African Journal of Law, Political Research and Administration
ISSN: 2689-5102
Volume 8, Issue 3, 2025 (pp. 24-35)
www.abjournals.org

CYBERSECURITY AND AI: THE ROLE OF INTERNATIONAL LAW IN PREVENTING AND RESPONDING TO AI-ENABLED CYBER THREATS

Adenike Awe Esq.

Legal Practitioner (Associate), S. A. Onadele & Co.

Email: aweadenike@gmail.com; Tel.: 08183522109

Cite this article:

Awe, A. (2025), Cybersecurity and AI: The Role of International Law in Preventing and Responding to AI-Enabled Cyber Threats. African Journal of Law, Political Research and Administration 8(3), 24-35. DOI: 10.52589/AJLPRA-5LA6H78Q

Manuscript History

Received: 15 Jul 2025

Accepted: 25 Aug 2025

Published: 4 Nov 2025

ABSTRACT: *Expectedly, International laws play an important role in cybersecurity and artificial intelligence (AI) by offering a framework to address new threats and regulate the development and application of AI technologies, especially with regard to potential cross-border cyberattacks. Imperatively, they ensure responsible behaviour by States and help to mitigate potential conflicts resulting from AI-powered cyber operations. However, because these technologies are developing so quickly, the extant laws that are supposed to address cyber threats arising from AI struggle to respond – partly because of the lack of flexibility of stakeholders. This paper is analytical in approach. It aims to examine international responses to AI-enabled cyber threats. In the end, it finds that the existing legal framework lacks robust provisions to address this growing threat. While the Malabo Convention lacks adequate domestication from the African jurisdictions, the Budapest Convention on Cybercrime and the EU GDPR do not have provisions on AI governance. To put this paper in perspective, some recommendations have been made, such as the adoption of compensatory enforcement mechanisms, enhanced liability mechanisms, and the legislation of a robust legal framework, among others.*

KEYWORDS: Cybersecurity, Cybercrime, AI, AI-enabled Cyber threats, International Law, Legislative Responses.

Article DOI: 10.52589/AJLPRA-5LA6H78Q
DOI URL: https://doi.org/10.52589/AJLPRA-5LA6H78Q

African Journal of Law, Political Research and Administration
ISSN: 2689-5102
Volume 8, Issue 3, 2025 (pp. 24-35)

www.abjournals.org

INTRODUCTION

It is anticipated that the market for cybersecurity solutions based on AI will increase from $24.8 billion in 2024 to $102 billion by 2032, demonstrating the vital role AI plays in contemporary defense tactics.[1] This increase is a result of the growing complexity of cyberattacks, in which adversaries also leverage cutting-edge technologies to get past defenses.[2] Yet, AI weaves a nuanced narrative – personifying a double-edged sword. In April 2018 for instance, Hackers leveraging AI to compromise companies targeted TaskRabbit, a well-known online marketplace owned by IKEA. [3]Matching local demand (Clients) with independent contractors (Taskers) in the housekeeping, moving, delivery, and related industries is the main objective of TaskRabbit. With millions of registered users at the time of the breach, it is a large-scale operation.[4]

What is more, using artificial intelligence (AI), Yum! Brands fell subject to a hack in January 2023.[5]The management initially believed that the hack was limited to corporate data, but it later became apparent that employee data was also compromised. With nine separate attacks over the past five years, this wireless network operator is no stranger to data breaches. Earlier in 2024, T-Mobile disclosed that a hack that started in November 2022 had stolen 37 million of its customers' records.[6] With these and many more cases arising, it becomes apparent that a critical solution is needed. This is the purpose of this paper – however, from the legal perspective.

In this light, this study will also explore the concepts of cybersecurity, artificial intelligence (AI), cyber threats, and AI-enabled threats. Armed with the doctrinal approach, it will provide recent examples of AI-enabled cyber threats that have occurred. Additionally, it will examine the role of international laws in preventing and responding to these AI-enabled threats, focusing on three existing legal frameworks, their limitations, and any gaps that may exist. Finally, to bring the point home, the paper will recommend strategies for effectively addressing AI-enabled threats.

