GÜVENLİK STRATEJİLERİ DERGİSİ

Güv. Str. Derg. 2024, War and International System Special Issue, 109-130
DOI: 10.17752/guvenlikstrtj.1491683

Research Article

The Threat of Tomorrow: Impacts of Artificial Intelligence-Enhanced Cyber-attacks on International Relations

Yarının Tehditleri: Yapay Zekâ-Güçlendirilmiş Siber Saldırıların Uluslararası İlişkiler Üzerindeki Etkileri

Esra Merve ÇALIŞKAN*

*Ph.D. Research Assistant, Istanbul Medipol University, Faculty of Business and Management Sciences, Department of Business Administration, Istanbul, Türkiye e-mail: ecaliskan@medipol.edu.tr, ORCID: 0000-0001-5226-3177

Geliş Tarihi / Submitted:
02.06.2024

Kabul Tarihi / Accepted:
31.07.2024

Abstract

Artificial intelligence (AI) has revolutionized many sectors with its development, but it is also likely to pose new threats when used maliciously. This study examines the implications of state and non-state actors using AI to conduct more sophisticated cyber-attacks and their potential consequences for international relations and global security. Cyber-attack detection has become more automated, targeted, and challenging due to rapid advances in AI. Thanks to AI, adversaries can now impersonate humans, manipulate data, eavesdrop on conversations, and exploit system weaknesses on an unprecedented scale. Unchecked, AI-enabled cyber-attacks can undermine diplomatic relations, increase the likelihood of military conflict between governments, and destabilize the economy. The international community will need new legal frameworks and technological measures to mitigate these risks. International cooperation is necessary to limit the development of AI cyber weapons, develop robust systems, and establish guidelines for responsible state activity in cyberspace. Through cooperation and foresight, the potential of AI is more likely to be achieved while reducing the likelihood of intensified cyber warfare. This paper provides a broad literature perspective and offers recommendations for both legal and technological solutions to reduce the likelihood of the effects of AI-based cyber-attacks.

Keywords: Artificial Intelligence, Cyber-attacks, Cyber Conflict, Cyber Security, International Security

Öz

Yapay zekâ (YZ) gelişimi ile birçok sektörde devrim yaratmıştır, ancak kötü niyetli kullanıldığında yeni tehditler de oluşturması muhtemeldir. Bu çalışmada, yapay zekâ kullanılarak devlet ve devlet dışı aktörlerin daha sofistike siber saldırılar gerçekleştirmesinin nasıl etkiler doğurabileceği ve bu durumun uluslararası ilişkiler ve küresel güvenlik açısından olası sonuçları incelenmektedir. Siber saldırı tespiti, YZ'deki hızlı gelişmeler nedeniyle daha otomatik, daha hedefli ve daha zorlu hale gelmiştir. Yapay zekâ sayesinde, düşmanlar artık insanları taklit edebilmekte, verileri değiştirebilmekte, konuşmaları dinleyebilmekte ve sistem zayıflıklarını daha önce hiç görülmemiş bir ölçekte kullanabilmektedir. Kontrol edilmeyen YZ-destekli siber saldırılar diplomatik ilişkileri baltalama, hükümetler arasında askerî çatışma olasılığını artırma ve ekonomiyi istikrarsızlaştırma kapasitesine sahiptir. Bu riskleri azaltmak için uluslararası toplumun yeni yasal çerçevelere ve teknolojik önlemlere ihtiyacı olacaktır. YZ siber silahlarının gelişimini sınırlandırmak, dirençli sistemler geliştirmek ve siber uzayda sorumlu devlet faaliyeti için kılavuz ilkeler oluşturmak için uluslararası iş birliği gereklidir. İş birliği ve öngörü yoluyla, yoğunlaştırılmış siber savaş olasılığını azaltırken YZ'nin potansiyeline ulaşılabilmesi daha olasıdır. Bu makale, YZ tabanlı siber saldırıların etkilerinin olasılığını azaltmak için geniş bir literatür perspektifi ortaya koymakta ve hem yasal hem de teknolojik çözümler için öneriler sunmaktadır.

Anahtar Kelimeler: Yapay Zekâ, Siber Saldırılar, Siber Çatışma, Siber Güvenlik, Uluslararası Güvenlik

Introduction

While the dizzying pace of technological progress with artificial intelligence (AI) continues to rise, research on the possible impact of AI-enabled cyber threats on international relations and global security is limited. Recent research has highlighted this gap, emphasizing the need for a thorough knowledge of how AI-enabled combat, particularly cyber threats, will transform global security dynamics.[1] However, this topic is critical for ensuring peace and stability in the 21st century. Robust inter-state cooperation is required before AI's uncertainties and hazards take on irreversible dimensions. According to this study, AI technology's rapid evolution in cybersecurity creates extraordinary opportunities and difficulties, necessitating ongoing research and worldwide collaboration to combat emerging threats.[2] Experts also note that while AI has the potential to improve cybersecurity capabilities dramatically, its implementation creates new risks and ethical concerns that must be carefully considered and addressed globally.[3] These complex dynamics highlight the critical need for expanded academic research and policy activities to address the multiple effects of AI-enabled cyber threats on global security and international relations.

Although AI's comprehensive reflection on daily life and cyber security continues, most studies focus on technical dimensions.[4] Studies focus mainly on how AI strengthens cyber-attacks and defenses and how these effects can be reflected in the dynamics of international relations.[5] However, studies on the potential effects of AI-supported cyber threats on inter-state relations, international security, and global peace remain scarce. The possible practical consequences of the uncertainties AI will bring to these areas have yet to be adequately addressed.[6] Also, theoretical discussions on this subject in the international relations literature are inadequate. We must understand the effects of AI-supported cyber-attacks on international security to grasp the international community's situation in this AI-shaped technological age.[7]

The study is generally shaped around the question, "How does AI-enhanced cyber-attack potential affect international relations and global security?". To answer this question, the following hypothesis has been formulated: "Developments in artificial intelligence technology have the potential to make cyber-attacks carried out by state and non-state actors more powerful and destructive. If not controlled, AI-supported cyber-attacks can lead to conflicts between states, threaten international stability, and increase the risks of war." According to this hypothesis, the advanced analysis and capabilities of learning and automation provided by AI make cyber-attacks faster, more scalable, and more destructive. AI-enabled attacks can lead to diplomatic, economic, and military tensions, jeopardizing peace. The study assesses the hypothesis that advances in AI technology have the potential to make cyber-attacks by state and non-state actors more powerful and destructive. When left

[1] James Johnson, "Artificial Intelligence & Future Warfare: Implications for International Security", *Defense and Security Analysis*, 35:2, 2019, p. 153.

[2] Ramanpreet Kaur, Dušan Gabrijelčič and Tomaž Klobučar, "Artificial Intelligence for Cybersecurity: Literature Review and Future Research Directions", *Information Fusion*, 97:September 1, 2023, p. 3.

[3] Mariarosaria Taddeo, Tom McCutcheon and Luciano Floridi, "Trusting Artificial Intelligence in Cybersecurity Is a Double-Edged Sword", Nature Machine Intelligence, 1: 12, November 11, 2019, p. 558.

[4] Joseph Nye, "Deterrence and Dissuasion in Cyberspace", *International Security,* 41:3, 2017, p. 67.

[5] Max Smeets, "A Matter of Time: On The Transitory Nature of Cyberweapons", *Journal of Strategic Studies,* 41:(1-2), 2018, p.10-12.

[6] Adam Segal, "The hacked world order: How nations fight, trade, maneuver, and manipulate in the digital age" *PublicAffairs,* 2016, p 68-70.

[7] Erik Gartzke and Jon R. Lindsay, "Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace", *Security Studies,* 24:2, 2015, p.320

unchecked, AI-enabled cyber-attacks can lead to conflicts in inter-state relations, threaten international stability, and increase the risk of war.

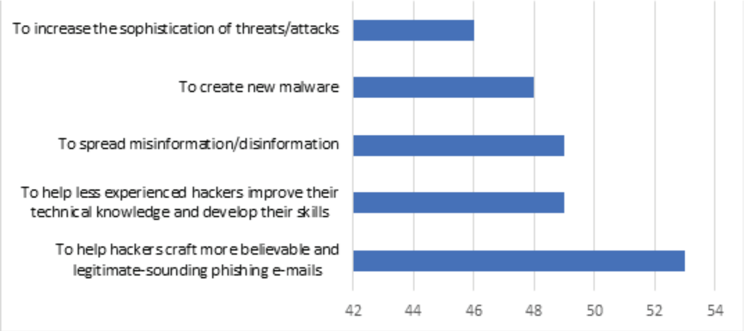
The scope of this study includes a wide range of AI technologies. This study covers not only language models such as ChatGPT but also other advanced language models such as GPT-3, BERT, XLNet, Roberta, T5, ALBERT, ELECTRA, and ERNIE, as well as the impact of machine learning, deep learning, neural networks, and other AI technologies on cyber security. This broad perspective will provide a more comprehensive understanding of how AI transforms cyber-attacks and defense mechanisms.

