JOURNAL OF SOCIAL SCIENCES AND HUMANITIES RESEARCH FUNDAMENTALS

VOLUME03 ISSUE10
DOI: https://doi.org/10.55640/jsshrf-03-11-10 Pages: 43-46

EMERGING SECURITY CONCERNS BECAUSE OF AI USAGE

Nurmukhammad Y. Samijonov
Independent Researcher, Tashkent State University Of Oriental Studies, Uzbekistan

ABOUT ARTICLE

Key words: Disruptive AI, Project Maven, the "third revolution in warfare", bias, deepfakes, discrimination.

Received: 14.11.2023
Accepted: 19.11.2023
Published: 24.11.2023

Abstract: Recently, there has been a lot of hype surrounding AI, bringing urgent concerns along with lots of myth, as the future of AI is still uncertain. While social media headlines warn that AI is about to outperform humans in near future, there's a good chance that attacks made possible by the increased application of AI will be very potent, precisely targeted, hard to identify, and likely to take advantage of holes in AI systems. This article analyzes the emerging security issues that are forming in the way AI is used in practice.

INTRODUCTION

Along with gunpowder and nuclear weapons, autonomous weapons and robotics are commonly referred to as the "fourth industrial revolution" or the "third revolution in warfare"(Johnson, 2019, p.6). The safety and vulnerability of AI are also security concerns. Even if society can benefit much from the specialized AI, it can also be tricked, spied on, or misled (Radulov, 2019, p.3). As AI is being used in society in multiple fields, the range of vulnerability is getting wider.

METHODS. Comparative, content and event analysis were used in this article.

RESULTS

Artificial intelligence assaults primarily impact five domains: content filters, law enforcement, military, civil society, and AI replacing duties that were previously performed by humans. Due to their increasing use of artificial intelligence for crucial functions, these domains are becoming increasingly vulnerable and appealing targets for attacks (Comiter, 2019). The global fight against crime can be significantly improved by early danger detection, precise forecasts in a diverse period, delivered sufficiently and promptly, and supported by comprehensive multi-factor scenarios of management decisions (Radulov, 2019, p.3).

AI may be utilized for both criminal investigation and prevention because of its enormous data analysis capacity. Currently, the police use robots for search and rescue missions, explosive device disposal during terrorist attacks, and even the destruction of armed offenders. Another task that AI can successfully complete with the right training is searching social networks for individuals who could be radicalized. In order to stop efforts to recruit new members of terrorist groups like ISIS and others,

various law enforcement agencies currently use social networking monitoring and analysis (Radulov, 2019, p.5). On the other hand, because of biased training data or algorithmic design, AI systems may unintentionally reinforce or magnify societal biases. It is essential to make investments in the creation of objective algorithms and a variety of training data sets in order to reduce discrimination and guarantee fairness. Deepfakes and other AI-generated content are used to manipulate public opinion and propagate misleading information. In the digital age, efforts to identify and counteract misinformation produced by AI are essential to maintaining the integrity of information.

While machine learning and generative AI programs are causing restrictions and sometimes phobias among local citizens in some countries, there have already been situations where they have been welcomed with open arms in some countries, and if necessary, they have been recommended to govern the state. For example, on March 31, 2023, Italy imposed a ban on the use of ChatGPT on Italian territory, becoming the first Western country to ban ChatGPT collectively. Illegal distribution of personal data and lack of legal basis for the distributed data were cited as the basis for this. The ban was lifted on April 28 only after nearly a month of discussions and improved service (Bertomeu, Lin, Liu, & Ni, 2023). During the 2017 presidential elections in Russia, the "Alisa" program created by Yandex was recommended by 40,000 Russian citizens for the presidency of the country. His advantage is his ability to work 24/7 and the fact that he is free from any emotion or human factor in making decisions. A similar situation occurred in Japan in 2018. The robot nominee "Mitchihido Matsuda" took 3rd place overall in terms of the number of votes given to the mayor of Tama City, Tokyo (Bistron & Piotrowski, 2021.p.12).

In 1942, American writer Isaac Asimov penned a piece titled "runaround". Three robot laws originated from Asimov's work:

1) Robots cannot harm people or allow others to be harmed by their actions or inaction;

2) Robots must comply with all human commands, with the exception of those that violate the first law; and

3) Robots must defend themselves. The only infractions that are not included are the first and second ones (Haenlein & Kaplan, 2019, p.7).

One of the main problems that have emerged since artificial intelligence was first developed is that it has no bearing on how people integrate into their communities or carry out its intended functions without undermining the liberalism and democratic principles that have been developed over many centuries. What will be the "social situation" and what is the current state of AI, as well as the role that robots will play in society and how they will respond to events if they are able to think because of the simulation of the human mind also begs the question of what action is appropriate. For the first time in human history, the robot "Sofia," created by the Hong Kong company "Hanson Robotics", was given Saudi citizenship in 2017 (Olivia, 2017). This in turn called into question the characteristics of democracy, as there are a number of benefits that are exclusive to citizens. Robots are not able to fully exercise their civil rights; instead, their status is limited to serving human interests and safety. They are not entitled to vote or hold office foreigners and slaves in classical Athens.