[1] Perception Point: AI in Cybersecurity: 13 Examples and Use Cases <https://perception-point.io/guides/ai-security/ai-in-cybersecurity-examples-use-cases/> accessed 28 February 2025.
[2] Perception Point (ibid).
[3] KelleWhite: Real-Live Examples of How AI was Used to Breach Businesses (Oxen, 6 March 2024) <https://oxen.tech/blog/real-life-examples-of-how-ai-was-used-to-breach-businesses-omaha-ne/> accessed 28 February 2025.
[4] KelleWhite (ibid).
[5] KelleWhite (ibid).
[6] KelleWhite (ibid).

Article DOI: 10.52589/AJLPRA-5LA6H78Q
DOI URL: https://doi.org/10.52589/AJLPRA-5LA6H78Q

African Journal of Law, Political Research and Administration
ISSN: 2689-5102
Volume 8, Issue 3, 2025 (pp. 24-35)

www.abjournals.org

CONCEPTUAL FRAMEWORK

Cybersecurity

Cybersecurity is defined as a combination of technologies, procedures, and practices designed to secure and defend networks, devices, software, and data against attacks, damage, or unauthorized access.[7] In our increasingly digital society, it has become essential. As technological advancements accelerate and interconnected systems proliferate, governments, corporations, and individuals find themselves deeper into cyberspace, making them easy targets for cyberattacks.[8] The rapid expansion of the digital economy and infrastructure further complicates security challenges, heightening the risk of cyberattacks with potentially dire consequences.[9]

By providing defensive mechanisms, intrusion detection methods, and encryption techniques, cybersecurity ensures confidentiality, integrity, and reliability services across various fields.[10] For instance, it plays a crucial role in smart grids, smart cities, smart health systems, and vehicular communication.[11] This highlights that as the world becomes increasingly digitized, cybersecurity is no longer optional—it is essential.

AI has dramatically transformed the field of cybersecurity. With the rise in cybercrimes—especially as more people engage in cyberspace—the limitations of traditional security methods have become increasingly apparent.[12] In response to these challenges, AI has emerged as a more effective and reliable solution for safeguarding digital environments. By utilizing data, algorithms, and advanced computing techniques, AI can learn from 'past attacks, identify vulnerabilities, analyze suspicious behaviors, and respond to threats in real-time.'[13] This capability not only enhances security measures but also provides a proactive approach to protecting sensitive information and critical systems.

Artificial Intelligence

Artificial Intelligence is present in our daily lives. We interact with it consistently. The use of AI tools such as ChatGPT and DeepSeek for research, writing, summarizing, and explaining documents, alongside personal assistants like Amazon Alexa, Apple Siri, and Google Assistant, has become increasingly common. Beyond individual usage, various industries—including healthcare, finance, transportation, and entertainment—are continually adopting AI

[7] Ramanpreet Kaur and others, 'Artificial Intelligence for Cybersecurity: Literature Review and Future Research Directions,' (2023) 97 Information Fusion <https://doi.org/10.1016/j.inffus.2023.101804> accessed 16 February 2025.

[8] A. Shaji George, 'Riding the AI Waves: An Analysis of Artificial Intelligence's Evolving Role in Combating Cyber Threats,' (2024) 2(1) PUIIJ <https://puiij.com/index.php/research/article/view/117/89> accessed 16 February, 2025.

[9] Kaur and others, 'Artificial Intelligence for Cybersecurity…'

[10] Wasyihun Sema Admass, and others, 'Cyber security: State of the art challenges and future directions,' (2024) 2 Cyber Security and Applications <https://doi.org/10.1016/j.csa.2023.100031>accessed 21 February 2025.

[11] Ibid.

[12] George (ibid).

[13] Ibid.

Article DOI: 10.52589/AJLPRA-5LA6H78Q
DOI URL: https://doi.org/10.52589/AJLPRA-5LA6H78Q

technologies.[14] One thing is clear: Artificial Intelligence is continually advancing and is here to stay.

Artificial intelligence is more than just a tool—it is a multidisciplinary field encompassing robotics, computer vision, natural language processing, machine learning, and expert systems.[15] These technologies enable AI to perform tasks that would typically require human intelligence such as decision-making, visual perception, and speech recognition.[16] By detecting patterns, interpreting complex information, and continuously learning from vast datasets through advanced algorithms, AI is revolutionizing how we process and interact with information.[17]