In terms of technique, this study employs a qualitative research approach and secondary data analysis. Academic articles, think tank reports, government policy documents, reports from international organizations, and trustworthy news sources have been thoroughly evaluated. The study uses the collected data to investigate how AI is developing cyber-attack capabilities, as well as the potential effects of these attacks on international relations, economic balances, and conflict risks. In the literature review part, we will thoroughly examine existing research in AI and cybersecurity. This will allow us to properly position our study within the current body of knowledge while emphasizing the unique contribution of our research. AI's impact extends beyond technology to politics, economics, and social issues. AI has significant implications for business, economics, and diplomacy. In addition, this study identifies and evaluates factors that contribute to a better understanding of the subject matter. In the conclusion section, we will present findings and recommendations for developing effective policies against AI-powered cyber threats. These guidelines apply to all actors, developers, and other stakeholders. Aiming to fill these gaps in the literature, this study aims to theoretically and empirically examine the effects of developments in AI technology on international peace and security. It aims to guide policymakers by comprehensively analyzing the possible effects of AI-enabled cyber-attacks on the international system.

1. Literature Review

With the rapid development of AI in recent years and its spread across all fields, a major mechanism of influence has emerged. The 3R (robustness, response, and resilience, created by AI for cyber-attacks has made the existing nature of cyber-attacks exceedingly difficult to control.[8]

Figure 1. Purpose of ChatGPT Usage in Cybercrime 2023[9]



[8] Mariarosaria Taddeo, Tom McCutcheon and Luciano Floridi, "Trusting Artificial Intelligence in Cybersecurity Is a Double-Edged Sword", *Nature Machine Intelligence*, 12:1, November 11, 2019, p. 557.

[9] Statista, "Possible usage of ChatGPT for cyber crime purposes according to IT and security professionals in selected countries worldwide as of January 2023", https://www-statista-com.eu1.proxy.openathens.net/statistics/1378211/chatgpt-usage-cyber-crime-global/, accessed 17.07.2024.

As shown in Figure 1, AI tools such as ChatGPT will be used in cybercrimes in many different areas around the world in 2023.[10] AI has now shown its effectiveness in cybercrimes and cyber-attacks.

In addition to ChatGPT, many other advanced AI applications have seen increased use in cyber-attacks. Experts have found that 70% of cyber-attacks worldwide were AI-enabled last year.[11] This situation reveals the gravity of the impact mechanism of AI. In the face of this spread of AI, states have had to take new initiatives to keep their security systems under control. The establishment of AI-supported infrastructure in attack and defense mechanisms has become a priority for states. With the development of AI and the increase in investments based on AI, the global commercial competition environment and the international security environment have experienced a significant transformation.[12] In addition to this transformation, the fact that AI enables attackers to automate, customize, and scale their attacks has begun to affect the cyber security capabilities of states.[13] In light of all these developments, this section will examine the literature on AI-supported cyber-attacks and international relations to better understand AI's rapid development. Considering the studies in AI and cyber security, essential theories, concepts, and findings in these fields will be summarized, and the theoretical basis will be supported with concrete facts.

Artificial intelligence (AI) refers to a field that aims to enable computer systems to acquire human-like thinking and learning capabilities. AI also includes many algorithms and techniques known for their data analysis, pattern recognition, autonomous decision-making, and problem-solving capabilities. Approaches such as machine learning and deep learning form the basis of AI applications. Thanks to this multifunctional structure, AI finds a wide range of applications in different sectors. Especially in cyber security, it has a high potential to be used effectively in both cyber-attacks and defense.

Within this development, the characteristics of AI will inevitably affect the global order.[14] In particular, advanced AI techniques such as deep learning have the potential to revolutionize cyber-attacks. Deep learning is defined as a subset of machine learning capable of learning and generalizing complex patterns from large data sets using multiple layers of artificial neural networks.[15] This technology allows malware to continuously improve itself, evade defenses, and mimic human behavior.[16] This multifaceted effect of deep learning takes the offensive defense system to a different dimension. It also has the potential to change the known war-conflict equation. Beyond traditional military balances of power, a country or group's cyber capabilities and the ability to use deep learning technology will make it a decisive factor in international relations and security policies.

Another significant impact of AI on the attack-defense balance is its ability to detect vulnerabilities and exploit large datasets much faster. This capability enables automated

[10] Statista, "Possible usage of ChatGPT for cyber crime purposes according to IT and security professionals in selected countries worldwide as of January 2023", https://www-statista-com.eu1.proxy.openathens.net/statistics/1378211/chatgpt-usage-cyber-crime-global/, accessed 17.07.2024.

[11] Adam Zaki, "85% of Cybersecurity Leaders Say Recent Attacks Powered by AI: Weekly Stat", https://www.cfo.com/news/cybersecurity-attacks-generative-ai-security-ransom/692176/ accessed ed 17.07.2024.

[12] Micheal N. Schmitt, "Weapon Systems and International Humanitarian Law: A Reply to the Critics", *Harvard National Security Journal Feature*, 2013, p. 3.

[13] Max Smeets, "A Matter of time: On the Transitory Nature of Cyberweapons", *Journal of Strategic Studies,* 41:1-2, 2018, p. 17.

[14] James P. Farwell and Rafal Rohozinski, "Stuxnet and the Future of Cyber War", *Survival*, 53:1, 2011, p. 33.

[15] LeCun Yann, Bengio Yoshua and Hinton Geoffrey, "Deep Learning", *Nature*, 521:7553, 2015, p. 436.

[16] Emily Otto, 2024, "Be-aware of AI-Enhanced Cyber-attacks", https://cepa.org/article/beware-of-ai-enhanced-cyber-attacks/, accessed 17.07.2024.

attacks on systems to scale even further. For example, by analyzing network traffic, machine learning algorithms can discover previously unknown vulnerabilities and use this knowledge to optimize attack vectors.[17] Furthermore, AI-based social engineering activities make it easier to manipulate human targets. Advanced language models and deep learning techniques can analyze the online behavior of targets to create personalized and persuasive messages.[18] This analysis can increase the success rate of phishing attacks and threaten corporate security. However, AI technologies are also used in defense. In areas such as anomaly detection, threat intelligence, and automated response systems, AI offers valuable tools to cyber security experts. However, the fine line between misuse and ethical use of these technologies will be one of the biggest challenges in cybersecurity in the future.

AI's advanced cyber capabilities and versatile attack mechanisms will inevitably become an essential threat to international security. Considering the effects of AI attacks, the activities of countries to strengthen their cyber security increase daily[19].

With the instantaneous orchestration of AI-based attacks, it has become relatively easy to paralyze critical infrastructures such as financial markets, energy grids, and transportation systems.[20] This increases the likelihood of economic crises and tensions between countries. In addition, automatic disinformation, propaganda, and political manipulation targeting democratic systems with the support of AI have the potential to destabilize regimes by interfering in elections and public opinion.[21] Again, as one of the possible attacks supported by AI, deepfakes, identity and content generation can undermine diplomatic confidence by misleading public opinion.[22] Finally, AI-enabled cyber-attacks are likely to lead to mutual retaliation and even conflict.[23] It is also possible to expect this tense situation to indirectly lead to an arms race and constitute a security crisis between states. All these types of attacks reveal that it has become easier to create more effective destruction with the effect of AI than conventional warfare.[24] Ultimately, this is a possible scenario threatening international stability and security.

The discussions in the international relations literature on AI are handled not only through possible attack potential and security mechanisms but also theoretically. Realist theorists have presented cyberspace as a new field of competition when addressing the issue. They have adopted the approach that cyber armament can change traditional military power balances. AI has also been readily adopted as an indispensable tool in the balance of power to gain power in this field. Liberal theorists, on the other hand, argue that the transparency and connectivity brought by AI can increase cooperation.[25] However, some theorists argue that this is an idealistic view. Structuralists argue that technological change will reshape power

[17] Olga Illiashenko et al., "Security-Informed Safety Analysis of Autonomous Transport Systems Considering AI-Powered Cyber-attacks and Protection", *Entropy (Basel),* 26-25(8):1123,2023, p. 5.

[18] Eleonore Fournier-Tombs et al., "Artificial Intelligence-Powered Disinformation and Conflict", Policy Brief, *United Nations University Centre for Policy Research,*2023, p. 3.

[19] Max Smeets, 2018, p. 21.

[20] Brandon Valeriano, Benjamin M. Jensen and Ryan C. Maness, *Cyber strategy: The Evolving Character of Power and Coercion*, Oxford University Press, New York, 2020, p. 70-73

[21] Susan Morgan, "Fake news, disinformation, manipulation and online tactics to undermine democracy", *Journal of Cyber Policy*,3:1, 2018, p. 40.

[22] Henry Ajder, Giorgio Patrini, Francesco Cavalli and Laurence Cullen, "The State of Deepfakes: Landscape, Threats, and Impact", *Deeptrace*, 2019, p. 9-11.

[23] Erik Gartzke and Jon R. Lindsay, "Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace", *Security Studies*, 24:2, 2015, p. 320.

[24] John R Lindsay, "Stuxnet and the Limits of Cyber Warfare", S*ecurity Studies*, 22:3, 2013, p. 369-370.

[25] Joseph Nye, "Deterrence and Dissuasion in Cyberspace", *International Security,*41:3, 2017, p. 50.

balances[26] and that cyberspace will inevitably become a new source of structural power. According to feminist theorists, the risks posed by the masculine cyber security discourses revealed in cyberspace make the field more complex.[27] They argue that cyberspace should focus on human security rather than armament and power and that the issue cannot be considered separately from gender identities.

On the theoretical grounds, AI has also affected the balance of power between countries. The United States (US) and China stand out as the leading powers in AI technologies. Both countries' human resources and strong research infrastructures have given them a dominant position in this field.[28] They use these advantages effectively, especially in developing AI's cybersecurity and attack capabilities.

