American Journal Of Applied Science And Technology
(ISSN – 2771-2745)
VOLUME 03 ISSUE 10 Pages: 39-43
SJIF IMPACT FACTOR (2021: 5. 705) (2022: 5. 705) (2023: 7.063)
OCLC – 1121105677
Publisher: Oscar Publishing Services

Journal Website: https://theusajournals.com/index.php/ajast

Research Article

AI FOR INFORMATION SECURITY AND CYBERSPACE

Submission Date: October 20, 2023, Accepted Date: October 25, 2023,
Published Date: October 30, 2023
Crossref doi: https://doi.org/10.37547/ajast/Volume03Issue10-08

Nurmukhammad Y. Samijonov
Independent Researcher, Uzbekistan

ABSTRACT

Taking into account the fact that artificial intelligence can expand the capabilities of humanity, accelerate the speed of data analysis several times, and help people reach correct and accurate conclusions in the decision-making process, it can improve data security or, on the contrary, target propaganda and fake news. Collecting information, taking very little responsibility, and taking into account the fact that social networks can expand the speed and extent of dissemination of information simultaneously in two opposite directions, AI can both strengthen cyber security or create new types of threats to it.

KEYWORDS

"Information technology security", "electronic information security", fake news, bots, target propaganda.

INTRODUCTION

Cyber security is a set of technologies to protect programs, devices and systems from attacks, damages and hacking. Cybercrimes in particular are classified as transboundary crimes because they can target digital computer equipment connected to any international Internet network, i.e., crimes that cross national borders.

In the real world, the overall national security of businesses, governments, organizations, and individual citizens of a country depends on the ability of security controls to detect and prevent cyber attacks in a timely and intelligent manner. Intelligent cybersecurity services and management are critical as large amounts of data on computers and other devices are collected, processed, and stored by government, military, corporate, financial, medical organizations, and more.

METHODS

In this article content, event and comparative analysis were used.

American Journal Of Applied Science And Technology
(ISSN – 2771-2745)
VOLUME 03 ISSUE 10 Pages: 39-43
SJIF IMPACT FACTOR (2021: 5. 705) (2022: 5. 705) (2023: 7.063)
OCLC – 1121105677
Publisher: Oscar Publishing Services

RESULTS

Cybersecurity generally refers to a set of technologies, procedures, and practices designed to protect networks, computers, software, and data from attack, disruption, or unauthorized access. It is also known as "information technology security" or "electronic information security".

In 2016, the AI market in the field of cyber security was equal to 1 billion dollars, and by 2025, these figures are predicted to reach 34.8 billion dollars. Over 3.3 billion cyberattacks were recorded worldwide in just the first half of 2018, which is 70% greater than all cyberattacks in 2017 (2.7 billion). Over 60% of these attacks, based on novel malware, persisted for less than an hour, based on estimates from Google (Taddeo, McCutcheon & Floridi, 2019, p.557). These numbers are rising through the years, and as more lives become dependent on the internet and telematics, the urgency of the issue can easily be felt. Regarding the fact that AI can detect and learn from the data over time, AI is believed to enhance the data and cybersecurity field.

According to the reports of Dmitry Samartsev and William Dixon, experts of the Cyber Security Center of the World Economic Forum, the speed of the Internet through 5G will increase 1000 times, and in turn, the number of cyber threats will increase accordingly. It is also emphasized that it is possible to create a global defense system against cyber threats through AI technologies and that biometric data is used more and more in security today; therefore, cyber security will be the most attacked in the next decade. It is noted that these data are personal biometric data (Samartsev & Dixon, 2019). Dixon claims that because social media and emails are so widely used, it will be simpler to attack people's biometric information and, in many cases, AI will be used to mimic their voice and behavior.

Cyber-attacks include malicious software attacks, ransomware, denial-of-service (DoS), and fraudulent withdrawal of bank customers' information via the Internet. Phishing, hacking through codes (SQL injection), attacks on interactive conversations (Man-in-the-Middle), software crashes (Zero-Day), or insider threats today are the most common.