Cyber Threats

Cyber threats[18] are not a new phenomenon. As far back as the early 2000s, attacks were carried out using worms like Code Red and Nimda, as well as viruses like ILoveYou.[19] However, with the rise of remote work and the Internet of Things (IoT), the attack surface of cyber threats has expanded significantly.[20] The impact of cyber threats has been devastating. As of 2024, the global loss due to cyberattacks was a devastating sum of $9.5 trillion.[21] This amount is more than the gross GDP of various countries. Aside from financial loss, cyber threats have led to reputational harm.[22] Cyber threats refer to malicious actions designed to damage data, steal information, or disrupt digital systems.[23] They also include risks associated with unauthorized access, intellectual property theft, and the compromise of computer networks.[24] Cyber threats are perpetrated through various means, including malware, phishing, denial of service (DoS) attacks, spoofing, identity-based attacks, supply chain attacks, social engineering attacks, and insider threats.[25]

AI-Enabled Cyber Threats

While AI has made significant positive contributions to our personal lives and cyberspace, its accessibility also makes it a tool that can be exploited by individuals with malicious intent. Threat actors have increasingly leveraged AI to execute sophisticated, highly targeted, and

[14] Tripti Bhushan, 'Artificial Intelligence, Cyberspace and International Law,' (2024) 21(2) Indonesian Journal of International Law <https://doi.org/10.17304/ijil.vol21.2.3> accessed 16 February, 2025.
[15] Ibid.
[16] George (ibid).
[17] Ibid.
[18] It can be referred to as Cyber-attack or Cybercrime.
[19] George (ibid).
[20] Ibid.
[21] Rodrigo Leme, 'The Impact of AI on Cyber Threat: The $9.5 Trillion Cybercrime of 2024,'(2024) <https://right-hand.ai/blog/impact-of-ai-on-cyber-threat/> accessed 21 February, 2025.
[22] Wasyihun Sema Admass, and others (Ibid).
[23] Abi Tyas Tunggal, 'What is a Cyber Threat?' (2025) <https://www.upguard.com/blog/cyber-threat> accessed 21 February 2025.
[24] Ibid.
[25] Kurt Baker, '12 Most Common Types of Cyberattacks,' (2024) <https://shorturl.at/bp69g> accessed 21 February, 2025.

Article DOI: 10.52589/AJLPRA-5LA6H78Q
DOI URL: https://doi.org/10.52589/AJLPRA-5LA6H78Q

large-scale cyber threats.[26] AI-enabled cyber threats refer to cyberattacks that utilize artificial intelligence to automate, quicken, and enhance various stages of malicious activities.[27] Machine learning algorithms play a crucial role in these attacks, enabling cybercriminals to develop adaptive strategies that evolve. This allows AI-driven threats to evade detection and bypass security measures with greater efficiency.[28] It is certain that as AI continues to advance, so will the potential for misuse, necessitating strengthened cybersecurity defenses against AI-powered attacks.

Demystifying AI-Enabled Cyber-Threats

Individuals with criminal intent have exploited AI in various ways to carry out cyber threats. This section of the paper will examine the various examples of these types of threats. They include:

Social Engineering Attacks

Humans are often considered the weakest link in the information security chain.[29] This is because even the strongest security measures cannot fully guard against human emotions, behavior, and personality traits. As a result, cybercriminals have successfully exploited these vulnerabilities through social engineering.[30] Social Engineering can be defined as the 'deliberate manipulation of individuals into releasing confidential information or performing actions that typically result in unauthorized access and potential breaches.'[31] Social engineering can be carried out through phishing, vishing, and smishing.[32] Even without AI, cybercriminals carried out social engineering attacks. However, with the integration of AI, these attacks are expected to become even more effective.[33] Cyberattackers utilize AI to target, create a persona with a corresponding online presence, initiate communication, craft a compelling scenario to capture the target's attention, and generate personalized messages or realistic audio and video content to engage the target.[34] This works because AI-generated messages demonstrate enhanced contextual understanding and the ability to use persuasive language, making them significantly more convincing.[35] For instance, this month, OpenAI had to remove some