Table 1. AI Investments by Countries[29]

Country	Number of AI Startups (2013-2022)	Private Investment (2013-2022) (billion dollars)
United States	4643	$249B
China	1337	$95B
United Kingdom	630	$18B
Israel	402	$11B
Canada	341	$9B
France	338	$7B
India	296	$8B
Japan	294	$4B
Germany	245	$7B
Singapore	165	$5B

The leadership of the US and China in AI is reflected in concrete data. Between 2013 and 2022, 4643 AI companies were established in the US, attracting $249 billion in private-sector investment. In the same period, China hosted 1337 AI companies and attracted $95 billion in private investment.[30] These figures show how both countries attach great importance to AI technologies and allocate resources to consolidate their leadership in this field. On the other hand, countries such as the UK, Israel, Canada, France, India, Japan, Germany, and Singapore have also made significant investments in AI, but these numbers are well below the investment in the US and China. The number of AI companies in these countries and the private investment they receive lag far behind the two giant economies.

Table 1 confirms the profound "knowledge and resource gap" in the development of AI technologies and their integration into cybersecurity.[31] The US and China use their human

[26] Amy Zegart, "Cheap Fights, Credible Threats: The Future of Armed Drones and Coercion", *Journal of Strategic Studies*, 41:1-2, 2018, p. 9-11.

[27] Elsa Bengtsson Meuller, "A Feminist Theorisation of Cybersecurity to Identify and Tackle Online Extremism", London: *Global Network on Extremism and Technology (GNET),* May 2023, p. 12.

[28] Tkacheva, Olesya, Lowell H. Schwartz, Martin C. Libicki, Julie E. Taylor, Jeffrey Martini and Caroline Baxter, "Internet Freedom and Political Space", Santa Monica, *CA: RAND Corporation*, 2013, p. 4-7.

[29] Allan Kennedy, "Ranked: Artificial Intelligence Startups, by Country", 2023, https://www.visualcapitalist.com/sp/global-ai-investment/, accessed 26.05.2024.

[30] Al Majalla, "US and China Forefront of AI Investment", https://en.majalla.com/node/305236/infographics/us-and-china-forefront-ai-investment accessed 25.05.2024.

[31] Allan Kennedy, "Ranked: Artificial Intelligence Startup by Country", 2023, https://www.visualcapitalist.com/sp/global-ai-investment/ , accessed 26.05.2024.

resource and financial superiority in this field to increase their effectiveness on a global scale. On the other hand, developing countries face significant challenges in accessing and integrating AI technologies. Problems such as inadequate infrastructure, budget constraints, and lack of qualified human resources make them vulnerable to cyber-attacks. Many developing countries that cannot keep up with these rapidly developing technologies become targets of attackers and suffer economic losses.

This situation causes significant power imbalances and instability in international relations. The knowledge and resource gap in AI leads developed countries to gain more influence in cyberspace and become more effective globally.[32] On the other hand, the inability of developing countries to access and integrate into this field causes them to lose power and experience greater vulnerability.[33]

While the impact of AI is so advanced and the potential for competition between countries has increased immensely, serious threats that may arise if AI is abused emerge. These real-life attack examples demonstrate the potential of AI to make cyber-attacks more effective and difficult to detect[34]. AI-enhanced phishing attacks reach targets by creating highly convincing e-mails. During the COVID-19 pandemic, cybercriminals have capitalized on fear and uncertainty to craft e-mails appearing to originate from legitimate sources and offer pandemic-related information or services.[35] These e-mails were virtually indistinguishable from authentic communications, significantly increasing the success rate of attacks.

In 2024, an Iranian government-backed hacker group interrupted TV streaming services in the United Arab Emirates (UAE) to broadcast a deepfake newsreader delivering a report on the war in Gaza.[36] This example reveals how powerful the impact of AI is.

Furthermore, in 2020, in an AI-powered voice cloning attack, criminals mimicked the voice of a UK firm's CEO to trick an employee into transferring $240,000 to a fake account.[37] This attack demonstrates AI's potential to provide a high degree of realism in social engineering attacks.

An advanced malware called DeepLocker remains dormant until it detects its specific target using AI through facial recognition, geolocation, or other parameters.[38] The malware is activated once the parameter set is detected, making it extremely difficult to detect and prevent.

With the increase in remote working, ransomware attacks have also increased. AI is constantly used to identify vulnerable systems and deploy ransomware more efficiently. For example, the use of AI to evade traditional security measures and distribute ransomware

[32] Joseph Nye, "Deterrence and Dissuasion in Cyberspace*", International Security,* 2017, p. 50.

[33] Myriam Dunn Cavelty and Andreas Wenger, *Cyber Security Politics: Socio-Technological Transformations and Political Fragmentation,* 1 Edition.New York, NY: Routledge, 2022, p. 6.

[34] MIT Technology, "Preparing for AI-Enhanced Cyber-attacks", 2021, https://www.technologyreview.com/2021/04/08/1021696/preparing-for-ai-enabled-cyber-attacks/, accessed 22.05.2024.

[35] MIT Technology, "Preparing for AI-Enhanced Cyber-attacks", 2021, https://www.technologyreview.com/2021/04/08/1021696/preparing-for-ai-enabled-cyber-attacks/, accessed 22.05.2024.

[36] Dan Milmo, "Iran-Backed Hackers Interrupt UAE TV Streaming Services With Deepfake News", 2024, https://www.theguardian.com/technology/2024/feb/08/iran-backed-hackers-interrupt-uae-tv-streaming-services-with-deepfake-news, aceessed 17.07. 2024.

[37] Giannis Tziakouris, "The Rise of AI-Powered Criminals: Identifying Threats And Opportunities", https://blog.talosintelligence.com/the-rise-of-ai-powered-criminals/, accessed 26.05. 2024

[38] Trend Micro, United Nations Interregional Crime and Justice Research Institute (UNICRI), and Europol, 2020, 'Exploiting AI', https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/exploiting-ai-how-cybercriminals-misuse-abuse-ai-and-ml, accessed 17.07. 2024.

has become a significant threat, especially for organizations depending on remote access solutions.[39]

Cybercriminals and state-sponsored actors have used AI to create deepfake videos and launch disinformation campaigns. These campaigns manipulate public opinion and spread fake information rapidly on social media platforms. For example, during the pandemic, AI-generated content was used to spread misinformation about COVID-19, tailoring content to specific demographic groups through machine learning.[40]

These examples illustrate the two-sided nature of AI. While AI offers significant benefits, it also enables cybercriminals to conduct more effective and harder-to-detect attacks. With the advancement of AI technology, there is a growing need for strong cybersecurity measures and AI-powered defense mechanisms.

Existing literature suggests that AI will play an important role in cyber-attacks and defense mechanisms. The development of AI technologies has increased the ability of attackers to automate, customize, and scale their attacks, thus impacting cyber security capabilities. Notably, advanced AI techniques such as deep learning have the potential to revolutionize cyber-attacks. However, the advancement of AI also offers the possibility to strengthen defense systems and detect vulnerabilities faster.[41]

The effects of AI in cyberspace have significant implications for international security and stability. The paralysis of critical infrastructures has the potential to lead to economic crises and tensions between countries. Moreover, AI-enabled disinformation, propaganda, and political manipulation can destabilize democratic systems. Therefore, countries are forced to invest in AI technologies to strengthen their cyber security.

In conclusion, the rapid development and proliferation of AI in cybersecurity has had a profound impact on international relations and security dynamics. AI technologies offer the potential to strengthen defense mechanisms while increasing the sophistication and impact of cyber-attacks. Advanced AI techniques such as deep learning have significantly increased the capabilities of attackers, enabling automated and scalable attacks. This development makes countries reassess their cybersecurity strategies and invest in AI-enabled defense systems. At the same time, the misuse of AI has given rise to new types of threats, such as deepfakes, social engineering, and disinformation campaigns. These developments affect the international balance of power, reinforcing the advantages of AI leaders, such as the US and China. The difficulties experienced by developing countries in accessing and integrating AI technologies deepen inequalities in the global cybersecurity ecosystem. As a result, the role of AI in cyberspace is becoming central to international security, diplomacy, and cooperation efforts. In the future, ethical and responsible use of AI technologies will be critical to stabilizing cyberspace and maintaining international security.

2. Method

This study aims to investigate the potential impacts of AI-enabled cyber-attacks on international relations and global security through a comprehensive literature review. The focus question of the study is, “How does the potential for AI-enabled cyber-attacks affect international relations and global security?” To answer this critical question, the following hypothesis was developed: “Recent advances in AI technology have the potential to make

[39] MIT Technology Review, 2021.
[40] Giannis Tziakouris, 2023.
[41] Max Smeets, 2018, p. 36.

cyber-attacks by state and non-state actors more powerful, smarter, and more destructive. If left unchecked, AI-enabled advanced cyber-attacks could lead to serious tensions and conflicts in inter-state relations, threaten international stability and security, and even increase the risks of hot conflict".[42]

The study adopts a systematic literature review methodology. This method involves systematically scanning, analyzing, and synthesizing existing academic studies, policy documents, and industry reports.[43] Academic databases, policy documents, think tank reports, sector reports, and publications of international organizations have been used for the literature review. The search strategy included keywords such as AI, cyber-attacks, international relations, and global security. The review covers studies published in the last ten years (2014-2024). The collected literature was systematically examined under the headings of international consequences, economic impacts, imbalances between countries, the inadequacy of defense measures, cybercrimes and economic losses, international cooperation, and the need for new rules. The quality of the sources included in the review has been evaluated according to criteria such as the reliability of the publication's source, the author's expertise, the soundness of the methodology, the consistency of the findings, and the currentness of the source. The information obtained from the reviewed literature has been synthesized under specified headings. Considering the findings from the literature review, comprehensive policy recommendations are developed in the conclusion section. These recommendations include measures that can be taken and strategies that international actors, states, and the private sector can follow against AI-supported cyber threats.

