Секция «Коммуникация в современном мире»

Malicious Use of Artificial Intelligence for Terrorist Purposes

Научный руководитель – Пашенцев Евгений Николаевич

Романовский Виталий Анатольевич
Graduate (master)
Дипломатическая академия Министерства иностранных дел Российской Федерации, Москва, Россия
E-mail: vitali.ramanouski@gmail.com

Artificial intelligence (AI) can be a potent tool, enabling significant advances in various fields and being used for malicious purposes when in the wrong hands [1]. Though terrorist organizations may tend towards conventional weapons, terrorism itself is not stagnant. And as soon as AI becomes more widespread, the technical skills and expertise to employ it will be lowered. So the question is 'when' AI will take its place in the terrorist toolbox and what counter-terrorism entities should expect. Terrorists are not bound by the bureaucracy and inertness of the security apparatus. They focus on effectiveness and thus, tactically, are very often one step ahead.

Terrorist groups and individuals can be very energetic and adapt to the changing circumstances very fast [2]. This is especially true concerning internet-based communication tools that have proved extremely valuable for radicalization, inspiring violence, recruiting and arousing fear. Notably, UN GA Res 72/284 (The United Nations Global Counter-Terrorism Strategy Review) of 2018 mentions "increasing use of information and communication technologies, particularly the internet and other media, and using such technologies to commit, incite, recruit for, fund or plan terrorist acts" [3].

Malicious actors can use AI in three security domains - cyber, physical and political [4].

1. In the cyber domain:

- The denial-of-service (DoS) or distributed denial-of-service (DDoS) attacks, when multiple connection requests exhaust a computer memory and make it temporarily impossible to use;
- Malware attacks, when malicious software intrudes into a computer or a computer network and brings it down;
- Ransomware attacks, when malicious software encrypts files and demands a ransom for the decryption;
- CAPTCHA (Completely Automated Public Turing Test to Tell Computers and Humans Apart) and password breaking.

2. In the physical domain:

- Data poisoning, when malicious actors modify the data sets or interfere in an AI employing system. That can be especially dangerous when malicious actors break into strategic systems, e.g. public transport, power stations, sewage systems, public healthcare infrastructure, military objects.
- Drones with facial recognition increase chances for the successful assassination of a public figure.

- Bioterrorism, when malicious actors attempt to create deadly strains of pathogens using the genetic data accumulated and processed with AI.

3. In the political domain:

- Agenda-setting. Terrorism as a socio-political phenomenon is about creating a context for socio-political transformations and decisions beneficial for the perpetrators of a terrorist act. With AI-driven technologies, terrorist groups can formulate political agendas in a single state or entire region.
- Propaganda and disinformation. Terrorism is always about political communication. To attain a political goal, malicious actors utilize fear and intimidation to create a context for a specific political decision. AI-related technologies will likely be used by terrorist for precisely this purpose - to worsen public distrust for state authorities. In contemporary military-political discourse, this is usually attributed as a cognitive operation. Among such technologies are deep fakes - a type of fake audio-visual content created with the Generative Adversarial Network (GAN) machine learning technique.

In the age of "post-truth" and complex social transitions, the cognitive sphere competition is an integral part of the competition in political, security, and economic spheres. Data and trust have become critical assets for today's leaders. Likewise, they are becoming targets for malicious actors, including adversary states and terrorist groups. Political stability in a single country is becoming linked with the population's psychological security [5].

The strategic and sensitive nature of the issue of AI use by terrorists presumes the national government's active role in developing policies to defend the population's psychological security and enhance the counter-terrorism and intelligence agencies' efforts. However, there are many challenges that the national security establishment have to overcome to develop respective policies and operational practices.

1) In the technical domain:

- Difficulties in adapting civilian technologies for security purposes;
- Lack of data or software to process available data;
- Lack of predictability of AI applications outputs;
- Lack of corresponding security firewalls to protect AI applications from breaches.

2) In the organization domain:

- Lack of R&D, designated budgets and human resources;
- Legal issues related to data privacy;
- Lack of effective operational practices;
- Lack of understanding of the roles and responsibilities in the human-machine squad.

Counter-terrorism entities might wish to pay attention to the following recommendations to increase the effectiveness of their work in countering terrorists that use AI for malicious purposes:

- Creation of interdisciplinary expert panels to assess the risks and provide recommendations for policymakers;
- Support of targeted R&D activities of the academic and practitioner's community;
- Creation of knowledge-sharing platform between entities working in the counter-terrorism field;

- Development of AI applications that can learn on the available counter-terrorism related data;
- Incorporation of AI-based analytical tools in routine analytical, planning and support activities;
- Coherent and focused monitoring of the cyber and AI capacities of the terrorist entities [6].

References

1) Ciancaglini, V. et al. Malicious Uses and Abuses of Artificial Intelligence. Trend Micro, EUROPOL and UNICRI. 2019. Accessible at http://unicri.it/sites/default/files/2020-11/AI%20MLC.pdf
2) Hoffman, B. Inside Terrorism, Third Edition. Columbia University Press. 2017.
3) The United Nations Global Counter-Terrorism Strategy Review. A/Res/72/284. Accessible at https://undocs.org/en/A/RES/72/284
4) Brundage, M. et al. The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation. 2018. Accessible at https://maliciousaireport.com/
5) nternational Psychological Security. 2020. Accessible at https://www.academia.edu/43406469/Experts_on_the_Malicious_Use_of_Artificial_Intelligence_Challenges_for_Political_Stability_and_International_Psychological_Security_Report_by_the_International_Center_for_Social_and_Political_Studies_and_Consulting_June_2020_
6) Antebi, L. Artificial Intelligence and National Security in Israel. The Institute for National Security Studies. Tel Aviv University Press. 2021.