ISSUE BRIEF

INSTITUTE OF STRATEGIC STUDIES ISLAMABAD
Web: www.issi.org.pk
Phone: +92-51-9204423, 24
Fax: +92-51-9204658

AI IN CYBERSECURITY: NAVIGATING THE DUAL-EDGED SWORD OF TECHNOLOGICAL ADVANCEMENT AND EMERGING THREATS

By
Hassan Mehmood
Intern
Arms Control & Disarmament Centre, ISSI

Supervised by
Sardar Jahanzaib Ghalib

August 21, 2024

Source: Business Standard

Traditional weapon systems are revolutionizing as the world rapidly shifts towards emerging technology. Surveillance and combat methodology is evolving rapidly, this significant change is due to technological advancements. Such advancements include Artificial Intelligence (AI), Lethal Autonomous Weapon Systems (LAWS), advanced nuclear weapons, direct energy weapons, and cyber warfare. AI evolution and development are most prominent in the 20th century, with the most composite and varied domains. The ultimate motive of AI is to carry out complex tasks and mimic typical human behavior and outcomes. The wide array of concepts and theories to comprehend human intelligence are created and developed by it.[1] For the time being, numerous industries and organizations are developing and revolutionizing their systems by using AI. The most prominent and effective application of AI is "Cyber Security" which can identify threats, and ensure better vulnerability management, and security.[2] Cyber security is considered one of the vital beneficiaries of AI. Considering AI applications, it is noted that there is a contradiction with both its positive and negative implications. Its integration into

1 Meraj Farheen Ansari et al., "The Impact and Limitations of Artificial Intelligence in Cybersecurity: A Literature Review," SSRN Scholarly Paper (Rochester, NY, September 1, 2022), https://papers.ssrn.com/abstract=4323317.

2 "AI in Cybersecurity Uses & Applications," Engati, accessed July 26, 2024, https://www.engati.com/blog/ai-in-cybersecurity.

everyday life, and its applications in areas such as businesses, healthcare, and cyber security can be considered as positive sides of AI. However, its darker sides are revealed when it is used for security breaches and evil purposes.[3] Moreover, advancements in AI can enhance modern warfare capabilities such as detection and response to threats, predictive analysis, and other related functions.[4]

To monitor, analyze, detect, and respond to cyber threats simultaneously AI-driven cyber security uses developed algorithms. It detects and analyses mass amounts of data, which is considered a threat to security. It can scan the data to identify and address vulnerabilities by mitigating the common types of cyberattacks.[5] It also reduces cyber security costs as a survey by International Business Machines (IBM) indicates some organizations that use AI and automation extensively report an average cost of data breaches at US$3.60 million, which was US$1.76 million less than breaches at organizations that did not use AI and automation capabilities.[6] AI holds the potential to revolutionize numerous industries, particularly in the realm of cyber security. However, it carries significant threats that must be carefully addressed, some of which are as follows:

i. AI and generative attacks

ii. AI-powered Cyberattack

iii. AI-driven malware

The emergence of AI and generative attacks, fueled by advanced machine learning algorithms, has introduced a new risk of cyber security threats. It includes deep fakes and AI-generated phishing attacks, and these threats pose significant challenges for traditional cyber security defense. AI has the potential to provide sudden detailed and multi-layered data regarding victims' digital footprints, including their online activities and communication methods, enabling the execution of such attacks with accuracy.[7]

---

3 "Artificial Intelligence: Threats and Opportunities," Topics | European Parliament, September 23, 2020, https://www.europarl.europa.eu/topics/en/article/20200918STO87404/artificial-intelligence-threats-and-opportunities.

4 Shubhangi Srivastava, "AI in Cybersecurity Uses & Applications."

5 "What is AI in Cybersecurity?," accessed July 26, 2024, https://www.sophos.com/en-us/cybersecurity-explained/ai-in-cybersecurity.

6 Anna fitzgerald, "AI in Cybersecurity: How it's used + 8 Latest Developments | SecureFrame," accessed July 26, 2024, https://secureframe.com/blog/ai-in-cybersecurity

7 Krasimir Vatchinsky, "Generative AI Attacks and Defending the Digital Frontier," Medium (blog), April 11, 2024, https://medium.com/@krasimirvatchinsky/generative-ai-attacks-and-defending-the-digital-frontier-93935669128c.

AI-generated cyberattacks utilize artificial intelligence and natural language processing to perpetrate cyber threats. These attacks are carried out by threat actors with malicious intents who employ AI-powered models and tools to create convincing phishing emails and malware-laden links. Identifying these attacks poses a challenge due to their close resemblance to regular emails or links[8].