Limitations of the study include the focus on English-language sources only, the inaccessibility of confidential or limited-access sources, and the risk that some information may be outdated due to rapid developments in AI and cyber security. This methodology aims to comprehensively examine the impact of AI-enabled cyber-attacks on international relations and global security and to provide guiding recommendations for policymakers in this field. Recommendations will include strengthening cybersecurity capacities, increasing international cooperation, developing AI regulations and codes of ethics, and strengthening defense mechanisms.[44] This article, which offers a different perspective to the studies in the field, aims to shed light on the possible threats of AI-assisted attacks in cyber security.

3. International Consequences

AI-assisted attacks are likely to have different impacts in many ways. The impact on international security is undeniable. Attacks on critical infrastructures target a country's economic and social stability.[45] Power outages, transportation disruptions, and financial collapses threaten personal security and ignite social unrest. In addition, cyber interference in political processes undermines the sovereignty and stability of countries and negatively affects democratization processes.[46] Election and public opinion manipulation has become a significant threat to regimes. In light of all these, the literature review reveals that

[42] Malatji M. Jourand Tolah Alaa, "Artificial Intelligence (AI) Cybersecurity Dimensions: A Comprehensive Framework for Understanding Adversarial and Offensive AI", *AI and Ethics*, Springer, p. 5.

[43] Kimberly A.Neuendorf, "Content Analysis and Thematic Analysis", *Advanced Research Methods for Applied Psychology*, 1:2, 2020, p. 214. John W. Creswell and David Creswell, *Research Design: Qualitative, Quantitative and Mixed Methods Approaches*, SAGE Publications, 2022, p. 76-78.

[44] "Net Losses: Estimating the Global Cost of Cybercrime", C*enter for Strategic and International Studies.* https://csiswebsiteprod.s3.amazonaws.com/s3fspublic/publication/140609_rp_economic_impact_cybercrime_report.pdf p. 6-8. accessed 17.07.2024.

[45] Lucas Kello, The Virtual Weapon and International Order, Yale University Press, 2017, p. 32-33.

[46] Joseph Nye, "Cyber Power ", *Belfer Center for Science and International Affairs*, 2021, p. 3-7.

AI-supported cyber-attacks have multifaceted effects on international relations and global security. This section will systematically present the findings from the reviewed studies.

The global proliferation of AI-supported cyber-attacks can have consequences that will profoundly shake the international system. Increasing cybercrime rates could jeopardize the economic stability of many countries.[47] Critical infrastructures such as finance, health, and education will especially be subject to intense attacks.[48] The inability of international organizations to prepare for this threat may call into question their legitimacy.[49]

It would be one-sided to evaluate the effects of AI on international security only in terms of attacks and threats. The ambiguity about the origins of these attacks will stoke distrust between states.[50] The triggering of an AI arms race is also likely. States will invest in cyber programs to increase deterrence capabilities. As in the Cold War era, the risks of a cyber arms race are likely to increase with the impact of AI.[51] It is also obvious that distrust can lead to miscalculations and conflicts. Cyber operations perceived as violations of sovereignty can lead to retaliation.[52] Escalation brought about by mutual cyber operations is also likely to occur. In addition, due to the difficulty of detecting and tracking them, these attacks may be attributed to wrong targets, or miscalculations may occur.[53] Ultimately, cyber-attacks can trigger military operations and lead to cyber armaments becoming a race.[54] Since cyber weapons are cheaper than conventional weapons, the race in this area can progress faster than in other areas. Losing control of this race can create a security dilemma. In addition, doubts and concerns will increase since it will not be transparent at what level of AI capability each state has. Increasing cyber espionage activities will also deepen distrust between national security institutions. All these factors bring the danger of creating a global crisis of confidence. The competition between the USA and China can be perceived as the driving force in the cyber race, but other powers may also try to participate in this race. Ultimately, if international cooperation cannot be achieved, this situation may lead to instability on a global scale. From the perspective of technological determinism, AI-supported cyber-attacks can redraw international power balances. Technologically superior actors can attack more effectively in cyberspace, while actors unable to develop defense capabilities become vulnerable. This situation will reveal the power balance in international relations from a technological perspective.

It is unavoidable that AI-powered attacks will impact political tensions as one of their potential impact centers. Using AI for attacks to manipulate political processes and public opinion will also entail political tensions. Organization of attacks such as interfering in elections, conducting smear campaigns against political opponents, and imposing mass

[47] Ramanpreet Kaur, et al., "Artificial Intelligence for Cybersecurity: Literature Review and Future Research Directions", *Information Fusion*, 97, 2023, p. 4-5.

[48] Zeinab Rouhollahi, "Towards Artificial Intelligence Enabled Financial Crime Detection", arXiv preprint arXiv:2105.10866. 2021, p. 10-11.

[49] Blessing Guembe et al. "The Emerging Threat of Ai-driven Cyber-attacks: A Review", *Applied Artificial Intelligence,* 36:1, 2022, p. 17

[50] John P. Caves, Jr., and W. Seth Carus, "The Future of Weapons of Mass Destruction: Their Nature and Role in 2030 ", Occasional Paper 10 National Defense University, 2021, p.52

[51] Eric Gartzke, "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth", *International Security,* 43:2, 2019, p. 64.

[52] Ben Buchanan, *The Cybersecurity Dilemma*, Oxford University Press, 2020, p. 118.

[53] John R. Lindsay, "The Impact of China on Cybersecurity: Fiction and Friction", *International Security,* 39:3, 2015, p. 33.

[54] Paul K. Davis, "Deterrence, Influence, Cyber-attack, and Cyberwar", *New York University Journal of International Law and Politics*, 47:2, 2014, p. 345.

censorship is also possible. Using AI to organize these attacks will both easily disable the tracking mechanism and expand the impact area. One possible consequence of this may be the wounding of democratic processes. As a result of the attacks, radicalizing public opinion, fueling tension between ethnic and religious groups, and encouraging protests can create social unrest.[55] In addition, deepfakes can undermine the credibility of politicians and institutions by shaking confidence, leading to legitimacy crises.[56] All of these actions may weaken political regimes by increasing the risks of social conflict. As a result, AI can become a means of political instability on a global scale.

AI-supported cyber-attacks in cyber security profoundly affect the international security paradigm. The digitization of the attack-defense balance and technological determinism factors transform the power structures in international relations. Uncertainties regarding attack and defense capabilities also reveal dangerous insecurity dynamics. By its very nature, cyber-attacks that may occur with the support of AI can trigger conflicts intentionally or accidentally, revealing new obstacles to cooperation that may arise in cyber security. All these show that new policies and practices are required in the AI age to maintain international peace and stability.[57] Developing global cyber security regimes and confidence-building measures are of vital importance.

On the other hand, regional security organizations will also gain significant importance. The North Atlantic Treaty Organization (NATO), the European Union (EU), and similar platforms can develop joint cyber defense mechanisms for their member states. Also, under the United Nations (UN) roof, there is an urgent need to establish a global agreement and rules regulating cyberspace.[58] Otherwise, global stability will be under serious threat.

4. Economic Impacts

The economic impact of AI-enabled cyber-attacks has become one of the most critical issues in today's global security environment. This section will examine the transformative impact of AI on cyber-attacks and its economic implications in light of the findings of the literature review. The reviewed studies show that AI technologies have made cyber-attacks more sophisticated, accessible, and widespread. These developments significantly impact a wide range of issues, from financial systems and critical infrastructure to intellectual property rights and the economics of attacks. The section provides a detailed analysis of these impacts, which is critical to understanding the economic dimension of AI-enabled cyber-attacks and assessing potential future threats.

Attacks on financial institutions, stock markets, and banking systems are likely to threaten stability.[59] AI-assisted attacks will make manipulating markets and disrupting money flows easier. The negative effects of attacks leaving profound impacts in a short period are reflected to a great extent. Another significant impact of AI-supported cyber-attacks is that

[55] Julien Nocetti, "Contest and Conquest: Russia and Global Internet Governance", *International Affairs,* 9:1, 2015, p. 120.

[56] Renee DiResta, "Computational Propaganda: If You Make It Trend, You Make It True", *Yale Law Journal*, 127:7, 2018, p. 2469.

[57] Paul Scharre, *Army of None: Autonomous Weapons and the Future of War*, WW Norton & Company, 2018, p. 242-243.

[58] Charles A. Jordan, Exploring the Cybersecurity Skills Gap: A Qualitative Study of Recruitment and Retention from a Human Resource Management Perspective, *Northcentral University ProQuest Dissertation & Theses,* 29320493, 2022, p. 95.

[59] Antoine Bouveret, "Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment.", *IMF Working Paper* No. 2018/143, p. 17. https://www.imf.org/en/Publications/WP/Issues/2018/06/22/Cyber-Risk-for-the-Financial-Sector-A-Framework-for-Quantitative-Assessment-45924, accessed 11.07.2024.

attacks on critical infrastructures such as energy networks and transportation infrastructures may have side effects such as damage to trade and increased logistics costs.[60] The sudden and rapid development of attacks will make economic recovery, stabilization, and trade balance challenging. Beyond the impact on production and the supply chain, attacks that compromise highly sensitive information, such as intellectual property theft and data breaches, may have more profound consequences in the long term.[61] Such attacks can undermine companies' competitive advantage and slow their economic growth. As a result, all these broader impacts can hinder economic growth and lead to increased unemployment, which in turn undermines national and global economic stability.