[26] Nektaria Kaloudi and Jingyue Li, 'The AI-Based Cyber Threat Landscape: A Survey,' (2020) 53 (1) ACM Computing Surveys, <http://dx.doi.org/10.1145/3372823> accessed 22 February 2025.
[27] Lucia Stanham, 'AI-Powered Cyberattacks,' (2025) <https://www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/ai-powered-cyberattacks/> accessed 19 February, 2025.
[28] Ibid.
[29] Henry Collier, 'AI: The Future of Social Engineering!' (2024) 23(1) European Conference on Cyber Warfare and Security <http://dx.doi.org/10.34190/eccws.23.1.2117> accessed 22 February 2025.
[30] Hussam N. Fakhouri, 'AI-Driven Solutions for Social Engineering Attacks: Detection, Prevention, and Response,' (2024) IEEE <http://dx.doi.org/10.1109/ICCR61006.2024.10533010> accessed 22 February 2025.
[31] Ibid.
[32] Collier, 'AI: The Future of Social Engineering!'
[33] Ibid.
[34] Stanham (Ibid).
[35] Yazan Alahmed and others, 'Exploring the Potential Implications of AI-generated Content in Social Engineering Attacks,' <https://clok.uclan.ac.uk/53352/1/53352%20Alahmed%20et%20al.%20AAM.pdf>accessed 22 February 2025.

Article DOI: 10.52589/AJLPRA-5LA6H78Q
DOI URL: https://doi.org/10.52589/AJLPRA-5LA6H78Q

ChatGPT accounts based in Cambodia that used OpenAI's technology to generate multilingual social media comments to deceive individuals and steal their money.[36]

Phishing Attacks

This type of social engineering attack occurs when a threat actor sends an email to a victim in an attempt to fool them into clicking on a malicious link. This link may download malware, granting the attacker access to their devices or locking them up with ransomware. Alternatively, the email may deceive them into disclosing sensitive information like their login credentials and other private information.[37] AI-enabled phishing is more convincing than regular phishing.[38] Threat actors make use of ChatGPT and other Large Language Models to make individualized phishing emails with perfect tone and language, examine prior email exchanges to imitate victims' writing styles, and automate spear-phishing attacks directed at certain people or businesses.[39] For example, AI tools have recently been used to generate sophisticated phishing emails that victims struggle to identify as fraudulent. By gathering information from social media platforms, the attackers can determine topics that potential victims are likely to engage with. They then send scam emails that appear to come from friends and family.[40]

Deepfakes

Deepfake attacks, which utilize AI-generated video, picture, or audio files to trick people, are used by threat actors to spread false information, create fake news, and slander prominent persons.[41] It involves the use of generative AI to digitally alter what is in a video in real time.[42] For instance, in September 2024, U.S. Senator Ben Cardin fell victim to an advanced deepfake operation involving a fake video call from a threat actor posing as Ukraine's former Foreign Minister, Dmytro Kuleba, using AI technology to mimic Kuleba's voice and likeness. [43] It was only due to the questions asked that the senator and his team realized something was amiss. [44]

Additionally, deepfake technology is exploited by cybercriminals to execute what are known as AI 'heists.'[45] They carry out these 'heists' by impersonating company executives to deceive

[36] Anna Tong, 'OpenAI removes users in China, North Korea suspected of malicious activities,' *Reuters News* (21 February, 2025) <https://www.reuters.com/technology/artificial-intelligence/openai-removes-users-china-north-korea-suspected-malicious-activities-2025-02-21/> accessed 22 February 2025.
[37] Collier, 'AI: The Future of Social Engineering!'
[38] 'How AI is Used in Social Engineering Attacks' <https://www.webasha.com/blog/how-ai-is-used-in-social-engineering-attacks-advanced-cyber-threats-protection-strategies> accessed 22 February, 2025.
[39] Ibid.
[40] Brooke Kato, 'Gmail, Outlook and Apple users urged to watch out for this new email scam: Cybersecurity experts sound alarm,' *New York Post* (New York, 4 January 2025) <https://nypost.com/2025/01/04/tech/gmail-outlook-and-apple-users-urged-to-watch-out-for-this-new-email-scam-cybersecurity-experts-sound-alarm/> accessed 22 February, 2025.
[41] Stanham (ibid).
[42] Dan Merica, 'Sophistication of AI-backed operation targeting senator points to future deepfakes schemes,' *U.S. News* (26 September, 2024) <https://apnews.com/article/deepfake-cardin-ai-artificial-intelligence-879a6c2ca816c71d9af52a101dedb7ff> accessed 22 February, 2025.
[43] Ibid.
[44] Ibid.
[45] Lizzie Dearden, 'AI increasingly used for sextortion, scams and child abuse, says senior UK police chief,' *The Guardian* (24 November, 2024) <https://www.theguardian.com/technology/2024/nov/24/ai-increasingly-used-for-sextortion-scams-and-child-abuse-says-senior-uk-police-chief> accessed 23 February, 2025.