For example, launching a DoS attack or actively scanning the network. In such situations, a cyber incident response system based on artificial intelligence helps, which allows processing a large number of information security incidents at the same time, automating the routine actions of information security analysts and quickly responding to incidents without human intervention (Sarker, Furhad & Nowrozy, 2021, p.1). Cybercrimes, sometimes known as security events, can have an impact on both individuals and companies, leading to both financial losses and disruptions. For example, according to an IBM report, data breaches cost the United States $8.19 billion, and the annual cost of cybercrime to the global economy is $400 billion (Pomerleau & Lowery, 2020).

AI for Information security.

The use of artificial intelligence in information security is necessary due to two factors: the need for rapid response in the event of a cyber incident and the shortage of skilled cyber defense professionals. In fact, in modern reality, it is very difficult to fill the staff list with qualified information security specialists with the necessary experience, and large-scale incidents threatening information security are developing more and more rapidly. If the company does not have a round-the-clock shift of information security analysts, then it will be difficult to provide high-quality protection outside of working hours without a rapid autonomous response system to cyber incidents. In addition, threat actors can perform diversions before

American Journal Of Applied Science And Technology
(ISSN – 2771-2745)
VOLUME 03 ISSUE 10 Pages: 39-43
SJIF IMPACT FACTOR (2021: 5. 705) (2022: 5. 705) (2023: 7.063)
OCLC – 1121105677
Publisher: Oscar Publishing Services

their attacks, such as launching a DoS attack or actively scanning the network. In such situations, a cyber incident response system based on artificial intelligence helps, which allows processing a large number of information security incidents at the same time, automating the routine actions of information security analysts, and quickly responding to incidents without human intervention.

Artificial intelligence (AI) can be trained to identify terms or subjects linked to dangerous content, thwarting any prospective cyberattack (Radulov, 2019, p.4). It enables you to examine the wording in the messages that are shared using Facebook's DeepText feature. By connecting words, this network attempts to decipher the underlying meaning. Stated differently, this approach enables Facebook to arrange the dispersed data in around 20 different languages using NLP systems of AI (Kalkenings & Mandl, 2022). One of the top providers of cybersecurity, anti-fraud, and data security solutions for businesses worldwide is Trustwave Software. This startup has created an open network called Social Mapper, which verifies account information based on the name and photo of the account holder and compares the information and people that compromise geopolitical security by spreading misinformation (Kamruzzaman, 2022). The Facebook social network's DeepFace feature uses an artificial intelligence neural system to recognize faces with 97% accuracy (Parkhi, Vedaldi & Zisserman, 2015, p.2).

Today, most of the online events and processes on the Internet are carried out by bots. Bots can hack into accounts using stolen codes, create fake accounts, or steal information, raising concerns about information security. A biological human-speed response may not be sufficient against such automated attacks. The ability of artificial intelligence to analyze large volumes of data in a short time and distinguish between useful and rogue bots increases its value in cyber security (Mohammed, 2020, p.3).

Political bots were utilized to disseminate false information and fake news on social media during the 2017 UK general election. Bots are self-governing programs designed to aggressively disseminate biased political messages under the guise of widespread support. Putting emphasis on these points, some experts believe that AI "stifles democracy" (Polonski, 2017).

Large economies are being seriously harmed by the speed at which fake news is spreading and the security of information. On May 22, 2023, an artificial intelligence (AI)-generated fake photo of an explosion close to the Pentagon in Washington, D.C., surfaced on Twitter. The image confused a lot of people even though it was promptly identified as bogus and removed from the network. The stock exchanges lost at least $500 billion following the release of this photograph.

DISCUSSION

The use of artificial intelligence systems in cyber security has the following disadvantages:

2. Autonomous systems alone cannot fully provide cyber security. Despite the great success of AI systems in cyber security in recent years, a fully autonomous security system has not yet been created. Human participation is still required as AI systems are not yet able to perform the human decision-making function.

3. Lack of development of legislation regulating the field. The lack of human control and AI's lack of responsibility for the decisions it makes, as well as its changing nature, reduce trust in AI.

American Journal Of Applied Science And Technology
(ISSN – 2771-2745)
VOLUME 03 ISSUE 10 Pages: 39-43
SJIF IMPACT FACTOR (2021: 5. 705) (2022: 5. 705) (2023: 7.063)
OCLC – 1121105677
Publisher: Oscar Publishing Services

4. Violation of information privacy. Artificial intelligence-based cyber security systems require large amounts of internal data to be submitted to artificial intelligence. For this reason, individuals and organizations who are concerned about their information security will be limited in their ability to fully utilize its capabilities (Wirkuttis & Klein, 2017, p.114).