When we look at the economic dimension of cyber-attacks, AI's development has made cyber-attacks more accessible and widespread. This has caused AI to reduce the cost of cyber-attacks further.[62] Actions that previously required hacking skills can now be easily performed by anyone. AI-powered cyber-attack tools have become available on the dark web at cheap and accessible prices.[63] This has led to automation, providing a mechanism that requires less manpower and time to plan, execute, and manage attacks. This cost reduction has made these cyber-attacks more accessible to more people or groups. As a natural consequence, everyone can now become a cyber-attacker. In addition, cloud-based attack services have also evolved to be highly accessible.[64] These for-hire attacks have taken the form of a subscription-based service. Decreased costs for this type of attack have made it easier for various actors to carry out these attacks.[65] As a result, AI-enabled cyber-attacks pose a greater variety and volume of threats than traditional cyber-attacks. They also allow non-state actors and individual hackers to participate more effectively on the international stage.

To summarize, the economic consequences of AI-enabled cyber-attacks are far-reaching and significant. These implications, which range from risks to financial system stability to damage to critical infrastructure, theft of intellectual property, and reduced assault costs, pose a severe threat to national and global economic stability. The literature review demonstrates that AI has made cyber-attacks more sophisticated, accessible, and widespread. This issue highlights the limitations of standard cyber security measures and the necessity for new defense techniques. The decreased cost of attacks and the increased number of attack tools democratizes cyber threats, making international security more complicated and uncertain. Established power dynamics are challenged as non-state actors and individual hackers become more active in the international arena. The international community must evaluate its cybersecurity plans and collaboration procedures in such a situation. In this new climate, where economic security and cybersecurity are increasingly interwoven, countries and international organizations must take a more proactive and collaborative approach to AI-driven threats.

5. Imbalances between Countries

AI-backed cyber-attacks create a significant power asymmetry between developed and developing countries.[66] Differences in technological competence have led to chasms in the

[60] Nir Kshetri, *Cybercrime and Cybersecurity in the Global South (*International Political Economy Series), 1st ed. Edition, Palgrave Macmillan, 2013, p. 34-35.

[61] James P. Farwell and Rafal Rohozinski, "The New Reality of Cyber War", *Survival: Global Politics and Strategy*, 54:4, 2012, p. 113.

[62] Max Smeets, 2018, p. 20.

[63] Joseph Nye, 2021, p. 7.

[64] P.W. Singer and Allan Friedman, *Cybersecurity: What Everyone Needs to Know*, Oxford University Press, 2014, p. 119-120.

[65] Nir Kshetri, 2013, p. 70.

[66] Adam Segal, "The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate In The Digital

attack and defense capabilities of the countries. This section examines how differences in technological capabilities lead to gaps in countries' offensive and defensive capabilities and their implications for international relations.

The US and China stand out as pioneers in AI and cybersecurity. Both countries have become dominant powers in this field thanks to their human resources and research infrastructures.[67] In contrast, underdeveloped countries appear to be highly vulnerable to cyber-attacks. This situation can affect power dynamics in international relations and lead to imbalances.

As the leading countries in AI technologies and cybersecurity, the US and China's rivalry significantly shapes developments in this field. Both countries see AI as a critical tool to strengthen their cyber-attack and defense capabilities and invest heavily in this area. The US allocates significant budgets to AI-supported cyber defense programs through federal agencies. In particular, Defense Advanced Research Projects Agency (DARPA) projects focus on using AI technologies to detect and prevent cyber-attacks.[68] In addition, American companies also play a pioneering role in this field, developing AI-enabled security solutions.

On the other hand, China also aims to play a global leadership role in this field through its strategic initiatives, such as the "Next Generation Artificial Intelligence Plan."[69] China conducts intensive research and development activities, especially in deep learning and machine learning, and uses AI to increase its cyber-attack and defense capabilities.

The rivalry between these two superpowers is also reflected in cyber security. Both sides try to utilize AI technologies to gain the upper hand in cyberspace. This rivalry brings the risk of a "cyber arms race."[70] Countries invest more in cyber programs to increase their deterrence capacity, which may increase mutual distrust.

Moreover, the geopolitical rivalry and power struggle between the US and China is also echoed in cyberspace. Both countries seek to undermine each other's cyber capabilities and maintain superiority. In this context, AI-enabled cyber-attacks and countermeasures become a strategic tool.[71] On the other hand, this rivalry also affects other countries. Developing countries may become more vulnerable to AI-enabled cyber-attacks due to their technological backwardness. Therefore, technology transfer and capacity-building efforts led by the US and China are needed.[72]This digital divide trend based on AI harbors risks of powerful states incorporating weaker states into their spheres of influence.[73] For a balanced international cyber security environment, technology transfer and capacity-building efforts are urgently required.[74]

Age", *PublicAffairs*, New York, 2016, p. 96.

[67] Tkacheva, Olesya, et al. "Internet Freedom and Political Space", *Santa Monica, CA: RAND Corporation*, 2013, p. 106.

[68] About DARPA, https://www.darpa.mil/about-us/about-darpa , accessed 11.07.2024.

[69] Graham Webster, Rogier Creemers, Elsa Kania and Paul Triolo, "China's 'New Generation Artificial Intelligence Development Plan'", 2017, https://digichina.stanford.edu/work/full-translation-chinas-new-generation-artificial-intelligence-development-plan-2017/, accessed 29.07.2024.

[70] Eric Gartzke, "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth", *International Security,* 43:2, 2019, p. 56.

[71] John R. Lindsay, "The Impact of China on Cybersecurity: Fiction and Friction", *International Security*, 39:3, 2015, p. 39.

[72] Brandon Valeriano, Benjamin M. Jensen and Ryan C. Maness, *Cyber Strategy: The Evolving Character Of Power And Coercion,* Oxford University Press, New York, 2020, p. 147.

[73] Joseph Nye, "Deterrence and Dissuasion in Cyberspace", *International Security,* 41:3, 2017, p. 58.

[74] Brandon Valeriano, Benjamin M. Jensen., & Ryan C. Maness, 2020, p. 128.

In a globalizing world, AI-backed cyber threats pose new risks to international security and relations. The superiority of developed countries in AI creates a deep "digital divide" threat on the North-South and West-East axis.[75] Major powers like the US, Russia, and China try to build a deterrent superiority in cyberspace by using their advanced AI research and qualified human resources advantages. In contrast, developing countries and small states are vulnerable due to inadequate technological infrastructures. This situation leaves them unprotected against AI-backed attacks.[76]

Imbalances in cyberspace can also lead to the disruption of traditional power relations. Some technologically lagging actors can easily carry out effective cyber operations thanks to easily accessible AI tools.[77] This possibility can create new and unpredictable threats in the international system. AI-backed attacks can also lead to diplomatic crises, confidence crises, and even economic losses in target countries. International trade and financial flows are directly affected by these attacks.

Capacity-building through cooperation and technology transfer is vital for establishing a balanced and equitable global cyber security order.[78] Developed countries should support developing countries through personnel training and technology transfer. In this way, all states can achieve a minimum deterrence and defense capability in cyberspace. Otherwise, an uncontrolled cyber arms race and AI technologies becoming destabilizing tools will be inevitable.

As a result, the disparity between AI-powered cyber-attacks and defense capabilities poses new and complex challenges to international relations. While developed countries, particularly the US and China, have gained a significant advantage, developing countries become increasingly vulnerable. This situation may alter established power dynamics and create new security risks. The international community must close the technical gap immediately and create a more equal cybersecurity environment. Technology transfer, capacity-building, and international cooperation are essential for meeting these difficulties. Otherwise, an unrestrained cyber arms race and the use of AI technology as destabilizing instruments will be unavoidable.

6. Inadequacy of Defense Measures

The rapid penetration of AI technologies into the field of cyber-attacks has also affected known security mechanisms. This section examines how AI-enabled cyber-attacks transform the international security paradigm and its implications for the global balance of power. Traditional security approaches are insufficient against cyber-attacks.[79] Especially deep learning and machine learning algorithms offer attackers unpredictable and unusual opportunities.[80] Cybercriminals can use these technologies to bypass defense mechanisms and continuously adapt their attacks.[81]

[75] Blessing Guamge et al., "The Emerging Threat of Ai-driven Cyber-attacks: A Review", *Applied Artificial Intelligence*, 36:1, 2022, p. 3-4.

[76] Ramanpreet Kaur et. al, "Artificial Intelligence for Cybersecurity: Literature Review and Future Research Directions", I*nformation Fusion*, 97: 101804, 2023, p. 7-9.

[77] Iram Bibi et al., "Deep AI-powered Cyber Threat Analysis in IIoT*", IEEE Internet of Things Journal*, 2022, p. 7750.

[78] Azza Bimantara, "The Normative Enactment of International Cybersecurity Capacity Building Assistance: A Comparative Analysis on Japanese and South Korean Practices", *Global: Jurnal Politik Internasional*, 24:1, 2022, p. 111.

[79] Blessing Guamge et al., "The Emerging Threat of Ai-driven Cyber-attacks: A Review", *Applied Artificial Intelligence*, 2022, p. 9.

[80] Ramanpreet Kaur et. al. 2023, p. 14.

[81] Sherali Zeadally et. al., "Harnessing Artificial Intelligence Capabilities to Improve Cybersecurity", *IEEE Access*, vol. 8, 2020, p. 23819.

