A., Rodolfa, K., Surani, F., Bommasani, R., ... & Ho, D. E. (2023). Ai regulation has its own alignment problem: The technical and institutional feasibility of disclosure, registration, licensing, and auditing. George Washington Law Review, Forthcoming.
24. Harari, Y. N. (2019). Who Will Win the Race for AI? Foreign Policy, (231), 52-54.
25. Harper, J. (2021). Federal AI spending to top $6 billion. National Defense Magazine. https://www.nationaldefensemagazine.org/articles/2021/2/10/federal-ai-spending-to-top-$6-billion
26. International Telecommunication Union. (2024). Global cybersecurity index 2024 (5th ed.). ITU Publications. https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/2401416_1b_Global-Cybersecurity-Index-E.pdf
27. Kello, L. (2024). Digital Diplomacy and Cyber Defence. The Oxford Handbook of Digital Diplomacy, 121.
28. Kreps, S., & Kriner, D. (2023). How AI threatens democracy. Journal of Democracy, 34(4), 122-131.
29. Korteling, J. H., van de Boer-Visschedijk, G. C., Blankendaal, R. A., Boonekamp, R. C., & Eikelboom, A. R. (2021). Human versus artificial intelligence. Frontiers in artificial intelligence, 4, 622364.
30. Lété, B. (2022). Paris Call and Activating Global Cyber Norms. German Marshall Fund of the United States.

31. Loureiro, S. M. C., Guerreiro, J., & Tussyadiah, I. (2021). Artificial intelligence in business: State of the art and future research agenda. Journal of Business Research, 129, 911-926.
32. Lundvall, B. Å., & Rikap, C. (2022). China's catching-up in artificial intelligence seen as a co-evolution of corporate and national innovation systems. Research Policy, 51(1), 104395.
33. Nair, M. M., Deshmukh, A., & Tyagi, A. K. (2024). Artificial intelligence for cyber security: Current trends and future challenges. Automated Secure Computing for Next-Generation Systems, 83-114.
34. Novanto, D. C., Putranti, I. R., & Basith Dir, A. A. (2021). Cybernorms: Analysis of International Norms in France's Paris Call for Trust and Security in Cyberspace. Journal of Islamic World and Politics, 5(2), 326-342.
35. Nyakomitah, K. (2023). Rethinking the Role of Diplomacy in Shaping World Politics. Journal of Research in Social Science and Humanities, 2(12), 1-5.
36. Nye Jr, J. S. (2022). The end of cyber-anarchy? How to build a new digital order. Foreign Aff., 101, 32.
37. Oosthuizen, M. E. (2024). Modern Diplomacy and the Changing Nature of International Politics in the 21st Century. Journal of BRICS Studies, 3(1), 27-41.
38. Pigatto, J. T., Datysgeld, M. W., & Silva, L. G. P. D. (2021). Internet governance is what global stakeholders make of it: a tripolar approach. Revista Brasileira de Política Internacional, 64(2), e011.
39. Pijpers, P. B., Boddens Hosang, J. F. R., & Ducheine, P. A. (2021). Collective cyber defence–the EU and NATO perspective on cyber attacks. Amsterdam Law School Research Paper, (2021-37).
40. Prantl, J., & Goh, E. (2022). Rethinking strategy and statecraft for the twenty-first century of complexity: a case for strategic diplomacy. International Affairs, 98(2), 443-469.
41. Radu, R. (2021). Steering the governance of artificial intelligence: national strategies in perspective. Policy and society, 40(2), 178-193.
42. Rocco, J., Sojwal, S., Stufano, A., Sy, C., Yeh, G. C. C., & González, S. K. (2020). Coronavirus case study from global to local: Framing the impact of COVID-19 on vulnerable populations living in NYC.
43. Rui, W. (2023). ASEAN Cybersecurity Policy and China-ASEAN Cooperation. China Int'l Stud., 98, 55.
44. Ruhl, C., Hollis, D., Hoffman, W., & Maurer, T. (2022). Cyberspace and geopolitics: Assessing global cybersecurity norm processes at a crossroads. Carnegie Endowment for International Peace.
45. Rymarczyk, J. (2020). Technologies, opportunities and challenges of the industrial revolution 4.0: theoretical considerations. Entrepreneurial business and economics review, 8(1), 185-198.
46. Sarkin, J. J., & Sotoudehfar, S. (2024). Artificial intelligence and arms races in the Middle East: the evolution of technology and its implications for regional and international security. Defense & Security Analysis, 40(1), 97-119.
47. Tarsney, C. (2024). Deception and Manipulation in Generative AI. arXiv preprint arXiv:2401.11335.

48. Waizel, G. (2024, July). Bridging the AI divide: The evolving arms race between AI-driven cyber attacks and AI-powered cybersecurity defences. In International Conference on Machine Intelligence & Security for Smart Cities (TRUST) Proceedings (Vol. 1, pp. 141-156).