Government officials can benefit greatly from the existence of surveillance cameras and facial recognition technology, which can also provide them more authority. This may, in part, discourage common people from protesting against the government because sophisticated surveillance techniques are in place to identify specific individuals. The issue with these surveillance systems is that they have technological issues and have difficulty identifying the faces of black or female people. This may have

detrimental effects on the cohesiveness of society and exacerbate issues with discrimination and gender equality, which could further impede the advancement of society (Schippers, 2020, p.33).

According to Johnson, there are three main categories in which AI-enhanced capabilities may potentially offer security threats: (1) digital security, which includes spear-phishing, speech synthesis, impersonation, automated hacking, and data poisoning; (2) physical security, which includes micro-drones in swarm attacks; and (3) political security, which includes coercion, deception, and surveillance, particularly in authoritarian states (Johnson, 2019, p.5).

Armed forces that employ AI will undoubtedly have a significant advantage over those that rely solely on human judgment in the battlefield (e.g., remote sensing, situational awareness, battlefield maneuverability, and a compressed decision-making loop), even if AI-augmented weapons and systems are not able to make better decisions than humans. This is especially true in operating environments that require endurance and quick decision-making across multiple combat zones (Johnson, 2019, p.5).

The United States Department of Defense launched Project Maven to analyze and interpret vast amounts of visual data that military drones collected by using artificial intelligence and machine learning technologies. Improving the military's ability to locate and monitor items of interest was its main objective. However, there was a lot of criticism against Project Maven and ethical questions raised by the use of AI in military applications. Public outcry and internal discussions about the possible dangers and ramifications of autonomous weapon systems ultimately led to its discontinuation.

As part of a larger plan to improve social control and public security, China has started using AI for mass monitoring. To monitor and follow people in public areas, the Chinese government has deployed a number of artificial intelligence (AI) technologies, including facial recognition software and data analysis algorithms. The declared goals are to protect public safety, stop and look into criminal activity, and boost law enforcement's effectiveness. However, privacy issues, human rights issues, and possible power abuse have been brought up by the widespread usage of AI for monitoring. It is significant to remember that talks on this subject frequently feature a range of viewpoints and opinions.

As a small number of powerful corporations and governments gain wealth and influence at the expense of smaller enterprises that find it difficult to compete, the concentration of AI development and ownership within these groups may worsen inequality. To counteract economic inequality, policies and programs that support economic equity—such as social safety nets, reskilling programs, and inclusive AI development that guarantees a more equitable distribution of opportunities—can be helpful (Marr, 2023).

DISCUSSION

It is evident in the security industry that those that utilize high technology employ more information that has been better processed and validated and have access to a larger range of standard management (Radulov, 2019, p.4).

The scalable application of AI systems to carry out tasks that would typically require human labor, intellect, and expertise could reduce the costs of assaults. Expanding the pool of actors capable of executing specific attacks, their attack velocity, and their pool of possible targets would be a natural consequence.

AI technologies have the potential to allow a small group of people to exert enormous political influence through corporations, governments, or other organizations because they can be implemented at scale without requiring a significant number of humans (Horowitz et al., 2019, p.21).

Regretfully, given the contemporary era's more complex relationship between government and industry and the rapid advancement of technology, artificial intelligence (AI) has the potential to be far more dangerous than these earlier incidents.

REFERENCES

1. Bertomeu, J., Lin, Y., Liu, Y., & Ni, Z. (2023). Capital Market Consequences of Generative AI: Early Evidence from the Ban of ChatGPT in Italy. Available at SSRN.
2. Bistron, M., & Piotrowski, Z. (2021). Artificial intelligence applications in military systems and their influence on sense of security of citizens. Electronics, 10(7), 871.
3. Buranov, S. (2023, May). GLOBAL SECURITY CHALLENGES: INFORMATION SECURITY AND ARTIFICIAL INTELLIGENCE. In International Scientific and Current Research Conferences (pp. 155-159).
4. Comiter, M. (2019). Attacking artificial intelligence. Belfer Center Paper, 8, 2019-08.
5. Haenlein, M., & Kaplan, A. (2019). A brief history of artificial intelligence: On the past, present, and future of artificial intelligence. California management review, 61(4), 5-14.
6. Horowitz, M. C., Allen, G. C., Saravalle, E., Cho, A., Frederick, K., & Scharre, P. (2018). Artificial intelligence and international security. Center for a New American Security.
7. Johnson, J. (2019). Artificial intelligence & future warfare: implications for international security. Defense & Security Analysis, 35(2), 147-169.
8. Marr, B. (2023, June 2). The 15 Biggest Risks Of Artificial Intelligence. Forbes. Retrieved from https://www.forbes.com/sites/bernardmarr/2023/06/02/the-15-biggest-risks-of-artificial-intelligence/?sh=7fac0b1f2706
9. Olivia, C. (2017, October 26). Saudi Arabia becomes first country to grant citizenship to a robot. Arab News. Retrieved from https://www.arabnews.com/node/1183166/saudi-arabia
10. Radulov, N. (2019). Artificial intelligence and security. Security 4.0. Security & Future, 3(1), 3-5.
11. Samijonov, N. Y. (2023, October). AI, ROBOTIZATION, AND DEHUMANIZATION: OPPORTUNITIES AND THREATS TO THE WORKING CLASS. In International Scientific and Current Research Conferences (pp. 184-187).
12. Schippers, B. (2020). Artificial intelligence and democratic politics. Political Insight, 11(1), 32-35.