Moreover, in AI-driven malware, malicious actors utilize AI to generate data that mimics human behavior, making it difficult for security systems to differentiate between legitimate and fake data. For example, Black Mamba a type of AI-generated malware, successfully evaded advanced endpoint detection and response (EDR) technologies. These capabilities demonstrate the application of AI in generating increasingly sophisticated and challenging-to-detect cyber threats, thereby exacerbating the security landscape. A more precise detail is mentioned in the given table:

Challenges	Description	Impact on Security System	Recent Incident
Malware Infiltration	Malware has the potential to infiltrate automated weapons systems, compromising their functionality.	Exploitation of AI can lead to unauthorized access and control of weapons systems, resulting in potential malfunctions	Cybercriminals attempt to deploy malware targeting military drones, potentially allowing for remote hijacking.
Data Poisoning	The manipulation of training data in AI systems can lead to the introduction of malicious data, particularly in systems that control weapons.	This can cause the AI to make incorrect decisions or target unwanted entities.	It has been noted that adversaries have attempted to manipulate AI training data for military drones and other autonomous weapons to effect the targeting accuracy
AI- Enhanced Cyber Warfares	AI technologies have the potential to weponized, enabling automated attacks on enemy system, include automated weapon system.	This raise the stakes in cyber warfares, as AI can enhance the speed and efficiency of attacks	Reports have emeged of stae-sponspred actors using AI to develop sophisticated malwares aimed at disabling enemy automated weapon systems.
Exploitation of Valnerabilities	Malwares can exploit known vulnerabilities in automated systems to gain control and casue harm.	It lesds to unauthorized use of weapons or data theft of sensitive military data	In 2023, vulnerabilities in military-grade drones were exploited leading to concerns about the security of sensitive operational data

8 "What Are AI Generated Attacks?," Https://Mixmode.Ai/ (blog), accessed July 29, 2024, https://mixmode.ai/what-is/ai-generated-attacks/.

Furthermore, self-generative malware deepens its roots in the host with the ability to destroy internal capabilities, ultimately leading to data leakage and privacy issues.[9] It provides numerous advantages to both individuals and various industries, However, its widespread adaptation presents benefits and complex challenges for the next generation. In the future AI-powered solutions leverage machine learning algorithms to swiftly and precisely identify potential security threats, surpassing the capabilities of traditional methods. These systems employ anomaly detection to recognize irregular data patterns, which could signify a cyber attack, allowing organizations to respond promptly and effectively. [10]

Moreover, As AI becomes more integrated into organizations and human lives it is also considered a challenge to the next generation. This integration gives rise to some ethical and legal challenges, particularly privacy and data security. Another significant challenge of AI in cyber security is the biases in AI systems. The quality of training data deeply relies on the effectiveness of AI in cyber security. The AI systems will produce off-center results if the data is unclear or incomplete.[11]

A new trend of challenges has emerged as the complexity of modern technologies and their swift spread is increasing. The security besides the potential risks that are linked with the advanced threats needs a new and comprehensive framework of implications. Governments need to build a solutions framework of safety measures to effectively shape laws and regulations, which is considered to this rapid response to emerging threats. These laws must focus on the legal and illegal use of AI. Secondly, it is important to take some steps to conduct AI training programs on both national and international levels for awareness and to develop relative skills.[12] Allocating resources to fund AI research programs can also address the challenges. This investment will not only strengthen international ties but also help us understand and collaborate with the most advanced AI-developed countries. AI is poised to become an integral component across diverse sectors ranging from healthcare, manufacturing, and education to transportation in the future. The profound implications of AI extend to the realm of cybersecurity, demonstrating its pervasive influence in safeguarding digital assets. Nevertheless, according to a University of Oxford report, the escalating dependency on AI systems may precipitate a multitude of challenges, encompassing issues of bias

9 Rasimir Vatchinsky, "Generative AI Attacks and Defending the Digital Frontier," Medium (blog), April 11, 2024, https://medium.com/@krasimirvatchinsky/generative-ai-attacks-and-defending-the-digital-frontier-93935669128c.

10 Eli Chachak, "The Future of AI in Cybersecurity: Are We Ready?," CyberDB, June 19, 2023, https://www.cyberdb.co/the-future-of-ai-in-cybersecurity-are-we-ready/.

11 "The Benefits And Challenges of AI in Cyber Security," May 2, 2023, https://www.metacompliance.com/blog/data-breaches/benefits-and-challenges-of-ai-in-cyber-security.

12 Bill Gates, " How to Manage Risks of AI | LinkedIn," accessed July 26, 2024, https://www.linkedin.com/pulse/how-manage-risks-ai-bill-gates/.

and the dissemination of misinformation.[13] As a result, the pervasive integration of AI presents a complex landscape characterized by both promising opportunities and considerable obstacles, especially for succeeding generations to navigate.[14]

13 Professor Brent Mittelstadt, "Expert Comment: No Need to Wait for the Future, the Danger of AI Is Already Here | University of Oxford," May 15, 2023, https://www.ox.ac.uk/news/2023-05-15-expert-comment-no-need-wait-future-danger-ai-already-here.

14 Brenda Wairimu, The Future of Artificial Intelligence: Opportunities and Challenges | LinkedIn," accessed July 26, 2024, https://www.linkedin.com/pulse/future-artificial-intelligence-opportunities-brenda-wairimu/.