In contrast, the use of AI in security solutions progresses very slowly. Barriers to progress include the complexity of AI, lack of human resources, cost, and other reasons that keep defenses weak. While attackers can quickly develop new attack vectors using AI tools, defense systems are slow to prepare updates against these attacks. This delay in defense gives attackers a serious advantage. Thus, there is a deep gap between AI-enabled attacks and the measures taken against them. In particular, the fact that AI-supported attacks are conducted by combining many different technologies makes it very difficult for defense systems to produce solutions and respond to them. Therefore, defense measures need to be effective against all these technologies.[82] However, developing and implementing such comprehensive solutions is difficult and costly.

One final factor that complicates defense measures is the lack of coordination. Different organizations adopt different security solutions. These differences prevent systems from working in harmony, leading to defense weaknesses. The imbalance caused by all these factors in cyber security is defined as the "artificial intelligence arms race" and needs to be supported by tailored policies and cooperation to prevent a possible crisis.[83] Otherwise, AI vulnerabilities are likely to deepen and reach uncontrollable dimensions. Governments and the private sector should invest in integrating AI into defense systems and training qualified human resources.[84] Without such a collective effort, it seems impossible to effectively prevent today's cyber threats.

Finally, the inadequacy of defense measures has profoundly impacted the international security environment in the face of AI-driven cyber-attacks. States have been forced to allocate more resources to cyber programs to increase their deterrence capacity against such attacks. However, this has further reinforced insecurity in the international arena.[85] Moreover, the uncertainties about the sources of AI-assisted attacks have fueled suspicions and misunderstandings between states.[86] All these efforts to strengthen defense systems and the environment's infrastructure suitable for misunderstanding have become a source of significant problems in the international environment.

In conclusion, the current state of AI-enabled cyber-attacks has led to a critical transformation in the international security environment. Factors such as the inadequacy of traditional defense mechanisms, technological complexity, lack of qualified human resources, and coordination problems put the defense side at a disadvantage. Moreover, the uncertainty about the source of AI-assisted attacks paves the way for misunderstandings and potential conflicts in inter-state relations. Comprehensive and coordinated efforts are needed at both national and international levels to deal with this complex and dynamic threat environment.

7. Cybercrime and Economic Losses

Integrating AI technologies into cybercrime poses an increasing threat to the global economy. This section examines the economic impact of AI-enabled cybercrime from a multi-dimensional

[82] Blessing Guamge et al., "The Emerging Threat of Ai-driven Cyber-attacks: A Review", *Applied Artificial Intelligence,* 36:1, 2022, p. 12-15.

[83] Iram Bibi et al., "Deep AI-powered Cyber Threat Analysis in IIoT", *IEEE Internet of Things Journal*, 2022, p. 7751.

[84] Charles A. Jordan, "Exploring the Cybersecurity Skills Gap: A Qualitative Study of Recruitment and Retention from a Human Resource Management Perspective", Northcentral University ProQuest Dissertation & Theses, 2022, p. 59.

[85] Erik Gartzke and Jon R. Lindsay, "Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace", *Security Studies*, 24:2, 2015, p. 331.

[86] P. Caves Jr. and W. Seth Carus, "The Future of Weapons of Mass Destruction: Their Nature and Role in 2030", Occasional Paper 10 National Defense University, 2014.

perspective. Critical sectors such as finance, energy, transportation, healthcare, and education have become targets of these next-generation threats, seriously jeopardizing the countries' economic stability and growth.[87] This section will discuss the impacts of AI-enabled cybercrime on various economic sectors in light of examples from past cases and potential future scenarios. It will also assess the cost of these threats to the global economy and their long-term implications for the economic security of countries. This analysis highlights the urgency and importance of the measures governments, the private sector, and the international community need to take against AI-enabled cyber threats.

While cyber-attacks cause serious economic damage to countries even before they merge with AI, the scale of these impacts will inevitably increase if combined with AI. For example, the WannaCry ransomware attack that shook the world in 2017 caused billions of dollars in damage to the global economy. The attack affected computers in more than 150 countries, shut down production facilities, and disrupted many others.[88] If an attack on a similar scale is supported by AI, the effects will be more extreme. Similarly, a cyber-attack on the Colonial Pipeline in 2021 seriously compromised the US oil and gasoline supply, leading to long queues in pumps and a rise in fuel prices. The attackers demanded $4.4 million in ransom from the company, threatening the country's energy security.[89] These cybercrimes, carried out at highly critical points, may have the capacity to do much more harm when supported by AI.

The increasing impact of AI on cybercrime has led to a significant increase in cyber fraud cases, particularly in the banking and finance sectors. Fraud, phishing attacks, credit card fraud, and money transfer hacking have become more widespread than ever with the support of AI.[90] Such attacks undermine the reliability and stability of the financial system, leading to economic losses. In addition, attacks on critical infrastructures cause disruptions in many services, from energy production and transportation systems to hospitals and schools. Many types of attacks, such as stopping production lines and canceling operations, have become easier and more destructive with the effect of AI.[91] This situation disrupts the economic activities and supply chains of countries.

Experts warn that AI-enabled cybercrime could cost the global economy more than $1 trillion annually, equivalent to more than 1% of global net domestic product (GDP).[92] In addition, large-scale data theft and infringement of intellectual property rights ruin research and development (R&D) investments[93]. As a result of all these factors, the growth rate of both national and global economies slows down.

[87] Ramanpreet Kaur et. al. 2023, "Artificial Intelligence for Cybersecurity: Literature Review and Future Research Directions", *Information Fusion,* 97:101804, 2023, p. 9.

[88] Ramanpreet Kaur et. al. 2023, p. 11.

[89] Sean Micheal Kerner, "Colonial Pipline Hack Explained: Everything You Need to Know", 2022, https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know , accessed 31.08.2024.

[90] Terence Huang, "The Dark Alliance: Addressing the Rise of AI Financial Frauds and Cyber Scams", 2024, https://sites.lsa.umich.edu/mje/2024/02/14/the-dark-alliance-addressing-the-rise-of-ai-financial-frauds-and-cyber-scams/ accessed 31.08.2024.

[91] Shaji George, et al.,"Cyber Threats to Critical Infrastructure: Assessing Vulnerabilities Across Key Sectors", *Partners Universal International Innovation Journal (PUIIJ),* 02:01, 2024, p. 57.

[92] Steve Morgan, 2020, "Cyberwarfare in C-Suite", https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/ , accessed 31.08.2024.

[93] Sherali Zeadally et. al., "Harnessing Artificial Intelligence Capabilities to Improve Cybersecurity", *IEEE Access*, 8, 2020, p. 23830.

In conclusion, the economic impact of AI-enabled cybercrime poses a serious threat on national and global scales. Attacks on critical sectors such as finance, energy, transportation, and healthcare jeopardize economic stability and growth. The WannaCry and Colonial Pipeline cases illustrate the potentially devastating impact of such attacks with the possible integration of AI technologies. The rise in cyber fraud cases undermines the credibility of the financial system, leading to economic losses. Economic actors need to be aware of and prepared for these next-generation threats. Only in this way will it be possible to minimize the economic impact of AI-driven cybercrime and protect sustainable economic growth.

8. Need for International Cooperation and New Rules

The rapid evolution of AI technologies has ushered in a new era of cybersecurity challenges that transcend national borders and traditional security paradigms. This section examines the pressing need for enhanced international cooperation and the establishment of new regulatory frameworks to address the complex threats posed by AI-backed cyber-attacks. It is important to consider how AI-backed attacks affect international security frameworks. We must recognize that in the face of cyber-attacks aided by AI, current international security frameworks are insufficient.[94] Cyber risks have not been included in traditional disarmament and control systems. For instance, the Nuclear Non-Proliferation Treaty (NPT) does not mention cyber weapons.[95] However, on a positive note, chemical and biological hazards are a focal point of the UN disarmament agenda.[96] As a result, the world community is confronted with a legal vacuum regarding the constantly changing cyber threats.

It becomes urgently necessary to create new standards and guidelines. The uncertainties in the cyber globe can be resolved only via multilateral diplomatic efforts. If not, an unchecked cyber arms race will inevitably occur. It is crucial to create a specific legal framework for cyber security within the UN. Regional platforms also need to develop their joint defense mechanisms.

Reports prepared by the UN Group on the Peaceful Uses of Cyber Space (UN GGE) reflect international efforts on cybersecurity. The 2013 and 2015 reports have identified standards to be followed in cyberspace.[97] However, these norms are not binding. The Budapest Convention on Cybercrime (2001), prepared by the Council of Europe, is the first binding treaty to define cybercrimes and provide international cooperation to combat these crimes.[98] However, this convention does not cover AI-supported cyber-attacks. NATO's Cyber Defense Policy (2014) aims to strengthen allies' cyber defense capabilities and enhance cooperation.[99] Nevertheless, this policy also does not focus on AI technologies. On the other hand, Shanghai Cooperation Organization (SCO) members pledged to cooperate on cybersecurity in 2009.[100] However, this commitment is not binding and does not cover AI-supported attacks.

[94] Irshaad Jada and Thembekile O. Mayayise, "The Impact of Artificial Intelligence on Organisational Cyber Security: An Outcome Of A Systematic Literature Review", *Data and Information Management*, 8:2:100063, 2024, p. 8.

[95] Treaty on the Non-Proliferation of Nuclear Weapons (NPT), https://disarmament.unoda.org/wmd/nuclear/npt/, accessed 20.07.2024.