Article DOI: 10.52589/AJLPRA-5LA6H78Q
DOI URL: https://doi.org/10.52589/AJLPRA-5LA6H78Q

their colleagues and employees into transferring substantial sums of money.[46] According to Mastercard, 46% of businesses fall victim to identity fraud involving deepfakes, with 37% targeted by deepfake voice fraud and 29% by deepfake videos.[47] Consumers are not exempt from this threat; over 50% of Mastercard consumers report being scammed at least once a week, resulting in losses exceeding $1 trillion in 2024.[48] Beyond financial fraud, generative AI is also misused by paedophiles to create images and videos of child pornography.[49] In the United Kingdom, Hugh Nelson was sentenced to 18 years in prison for selling and distributing AI-generated child pornography on an online paedophile network.[50]

The impact of AI-enabled cyber threats extends far beyond financial loss; it has significant social and ethical implications. People have become increasingly skeptical and distrustful of digital content due to threat actors utilizing deepfake technology to disseminate fake news and misinformation. The psychological effects of these threats are alarming. In 2022, reports indicated that 16% of identity theft victims contemplated suicide.[51] The use of generative AI to create and share images and videos of child abuse has raised serious ethical concerns, highlighting the urgent need for robust international frameworks to address this pervasive issue. AI-enabled cyber threats are relentlessly undermining the foundations of our digital society.

International Responses to AI-Enabled Cyber-Treats

Various international frameworks[52] safeguard the rights of individuals and states by establishing key principles like fundamental human rights, the sovereignty of states, non-interference, and peaceful resolution of disputes. While these principles can be applied to the digital age, their effectiveness is limited. In response to the growing prevalence of cyber threats, international laws were created and adopted; some of these international legal frameworks will be reviewed. They include:

[46] Ibid.

[47] Damian Chmiel, 'Nearly 50% of Companies Targeted by AI Deepfakes, Mastercard Report Reveals,' <https://www.financemagnates.com/forex/analysis/nearly-50-of-companies-targeted-by-ai-deepfakes-mastercard-report-reveals/> accessed 23 February, 2025.

[48] 'Mastercard and Feedzai join forces to protect more consumers and businesses from scams,' *Mastercard News* (London, February 18, 2025) <https://www.mastercard.com/news/press/2025/february/mastercard-and-feedzai-join-forces-to-protect-more-consumers-and-businesses-from-scams/>accessed 23 February, 2025.

[49] Dearden, 'AI increasingly used for sextortion, scams and child abuse, says senior UK police chief.'

[50] Ewan Gawne, 'Man who made 'depraved' child images with AI jailed,' *BBC News* (Manchester, 28 October 2024) <https://www.bbc.com/news/articles/cq6l241z5mjo> accessed 23 February, 2025.

[51] Blake Hall, 'How AI-driven fraud challenges the global economy - and ways to combat it,'(Article is part of World Economic Forum Annual Meeting, 2025) <https://shorturl.at/1CNfR> accessed 23 February, 2025.

[52] These include the Universal Declaration of Human Rights, UN Charter, and the International Covenant on Civil and Political Rights.

Article DOI: 10.52589/AJLPRA-5LA6H78Q
DOI URL: https://doi.org/10.52589/AJLPRA-5LA6H78Q

African Journal of Law, Political Research and Administration
ISSN: 2689-5102
Volume 8, Issue 3, 2025 (pp. 24-35)
www.abjournals.org

The Budapest Convention on Cybercrime

The Budapest Convention on Cybercrime is a legal framework that was adopted by the Council of Europe on November 8th, 2001 and entered into force on the 1st of July, 2004.[53] The main objective of the convention as stated in its preamble is to:

…deter action directed against the confidentiality, integrity, and availability of computer systems, networks, and computer data as well as the misuse of such systems, networks, and data by providing for the criminalization of such conduct, as described in this Convention, and the adoption of powers sufficient for effectively combating such criminal offenses, by facilitating their detection, investigation, and prosecution at both the domestic and international levels and by providing arrangements for fast and reliable international co-operation.[54]

In achieving this objective, the Convention consists of 48 Articles that cover the criminalization of cyber threats, including unauthorized access,[55] data and system interference,[56] computer-related fraud,[57] and the distribution of child exploitation material.[58] It also contains legal procedures for investigating cybercrime and obtaining electronic evidence for any criminal cyber activity.[59] Additionally, it encourages effective international collaboration among participating States.[60]

