

International security in the AI era

Научный руководитель – Добросклонская Татьяна Георгиевна

Голикова Анна Александровна

Студент (бакалавр)

Московский государственный университет имени М.В.Ломоносова, Факультет мировой политики, Кафедра информационного обеспечения внешней политики, Москва, Россия

E-mail: annagolikova2107@gmail.com

Information security is a substantial part of the modern world. Information security began to be discussed at the end of the 20th century with the advent of the Internet and its spread in the 1980s. Currently we are witnessing the digitalization of all processes in the international relations. The dependence of modern societies on information technology makes it necessary to look for methods of countering various cyberthreats and, at the same time, methods of conducting offensive operations against possible adversaries. Now we are talking not only about the possibilities, but about the real facts of the confrontation between states in cyberspace. In fact, for the first time since the appearance of nuclear weapons in the 1940s a fundamentally new sphere of force use in international relations appeared. Provision of cybersecurity, accordingly, is becoming one of the most important problems of modern international security[1]. The AI plays an important role in the cyberthreat landscape and it influences and changes information security.

We increasingly come across the opinion that AI will shape future strategic security. Artificial intelligence, capable of analyzing massive amounts of threat data, is revolutionizing the way cybersecurity is approached, accelerating response times and empowering under-resourced security forces[2]. In its 2013 impact assessment, the European Commission stated that there is an ‘insufficient level of protection’ against network and information security incidents undermining the ‘services that support our society’ (for example, public administrations, finance and banking, energy, transport, health)[3].

The U.S. Department of Defense defines AI as “the ability of machines to perform tasks that normally require human intelligence,” such as “recognizing patterns, learning from experience, drawing conclusions, [and] making predictions.” At the same time, internal problems are becoming the main source of tension in international relations. The threat of terrorism, which emerged in the 19th century, has risen to a global level with the development of science and technology. Technological development opens up new areas of confrontation, including military ones, such as cyberspace.

AI’s use can both exacerbate and mitigate the effects of disinformation within an evolving information ecosystem. Similar to the role of AI in cyberattacks, AI provides mechanisms to narrowly tailor propaganda to a targeted audience, as well as increase its dissemination at scale - heightening its efficacy and reach.

It is important to consider cyber defense (detecting and protecting) and cyber offense (detecting and exploiting). Cyberattacks exploit previous, well-known vulnerabilities that systems designers have simply failed to secure. Artificial intelligence contributes to the complexity of cyberspace defense systems.

The importance of AI is due to the presence of various factors:

- AI automates repetitive learning and discovery through data;
- AI analyzes more and deeper data using neural networks that have many hidden layers;

The Internet of Things (IoT) and sensors have the ability to harness large volumes of data, while artificial intelligence (AI) can learn patterns in the data to automate tasks for a variety of business benefits;

It is a wide-ranging tool that enables people to rethink how we integrate information, analyze data, and use the resulting insights to improve decision-making[4].

It is important to consider that artificial intelligence can influence and aggravate traditional threats as well. All this leads to the fact that AI will affect both the military sphere and the rivalry between countries. In the U.S. Military Academy, the cadets have programmed the tank with an algorithm directing it to use its lance to “kill” the enemy fighters. Governments all around the world support the development of autonomous weaponry. Thus, in December 2020 American Air Force used artificial intelligence on a U-2 spy plane for the first time[5].

In October 2012, Human Rights Watch and several nongovernmental organizations started the Campaign to Stop Killer Robots. In 2013 the U.N. Convention on Certain Conventional Weapons (CCW) raised a question of whether the creation, sale and use of lethal autonomous weapons systems should be banned. In 2020 the Campaign to Stop Killer Robots conducted a research and found the opposition to the development of AI weapons in 26 out of 28 countries, including Russia, China and the U.S.

In order to prevent the spread of the AI threat to security, it is necessary to create a framework for monitoring the development of technologies. This will allow us to take advantage of modern technology. In order to maximize AI benefits, we have to:

- Encourage greater data access for researchers without compromising users’ personal privacy;
- Invest more government funding in unclassified AI research;
- Promote new models of digital education and AI;
- Engage with state and local officials so they enact effective policies;
- Regulate broad AI principles rather than specific algorithms;
- Maintain mechanisms for human oversight and control;
- Penalize malicious AI behavior and promote cybersecurity[6].

[1] Традиционные вызовы и угрозы. // [Электронный ресурс] URL: <https://carnegie.ru/2015/06/08/ru-pub-60343> (дата доступа: 01.03.2021)

[2] Влияние искусственного интеллекта. // [Электронный ресурс] URL: <https://www.osce.org/ru/node/461023> (дата доступа: 01.03.2021)

[3] European Commission 2013, Executive Summary of the Impact Assessment. Accompanying the document Proposal for a Directive of the European Parliament and of the Council Concerning measures to ensure a high level of network and information security across the Union, Strasbourg, July 2013

[4] How artificial intelligence is transforming the world. // [Electronic source] URL: <http://www.brookings.edu/research/how-artificial-intelligence-is-transforming-the-world/> (date of access: 01.03.2021)

[5] The Washington Post Magazine, p. 8-13, February 21, 2021.

[6] How artificial intelligence is transforming the world. // [Electronic source] URL: <http://www.brookings.edu/research/how-artificial-intelligence-is-transforming-the-world/> (date of access: 01.03.2021)