[96] "Securıng Our Common Future", Office for Disarmament Affairs New York, 2018 An Agenda for Disarmament, www.un.org/disarmament/sg-agenda, accessed 20.07.2024.

[97] Bart Hogeveen, "The UN norms of responsible state behaviour in cyberspace", International Cyber Policy Center, 2022, https://documents.unoda.org/wp-content/uploads/2022/03/The-UN-norms-of-responsible-state-behaviour-in-cyberspace.pdf, accessed 20.07.2024.

[98] "Convention on Cybercrime", European Treaty Series - No. 185, Council of Europe, Budapest, 23.9.2021. https://rm.coe.int/1680081561, accessed 20.07.2024.

[99] "Cyber Defence", 2023, https://www.nato.int/cps/en/natohq/topics_78170.htm#:~:text=At%20the%202014%20NATO%20Summit,5%20of%20NATO's%20founding%20treaty, accessed 20.07.2024.

[100] "Shanghai Cooperation Organisation", https://ccdcoe.org/organisations/sco/, accessed 20.07.2024.

Existing international treaties and texts do not fully address the threats posed by AI-supported cyber-attacks in general terms. Therefore, new legal frameworks and binding agreements are needed to fill the gap.

Non-governmental actors must also be involved in this process. Dialogue and cooperation with leading technology companies and civil society organizations are vital. The rules governing the cyber world can only be defined with a multi-party approach. Without this kind of collective effort, the world will inevitably face one of the most significant global threats of the 21st century.[101]

There are necessary steps to be taken in international law and diplomacy. Existing disarmament and control regimes must be updated to cover cyber weapons and AI-supported attacks. In this context, the role of organizations such as the UN Disarmament Commission (UNDC) and the International Telecommunications Union (ITU) is critical.[102]

It is also imperative to take confidence-building measures among countries. Detection of the source of cyber-attacks, transparency, information sharing, joint exercises, and training are steps that will increase mutual trust.[103] These steps will also prevent misunderstandings and unintentional clashes.

As a result, AI-backed cyber-attacks threaten global security, requiring urgent and coordinated action by the international community. Creating new legal frameworks, taking confidence-building measures, and strengthening multilateral cooperation are the keys to dealing with this threat. Otherwise, the world could be dragged into an uncontrolled cyber arms race and instability.

Conclusion

AI-enabled cyber-attacks constitute one of the most important international security threats of the 21st century. These attacks have the potential to profoundly affect the offense-defense balance, security regimes, inter-state relations, and the global political economy. This study has comprehensively examined the potential impacts of AI-enabled cyber-attacks on international relations and global security. The research has revealed how these next-generation threats transform traditional security paradigms and create new challenges in the international system. The findings show that AI technologies have made cyber-attacks more sophisticated, accessible, and pervasive. These developments have significantly impacted a wide range of issues, from financial systems and critical infrastructure to intellectual property rights and the economics of attacks. In particular, the decreasing cost of AI-enabled cyber-attacks and the proliferation of attack tools democratize cyber threats and make the international security environment more complex and uncertain. The international community needs to take urgent and coordinated measures against this threat.

First, the international community should develop new regimes to limit AI-enabled cyber weapons. In this context, a "Convention on Artificial Intelligence and Cybersecurity" should be negotiated and adopted within the UN. This convention should define AI-enabled attacks, mechanisms for international cooperation to combat them, and norms to be observed.

[101] "Cyber Capabilities and National Power Volume 2", The International Institute For Strategic Studies, https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/2023/09/cyber-capabilities-and-national-power-vol-2/cyber-capabilities-and-national-power_volume-2.pdf, p.63., accessed 20.07.2024.

[102] United Nations Meeting Coverages, Seventy-Eighth Session, 20th & 21st Meeting, 24 October 2023, https://press.un.org/en/2023/gadis3725.doc.htm, accessed 20.07.2024.

[103] Paul Scharre, *Army of None: Autonomous Weapons and the Future of War*, WW Norton & Company, 2018, p. 212-213.

Furthermore, an international mechanism should be established to oversee this convention's implementation and the parties' compliance.

The international community and institutions should carry out numerous responsibilities to address the threat of AI-enabled cyber-attacks to international peace and security. First, the UN should establish a new regime of disarmament and confidence-building measures in cyberspace. This regime should prohibit developing, producing, and using AI-based cyber weapons and include transparency mechanisms and oversight processes. A permanent Cyber Security Council should also be established within the UN, setting policies and regulations to prevent AI-based cyber-attacks. This Council would conduct disarmament negotiations and implement mechanisms of transparency and oversight. It would be funded by contributions from member states and employ specialized staff.

Second, joint cybersecurity centers should be established to increase cooperation between countries, especially for AI-based attacks, and information-sharing mechanisms should also be developed. The private sector should also be involved in these efforts, encouraging technology companies to comply with cybersecurity standards. Third, new diplomatic norms and codes of conduct should be established. For example, targeting critical infrastructure should be prohibited, and agreements should be reached on a proportionate response to attacks.

Fourth, the international community should invest in human and technical capacity-building in AI and cybersecurity. In particular, developed countries should provide developing countries with training and infrastructure support in these areas. Through this cooperation, the technological divide can be avoided, and the risks of power imbalances can be reduced. Finally, a sense of collective responsibility for maintaining international peace should be developed, and awareness-raising efforts should be carried out. It should be emphasized that AI should be managed and supervised following ethical and humanitarian values to contribute to human welfare.

When we look at the responsibilities of states in general, they should increase their investments in cyber security and strengthen cooperation in this field. Particularly, the focus should be on helping to build the capacities of developing countries. Activities such as technology transfer, personnel training, and joint exercises will strengthen the defense capabilities of developing countries. In addition, universities and educational institutions should conduct more programs to train qualified human resources in cyber security.

In addition, measures should be taken to increase transparency and trust between states. Detecting the source of cyber-attacks, information sharing, and joint exercises will increase mutual trust. These activities can help the states to avoid misunderstandings and unintentional conflicts. Furthermore, regional security organizations should develop joint cyber defense mechanisms and strengthen the capacities of member states. Also, dialogue and cooperation among governments, technology companies, and civil society organizations should be strengthened. Developments in AI and cybersecurity need to be addressed with a multi-stakeholder approach. Technology companies can have a vital role in addressing vulnerabilities and improving defense mechanisms. Civil society organizations can help raise public awareness and contribute to policy processes.

Finally, combating AI-enabled cyber-attacks should be treated as part of human security, not just as a technical issue. Cybersecurity policies should be designed to protect the rights and freedoms of societies and individuals. At the same time, principles such as gender equality and inclusiveness should be considered when formulating these policies.

As a result, the research reveals that current defense measures are insufficient against AI-powered cyber-attacks. Traditional security approaches are ineffective against this new generation of threats. This situation leads to a serious transformation in the international security environment and forces states to allocate more resources to increase their deterrence capacity. Moreover, another important finding of the study is that AI-enabled cyber-attacks create a significant power asymmetry among countries. While developed countries, especially the US and China, gain significant advantages, developing countries become increasingly vulnerable. This asymmetry has the potential to alter established power dynamics and create new security risks. Ultimately, our findings suggest that the international community needs to take urgent and coordinated actions against AI-enabled cyber threats. Creating new legal frameworks, adopting confidence-building measures, and strengthening multilateral cooperation are keys to tackling this threat. Otherwise, the world could be plunged into an uncontrolled cyber arms race and instability.

In conclusion, this study emphasizes that maintaining international peace and stability in the age of AI requires collective action and a sense of responsibility. Strengthened dialogue and cooperation among the international community, governments, technology companies, and civil society organizations is critical to tackling this complex threat. The study has taken a step forward in understanding the impact of AI-enabled cyber threats on international security and developing policy recommendations to address these threats. However, there is still a need for continued research and collaboration in this rapidly evolving field.

Conflict of Interest Statement:

The author declares that there is no conflict of interest.

REFERENCES

Published Works

AJDER Henry PATRINI Giorgio CAVALLI Francesco and CULLEN Laurence (2019). "The State of Deepfakes: Landscape, Threats, and Impact", *Deeptrace*, 1-28.

BIBI Iram and AKHUNZADA Adnan (2022). "Deep AI-powered Cyber Threat Analysis in IIoT", *IEEE Internet of Things Journal*, 9:10, 7748-7763.

BIMANTARA Azza (2022). "The Normative Enactment of International Cybersecurity Capacity Building Assistance: A Comparative Analysis on Japanese and South Korean Practices", *Global: Jurnal Politik Internasional,* 24:1, 109-138.

BUCHANAN Ben (2020). *The Cybersecurity Dilemma,* Oxford University Press, Oxford.

CAVELTY Myriam Dunn and WENGER Andreas (2022). *Cyber Security Politics: Socio-Technological Transformations and Political Fragmentation*, 1st Edition, Routledge, New York.

CAVES John P. Jr. and CARUS W. Seth (2021). *The Future of Weapons of Mass Destruction: Their Nature and Role in 2030*, Occasional Paper 10, National Defense University Press, Washington.

CRESWELL John W. and CRESWELL David (2022). *Research Design: Qualitative, Quantitative and Mixed Methods Approaches*, SAGE Publications, California.

DAVIS Paul K. (2014). "Deterrence, Influence, Cyber-attack, and Cyberwar", *New York University Journal of International Law and Politics*, 47:2, 327-355.

DiRESTA Renee (2018). "Computational Propaganda: If You Make It Trend, You Make It True", *Yale Law Journal,* 127:7, 2460-2483.