This Convention represents the first binding international framework that comprehensively addresses cybercrime.[61] By January 2025, a total of 78 countries, including those outside Europe, have ratified this convention, demonstrating its growing global influence.[62] It has significantly shaped cybercrime legislation worldwide, as various nations have utilized the Convention as a model for drafting their cybercrime laws.[63] Notable examples include Sri Lanka's Computer Crime Act of 2007, the Dominican Republic's Law 53-07, and Tonga's Computer Crimes Act, all of which are based on the principles established by the Convention.[64]

However, going through this legal document that aims at effectively preventing and responding to cybercrime, there is no provision made for artificial intelligence or artificial intelligence-enabled cyber-attacks. This makes this convention inadequate to prevent or respond to the new form of cyberattacks—AI-enabled cyber threats. This inadequacy may be due to the time when

[53] 'Convention on Cybercrime, | EUR-Lex,'(2023)<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=legissum:4656911>accessed 22 February 2025.
[54] Preamble, The Budapest Convention on Cybercrime.
[55] Article 2, ibid.
[56] Article 4 and 5, ibid.
[57] Article 7 and 8, ibid.
[58] Article 9, ibid.
[59] Article 16-21, ibid.
[60] Article 23-35, ibid.
[61] Chat Le Nguyen and Wilfred Golman, 'Diffusion of the Budapest Convention on Cybercrime and the development of cybercrime legislation in Pacific Island countries: 'Law on the books' vs 'law in action',' (2021) 40 Computer Law & Security Review <https://doi.org/10.1016/j.clsr.2020.105521> accessed 22 February 2025.
[62] 'Rwanda becomes the 78th Party to the Convention on Cybercrime and accedes to the First Protocol,' *T-CY News* (Strasbourg, 10 January 2025) <https://www.coe.int/en/web/cybercrime/-/rwanda-becomes-the-78th-party-to-the-convention-on-cybercrime-and-accedes-to-the-first-protocol> accessed 23 February, 2025.
[63] 'Achievement,' (2021) <https://www.coe.int/en/web/cybercrime/achievements> accessed 23 February, 2025.
[64] Ibid.

Article DOI: 10.52589/AJLPRA-5LA6H78Q
DOI URL: https://doi.org/10.52589/AJLPRA-5LA6H78Q

this convention was created and entered into force—2004, a time when AI has not advanced. This therefore calls for a new and updated international legal framework.

African Union Convention on Cybersecurity and Personal Data Protection (Malabo Convention)

The African Union Convention on Cybersecurity and Personal Data Protection, commonly known as the Malabo Convention, was adopted by the African Union on June 27th, 2014, to tackle cybercrime and data protection across the continent. [65] This framework positions Africa as the only region with a continental agreement addressing cybercrime, cybersecurity, electronic transaction security, and data protection within a single treaty. [66] However, the Convention only came into force on June 8, 2023.[67] The delay in its implementation was due to Article 36, which stipulates that 15 countries must ratify the Convention for it to take effect; it took nine years for this requirement to be met. [68] Even after its enforcement in 2023, only one additional African country, São Tomé, has ratified the Convention. [69]

Consequently, only 16 out of 55 African Union member States have ratified this agreement. This low rate of ratification undermines the Convention's effectiveness in enforcement. The effectiveness of enforcing this Convention is significantly undermined by the lack of harmonization in cybercrime, cybersecurity, and data protection laws across African countries, as many have yet to align their legislation with the Convention's standards.[70] Additionally, several African nations lack comprehensive legal frameworks to address cybercrime, cybersecurity, and data protection, which impedes their ability to acquire the necessary legal tools for implementing the Malabo Convention.[71]

The Convention comprises 38 Articles that criminalize cyber offenses,[72]promote cybersecurity,[73] protect personal data,[74] stipulate the rights of data subjects, and outline the obligations of personal data controllers.[75] Additionally, it encourages cooperation among

[65] Shamaa Sheik, 'AU Convention on Cybersecurity and Personal Data Protection| Malabo Convention,' (2023) <https://www.michalsons.com/blog/au-convention-on-cyber-security-and-personal-data-protection-malabo-convention/65281#:~:text=Fast%20facts%20about%20the%20Convention,Principe%2C%20Senegal%2C%20and%20Zambia.> accessed 23 February, 2025.