Governments have already prioritized the usage of AI in cyberspace.. In 2018, the United States announced its national cyber security strategy, and in December 2019, it announced a strategic plan for the development and research of the field. The UK launched its cyber security strategy in 2016 and has since announced that it doubled the sector's budget by 2020. China developed a rapid response plan to cyber attacks in June 2017, and South Korea developed a national cyber security project in September 2019 and designated ministries responsible for the project (Christou & Lee, 2022).

Consequently, no nation can effectively combat this kind of threat on its own, especially considering how widespread this kind of crime is getting. The only options in this kind of circumstance are to increase global collaboration, control the actions of pertinent organizations in the area of coordinated response to cybercrime and its investigation, and create global legal frameworks for reciprocal assistance. As a result, the global issue of cybercrime pushes nations to establish national and international legislative frameworks, protect information security, and take other required steps to combat this kind of crime.

REFERENCES

1. Buranov, S. (2023, May). GLOBAL SECURITY CHALLENGES: INFORMATION SECURITY AND ARTIFICIAL INTELLIGENCE. In International Scientific and Current Research Conferences (pp. 155-159)
2. Christou, G., & Lee, J. S. (2022). EU-South Korea Cooperation on Cybersecurity, Data Protection and Emerging Technologies. Cybersecurity Policy in the EU and South Korea from Consultation to Action: Theoretical and Comparative Perspectives, 41-66.
3. Horowitz, M. C., Kahn, L., & Mahoney, C. (2020). The future of military applications of artificial intelligence: A role for confidence-building measures?. Orbis, 64(4), 528-543.
4. Kalkenings, M., & Mandl, T. (2022, July). University of Hildesheim at SemEval-2022 task 5: combining deep text and image models for multimedia misogyny detection. In Proceedings of the 16th International Workshop on Semantic Evaluation (SemEval-2022) (pp. 718-723).
5. Kamruzzaman, M. M. (2022). Impact of social media on geopolitics and economic growth: Mitigating the risks by developing artificial intelligence and cognitive computing tools. Computational Intelligence and Neuroscience, 2022.
6. Mohammed, I. A. (2020). Artificial intelligence for cybersecurity: A systematic mapping of literature. Artif. Intell, 7(9), 1-5
7. Parkhi, O., Vedaldi, A., & Zisserman, A. (2015). Deep face recognition. In BMVC 2015-Proceedings of the British Machine Vision Conference 2015. British Machine Vision Association.
8. Polonski, V. (2017, August 9). How artificial intelligence silently took over democracy. World Economic Forum. Retrieved from https://www.weforum.org/agenda/2017/08/artificial-intelligence-can-save-democracy-unless-it-destroys-it-first/

American Journal Of Applied Science And Technology
(ISSN – 2771-2745)
VOLUME 03 ISSUE 10 Pages: 39-43
SJIF IMPACT FACTOR (2021: 5. 705) (2022: 5. 705) (2023: 7.063)
OCLC – 1121105677
Crossref doi Google Scholar WorldCat MENDELEY
Publisher: Oscar Publishing Services

9. Pomerleau, P. L., & Lowery, D. L. (2020). Countering Cyber Threats to Financial Institutions. In A Private and Public Partnership Approach to Critical Infrastructure Protection. Springer.
10. Radulov, N. (2019). Artificial intelligence and security. Security 4.0. Security & Future, 3(1), 3-5.
11. Samartsev, D. ,Dikson, V(2019, July 9). 5G, AI and biometrics to define cybersecurity. Technical review Middle East. Retrieved from https://www.technicalreviewmiddleeast.com/it/information-security/5g-ai-and-biometrics-to-define-cybersecurity-strategy
12. 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).
13. Sarker, I. H., Furhad, M. H., & Nowrozy, R. (2021). Ai-driven cybersecurity: an overview, security intelligence modeling and research directions. SN Computer Science, 2, 1-18.
14. Taddeo, M., McCutcheon, T., & Floridi, L. (2019). Trusting artificial intelligence in cybersecurity is a double-edged sword. Nature Machine Intelligence, 1(12), 557-560.
15. Wirkuttis, N., & Klein, H. (2017). Artificial intelligence in cybersecurity. Cyber, Intelligence, and Security, 1(1), 103-119.