FARWELL James P. and ROHOZINSKI Rafal (2011). "Stuxnet and the Future of Cyber War", *Survival: Global Politics and Strategy,* 53:1, 23-40.

FOURNIER-TOMBS Eleonore BRUBAKER Rebecca and ALBRECHT Eduardo. (2023). "Artificial Intelligence-Powered Disinformation and Conflict", *United Nations University Centre for Policy Research*, Policy Brief, 1-12.

GARTZKE Erik (2019). "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth", *International Security*, 43:2, 41-73.

GARTZKE Erik and LINDSAY Jon R. (2015). "Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace", *Security Studies*, 24:2, 316-348.

GEORGE Shaji BASKAR Dr T and SRİKAANTH Balaji. (2024). "Cyber Threats to Critical Infrastructure: Assessing Vulnerabilities Across Key Sectors", *Partners Universal International Innovation Journal,* 2:1, 54-63.

GUEMBE Blessing AZETA Ambrose and MISRA Sanjay. (2022). "The Emerging Threat of AI-driven Cyber-attacks: A Review", *Applied Artificial Intelligence,* 36:1, 1-23.

ILLIASHENKO Olga VYACHESLAV Kharchenko IEVGEN Babeshko FESENKO Herman and GIANDOMENICO Felicita Di. (2023). "Security-Informed Safety Analysis of Autonomous Transport Systems Considering AI-Powered Cyber-attacks and Protection", *Entropy*, 25:8, 1123-1145.

JADA Irshaad and MAYAYISE Thembekile O. (2024). "The Impact of Artificial Intelligence on Organisational Cyber Security: An Outcome of a Systematic Literature Review", *Data and Information Management*, 8:2, 100063.

JOHNSON James (2019). "Artificial Intelligence & Future Warfare: Implications for International Security", *Defense and Security Analysis*, 35:2, 147-169.

JORDAN Charles A. (2022). Exploring the Cybersecurity Skills Gap: A Qualitative Study of Recruitment and Retention from a Human Resource Management Perspective, *Northcentral University ProQuest Dissertation & Theses*, 29320493.

KAUR Ramanpreet, GABRIJELČIČ Dušan and KLOBUČAR Tomaž (2023). "Artificial Intelligence for Cybersecurity: Literature Review and Future Research Directions", *Information Fusion*, 97, 1-15.

KELLO Lucas (2017). *The Virtual Weapon and International Order*, Yale University Press, New Haven.

KSHETRI Nir (2013). *Cybercrime and Cybersecurity in the Global South*, Palgrave Macmillan, London.

LeCUN Yann BENGIO Yoshua and HINTON Geoffrey (2015). "Deep Learning", *Nature,* 521:7553, 436-444.

LINDSAY John R. (2013). "Stuxnet and the Limits of Cyber Warfare", *Security Studies,* 22:3, 365-404.

LINDSAY John R. (2015). "The Impact of China on Cybersecurity: Fiction and Friction", *International Security*, 39:3, 7-47.

MORGAN Susan (2018). "Fake News, Disinformation, Manipulation and Online Tactics to Undermine Democracy", *Journal of Cyber Policy*, 3:1, 39-43.

NEUENDORF Kimberly A. (2020). "Content Analysis and Thematic Analysis", *Advanced Research Methods for Applied Psychology,* 1:2, 211-223.

NOCETTI Julien (2015). "Contest and Conquest: Russia and Global Internet Governance", *International Affairs*, 91:1, 111-130.

NYE Joseph (2017). "Deterrence and Dissuasion in Cyberspace", *International Security*, 41:3, 44-71.

ROUHOLLAHI Zeinab (2021). "Towards artificial intelligence enabled financial crime detection", arXiv preprint arXiv:2105.10866, 1-15.

SCHARRE Paul (2018). *Army of None: Autonomous Weapons and the Future of War,* WW Norton & Company, New York.

SEGAL Adam (2016*). The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age,* PublicAffairs, New York.

SINGER P. W. and FRIEDMAN Allan (2014). *Cybersecurity: What Everyone Needs to Know*, Oxford University Press, Oxford.

SMEETS Max (2018). "A Matter of Time: On the Transitory Nature of Cyberweapons", *Journal of Strategic Studies*, 41:1-2, 6-32.

TADDEO Mariarosaria McCUTCHEON Tom and FLORIDI Luciano (2019). "Trusting Artificial Intelligence in Cybersecurity Is a Double-Edged Sword", *Nature Machine Intelligence*, 1:12, 557-560.

TKACHEVA Olesya vd. (2013). "Internet Freedom and Political Space", *RAND Corporation*, Santa Monica.

VALERIANO Brandon JENSEN Benjamin M. and MANESS Ryan C. (2020). *Cyber Strategy: The Evolving Character of Power and Coercion*, Oxford University Press, New York.

ZEADALLY Sherali vd. (2020). "Harnessing Artificial Intelligence Capabilities to Improve Cybersecurity", *IEEE Access*, 8, 23817-23837.

ZEGART Amy (2018). "Cheap Fights, Credible Threats: The Future of Armed Drones and Coercion", *Journal of Strategic Studies*, 41:1-2, 6-48.

Internet Sources

"About DARPA", https://www.darpa.mil/about-us/about-darpa, accessed 11.07.2024.

BOUVERET Antoine (2018). *Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment,* IMF Working Paper No. 2018/143, International Monetary Fund, Washington. https://www.imf.org/en/Publications/WP/Issues/2018/06/22/Cyber-Risk-for-the-Financial-Sector-A-Framework-for-Quantitative-Assessment-45924 accessed 11.07.2024.

"Cyber Defence", https://www.nato.int/cps/en/natohq/topics_78170.htm, accessed 20.06.2024.

"Convention on Cybercrime", European Treaty Series - No. 185, Council of Europe, https://rm.coe.int/1680081561, accessed 20.06.2024.

"Cyber Capabilities and National Power Volume 2", The International Institute For Strategic Studies, https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/2023/09/cyber-capabilities-and-national-power-vol-2/cyber-capabilities-and-national-power_volume-2.pdf, accessed 20.06.2024.

HOGEVEEN Bart (2022). "The UN norms of responsible state behaviour in cyberspace", International Cyber Policy Center, https://documents.unoda.org/wp-content/uploads/2022/03/The-UN-norms-of-responsible-state-behaviour-in-cyberspace.pdf, accessed 20.06.2024.

HUANG Terence (2024). "The Dark Alliance: Addressing the Rise of AI Financial Frauds and Cyber Scams", https://sites.lsa.umich.edu/mje/2024/02/14/the-dark-alliance-addressing-the-rise-of-ai-financial-frauds-and-cyber-scams/, accessed 31.08.2024.

KENNEDY Allan (2023). "Ranked: Artificial Intelligence Startups, by Country", https://www.visualcapitalist.com/sp/global-ai-investment/, accessed 26.05.2024.

KERNER Sean Micheal (2022). "Colonial Pipline Hack Explained: Everything You Need to Know", https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know, accessed 31.08.2024.

MILMO Dan (2024). "Iran-backed hackers interrupt UAE TV streaming services with deepfake news", https://www.theguardian.com/technology/2024/feb/08/iran-backed-hackers-interrupt-uae-tv-streaming-services-with-deepfake-news, accessed 26.05.2024.

MORGAN Steve (2020). "Cyberwarfare in C-Suite", https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/, accessed 31.08.2024.

"Net Losses: Estimating the Global Cost of Cybercrime", Center for Strategic and International Studies, https://csiswebsiteprod.s3.amazonaws.com/s3fspublic/publication/140609_rp_economic_impact_cybercrime_report.pdf, accessed 20.06.2024.

OTTO Emily (2024). "Be-aware of AI-Enhanced Cyber-attacks", https://cepa.org/article/beware-of-ai-enhanced-cyber-attacks/, accessed 17.07.2024.

"Securing Our Common Future", Office for Disarmament Affairs New York, 2018, www.un.org/disarmament/sg-agenda, accessed 20.06.2024.

"Shanghai Cooperation Organisation", https://ccdcoe.org/organisations/sco/, accessed 20.06.2024.

"Statista - Possible usage of ChatGPT for Cyber Crime Purposes", https://www-statista-com.eu1.proxy.openathens.net/statistics/1378211/chatgpt-usage-cyber-crime-global/, accessed 17.07.2024.

"Treaty on the Non-Proliferation of Nuclear Weapons (NPT)", https://disarmament.unoda.org/wmd/nuclear/npt/, accessed 20.06.2024.

TZIAKOURIS Giannis (2023). "The rise of AI-powered criminals: Identifying threats and opportunities", https://blog.talosintelligence.com/the-rise-of-ai-powered-criminals/, accessed 26.05.2024.

United Nations Meeting Coverages, Seventy-Eighth Session, 20th & 21st Meeting, https://press.un.org/en/2023/gadis3725.doc.htm, accessed 20.06.2024.

WEBSTER Graham CREEMERS Rogier KANİA Elsa and TRİOLO Paul (2017). "China's 'New Generation Artificial Intelligence Development Plan'", https://digichina.stanford.edu/work/full-translation-chinas-new-generation-artificial-intelligence-development-plan-2017/, accessed 29.07.2024.

ZAKI Adam (2024). "85% of Cybersecurity Leaders Say Recent Attacks Powered by AI: Weekly Stat", https://www.cfo.com/news/cybersecurity-attacks-generative-ai-security-ransom/692176/, accessed 17.07.2024.