[66] Nnenna Ifeanyi-Ajufo, 'The AU took important action on cybersecurity at its 2024 summit- but more is needed,' (2024) <https://www.chathamhouse.org/2024/02/au-took-important-action-cybersecurity-its-2024-summit-more-needed> accessed 23 February, 2025.

[67] Yohannes Eneyew Ayalew, 'The African Union's Malabo Convention on Cyber Security and Persoanl Data Protection enters into force nearly after a decade. What does it mean for Data Privacy in Africa or beyond,' (Blog of the European Journal of International Law, 2023) <https://www.ejiltalk.org/the-african-unions-malabo-convention-on-cyber-security-and-personal-data-protection-enters-into-force-nearly-after-a-decade-what-does-it-mean-for-data-privacy-in-africa-or-beyond/> accessed 23 February, 2025.

[68] Ibid.

[69] Ifeanyi-Ajufo (ibid).

[70] Mohamed Aly Bouke and others, 'African Union Convention on Cyber Security and Personal Data Protection: Challenges and Future Directions,' (2023) <http://dx.doi.org/10.48550/arXiv.2307.01966> accessed 23 February, 2025.

[71] Ibid.

[72] Article 29-31, African Union Convention on cybersecurity and Personal Data Protection.

[73] Article 24-27, ibid.

[74] Article 8-15, ibid.

[75] Article 16-23, ibid.

Article DOI: 10.52589/AJLPRA-5LA6H78Q
DOI URL: https://doi.org/10.52589/AJLPRA-5LA6H78Q

member states in addressing cybercrimes.[76] In reviewing the provisions related to cyber offenses, the framework primarily focuses on general cybercrime issues like hacking,[77] fraud,[78] and child pornography.[79] However, the Convention does not have specific or robust provisions regarding AI-enabled cyber threats. With the rapid advancement of AI, new threats to cyberspace are rapidly growing. Unfortunately, it does not have provisions that can address these new threats.

European Union General Data Protection Regulation

The European Union General Data Protection Regulation (EU GDPR) came into effect on May 24, 2016, and became enforceable on May 25, 2018.[80] Often regarded as the "strongest privacy and security law in the world," the EU GDPR governs the protection of personal data belonging to individuals, known as data subjects, ensuring that their information is not mishandled by companies or organizations, known as data controllers or processors.[81] The GDPR comprises 99 articles and 173 recitals, outlining several rights for individuals, including the right to access their data,[82] the right to be forgotten,[83] the right to restrict data processing,[84] and the right not to be subjected to automated individual decision-making.[85] If data controllers or processors violate these rights, they may face penalties imposed by member States,[86] including compensation[87] and administrative fines.[88]

This regulation is mandatory for all 27 EU Member States, the United Kingdom, and three EEA countries: Norway, Iceland, and Liechtenstein.[89] This fosters uniformity in data protection standards throughout the region. Furthermore, any company or organization that processes the personal data of individuals in these regions is also subject to GDPR compliance.[90] The EU GDPR has gained international recognition, serving as a model for privacy legislation in numerous countries outside of Europe.[91] Notable examples include Ecuador, Rwanda, Zambia, Belize, the British Virgin Islands, Oman, Mongolia, and Zimbabwe.[92]

[76] Article 28, ibid.
[77] Article 29 (2), ibid.
[78] Article 29 (1), ibid.
[79] Article 29 (3), ibid.
[80] European Commission, 'Legal framework of EU data protection,' (2023) <Legal framework of EU data protection - European Commission> accessed 23 February, 2025.
[81] European Council, 'The General Data Protection Regulation,' (2024) <The general data protection regulation - Consilium> accessed 23 February, 2025.
[82] Article 15, EU GDPR.
[83] Article 17, ibid.
[84] Article 18, ibid.
[85] Article 22, ibid.
[86] Article 84, ibid.
[87] Article 82, ibid.
[88] Article 83, ibid.
[89] Domonic Grande, 'Which Countries are GDPR Countries?' (2022) <Which Countries Are GDPR Countries - GDPR Countries 2023> accessed 23 February 2025.
[90] Ibid.
[91] Graham Greenleaf, 'Now 157 countries: Twelve data privacy laws in 2021/22,' (2022) UNSW Law Research <https://ssrn.com/abstract=4137418> accessed 23 February 2025.
[92] Ibid.

Article DOI: 10.52589/AJLPRA-5LA6H78Q
DOI URL: https://doi.org/10.52589/AJLPRA-5LA6H78Q

The EU GDPR does not specifically address AI-enabled cyber threats; however, it does provide provisions to protect data subjects from decisions made solely through automated processing, including profiling, which may have legal or significant effects.[93] There are exceptions to this rule: if the data subject has given explicit consent, if the automated decision is necessary for entering into or performing a contract between the data subject and the data controller, or if it is authorized by Union or Member State law to which the data controller is subject, provided that suitable measures are in place to protect the rights of the data subject.[94]

Automated decision-making (ADM) refers to the use of a programmed IT system to make significant decisions based exclusively on algorithmic evaluations of a data subject's personal data, without human intervention.[95] This concept can also encompass the use of AI to make legal or significant decisions that may affect the data subject.[96] While the regulation employs neutral language that includes artificial intelligence, it still lacks robust provisions specifically addressing AI-enabled cyber threats.

RECOMMENDATION

To effectively prevent and respond to AI-enabled cyber threats, international bodies and countries across the globe should implement the following solutions:

AI and Cybersecurity Treaty:

In this paper, three major international laws were analyzed based on several parameters: the number of countries that enforce them, their robust provisions regarding AI-enabled cyber threats, their extensive domestication and rectification, and their enforcement approaches, whether compensatory or criminal. The analysis reveals that the Budapest Convention stands out as the most comprehensive treaty for addressing cybercrime. However, it, along with all other international frameworks, falls short in the area of robust provisions for AI-enabled cyber threats, as they offer minimal or no guidelines concerning AI and the risks it poses to the digital landscape. Consequently, this paper advocates for the establishment and adoption of a globally binding legal framework that governs AI, including AI-enabled cyber threats, and promotes cybersecurity cooperation among States worldwide.

Compensatory Enforcement Mechanism:

In examining the three major international legal frameworks, the approach to enforcement was analyzed. All three frameworks criminalize cyber threats, stipulating that perpetrators of cyber-attacks may face criminal sanctions which include fines, or imprisonment. However, two of these frameworks do not address the compensation of victims, particularly those affected by financial fraud. To effectively prevent and respond to cyber threats, including those enabled by AI, these frameworks should be amended, or a new supplementary protocol should be established to include victim compensation for all forms of cyber threats. This would not only

[93] Article 22 (1), EU GDPR.
[94] Article 22(2), ibid.
[95] Elen Falletti, 'Automated Decisions and Article No.22 GDPR of the European Union: An Analysis of the Right to an "Explanation,"' (2019) SSRN <https://dx.doi.org/10.2139/ssrn.3510084> access3 February 2025.
[96] Ibid.

Article DOI: 10.52589/AJLPRA-5LA6H78Q
DOI URL: https://doi.org/10.52589/AJLPRA-5LA6H78Q

serve as a deterrent to potential offenders but also provide a means of restoration for unsuspecting victims.

Enhance Liability Mechanism:

In reviewing international frameworks, one notable encouragement is the promotion of international cooperation in addressing cybercrimes, which is commendable. However, it is essential for countries to implement these frameworks, particularly concerning AI-enabled threats. Therefore, this paper recommends that nations worldwide should collaborate and unite efforts to identify and prosecute individuals responsible for AI-enabled threats. This can be achieved by signing agreements that ensure the necessary tools and manpower are established for the successful implementation of this objective.

Building Legal and Technical Capacity:

Every nation, including those in the developing world, must enhance its technical and legal capabilities to effectively address AI-enabled cyber threats. This can be achieved by training stakeholders such as government officials, law enforcement agencies, and legal professionals in the skills and knowledge pertinent to artificial intelligence, cybersecurity, and data protection. Additionally, it is crucial to raise awareness about the global implications of AI-enabled cyber threats. To facilitate this, countries should work together to organize workshops, conferences, and training programs.

CONCLUSION

This paper has explored the concepts of cybersecurity, artificial intelligence, cyber threats, and AI-enabled cyber threats. It went on to explore the various examples of AI-enabled cyber threats with real-life examples. Additionally, the paper reviewed three major international legal frameworks governing cybercrime, cybersecurity, and data protection. Finally, it proposed key solutions to enhance international responses to cybercrime, with a particular focus on addressing the challenges posed by AI-enabled cyber threats.

Article DOI: 10.52589/AJLPRA-5LA6H78Q
DOI URL: https://doi.org/10.52589/AJLPRA-5LA6H78Q