International Journal of Multicultural and Multireligious Understanding

http://ijmmu.com
editor@ijmmu.com
ISSN 2364-5369
Volume 10, Issue 4
April, 2023
Pages: 535-543

Potential Risks of ChatGPT: Implications for Counterterrorism and International Security

Yaser Esmailzadeh

Postdoctoral Researcher, Department of Regional Studies, Faculty of Law & Political Science, University of Tehran, Iran

E-mail: esmailzadeh.yaser@ut.ac.ir

http://dx.doi.org/10.18415/ijmmu.v10i4.4590

Abstract

This article explores the potential risks of chatGPT, a language generation model developed by OpenAI, for counterterrorism and international security. With its ability to generate human-like text, chatGPT has rapidly gained popularity and become one of the fastest-growing consumer applications in history, with over 100 million active users. However, practical and ethical concerns regarding its strengths and weaknesses remain under debate. Terrorists' increasing use of modern communication technologies has made the intelligence problem more complex, as access to critical data becomes increasingly challenging for intelligence agencies. Terrorists have also adopted new technologies and implemented operational security measures to evade sophisticated intelligence collection operations. Furthermore, artificial intelligence has enabled individuals and groups to exploit newer technologies, heightening the threat of cyberattacks and espionage. This article analyzes the potential risks of chatGPT in four key areas: the implications of artificial intelligence for future threats and international security, the impact of chatGPT on cyberterrorism and artificial intelligence, the dangers of fragmented and secondary information for violence and sabotage operations, and conducting psychological warfare against targets. By providing insights and recommendations, this study can assist policymakers and researchers in utilizing artificial intelligence technology effectively while mitigating potential risks.

Keywords: *Terrorism; Counterterrorism; Cyberterrorism; ChatGPT; Artificial Intelligence; International Security*

Introduction

The field of artificial intelligence (AI) aims at the automation of a broad range of tasks. Typical tasks studied by AI researchers include playing games, guiding vehicles, and classifying images. In principle, though, the set of tasks that could be transformed by AI is vast. At minimum, any task that humans or non-human animals use their intelligence to perform could be a target for innovation. ChatGPT, developed by OpenAI, is a language generation model with the ability to generate human-like text. It had a significant impact on various industries, including media and science. Its strengths and weakness are subject to an important debate including practical and ethical concerns (Rudolph et al.

2023). ChatGPT, a new-generation chatbot released by OpenAI in November 2022, has become so sensational that we information professionals probably cannot afford to be bystanders. In early 2023, it reached 100 million active users two months after its launch and became the fastest-growing consumer application in history (Hu, 2023).

New technologies and resources available to terrorists have clearly made the intelligence problem much more difficult. Modern communications technologies, such as cell telephones and the Internet, in particular, have enabled terrorist operations on a new scale. Increasing use of such technologies by terrorists, with corresponding improvements in operational security, have made timely and accurate access to critical data by intelligence agencies more difficult. For their part, many terrorists have changed their mode of operations, adopting these new technologies and implementing various operational security measures designed to avoid or defeat sophisticated intelligence collection operations (Wagner, 2007: 49-50).

In recent decades, communications intercept has become a crucial intelligence capability, and for good reason. The evolution of communication technologies has been exponential, and the costs associated with them have decreased dramatically. As a result, these technologies have become widely available in virtually every nation, utilized by business people, school children, terrorists, and others alike. Modern communication systems such as cellular telephones, the Internet, and other digital platforms have proliferated globally at rates that were unimaginable just a few years ago (Wagner, 2007a). For terrorists, these technologies offer the ability to communicate and coordinate worldwide operations with reasonable expectations of privacy and security. Meanwhile, artificial intelligence has been able to exploit newer technologies for individuals and groups, making the threat of cyberattacks and espionage more pervasive than ever before.

As a cornerstone intelligence capability, communications intercept is critical for detecting and preventing threats to international security. The development of advanced signal processing algorithms and machine learning techniques has enabled analysts to quickly and accurately process large volumes of intercepted data, identifying and analyzing patterns of interest in near-real time.

However, the proliferation of modern communication technologies has also created new challenges for states, including the need to keep pace with rapidly evolving technologies, deal with the increasing volume of intercepted data, and address privacy concerns. Despite these challenges, the continued evolution of communication technologies and the growing sophistication of artificial intelligence will undoubtedly continue to shape the landscape of modern intelligence collection and analysis.

The following article aims to answer the question: "What are the implications of chatGPT artificial intelligence technology for the fields of counterterrorism and international security?" To achieve this goal, the study will confirm the practical and useful aspects of artificial intelligence and specifically chatGPT technology for communities and groups. Additionally, the research will investigate the risk potential of this technology in line with the misuse of terrorism to carry out destructive operations and nefarious purposes. The study will analyze four key areas: section 1 examines the implications of artificial intelligence for future threats and international security; section 2 evaluates the impact of chatGPT on cyberterrorism and artificial intelligence; section 3 highlights the dangers of fragmented and secondary information for violence and sabotage operations; and section 4 explores the use of psychological warfare against targets.

As artificial intelligence, particularly chatGPT technology, becomes increasingly prevalent in various fields, including security and counterterrorism, it is essential to examine the potential risks associated with this technology. The insights and recommendations provided by this study can assist security agencies in effectively utilizing artificial intelligence technology while mitigating any associated risks.

Literature Review

Research on the use of new technologies and digital tools by terrorism and terrorist groups has become increasingly important in recent years. With the rise of the internet and social media, terrorist organizations have been able to exploit these platforms to recruit, fundraise, and plan attacks. Many studies have looked at how terrorist groups like ISIS use social media to disseminate propaganda and radicalize individuals. For example, Berger and Morgan (2015) analyzed ISIS's use of Twitter and found that the group was able to create a large and engaged online following.

Some terrorist groups have also attempted to use cyberattacks to disrupt critical infrastructure or steal sensitive information. For instance, Lazarus Group, believed to be linked to North Korea, has been responsible for several high-profile cyberattacks on banks and cryptocurrency exchanges (Nakashima, 2021).

Cryptocurrencies have become a popular way for terrorist groups to fundraise, as they provide a way to transfer funds anonymously. A study by Kshetri (2018) found that ISIS and other groups have used Bitcoin and other cryptocurrencies for fundraising purposes.

Terrorist groups have also used encrypted messaging apps like Telegram and WhatsApp to communicate securely. A study by Ali and Shukla (2021) examined the use of these apps by terrorist groups and the challenges they pose for law enforcement.

Hans-Jakob Schindler's article (2021) highlights two significant challenges for combating the financing of terrorism (CFT) in the EU. Firstly, there is a need to address the financing of violent right-wing extremism/terrorism, which is currently on the rise. Secondly, the increasing misuse of new technologies such as internet tools and cryptocurrencies for terrorism financing presents a significant challenge. The article points out that there is a lack of common understanding of the threat landscape, and existing EU CFT instruments have not been adequately adjusted to address these emerging challenges. However, the author suggests that multilateral discussions concerning the threat posed by right-wing extremism/terrorism, and the planned regulations of the cryptocurrency sector in the EU, offer new opportunities for progress in the fight against terrorism financing.

Abraham Wagner's (2007) article provides a critical overview of the challenges that modern terrorist operations pose for law enforcement and security services. The author emphasizes that the use of new technologies by terrorist organizations has enabled them to carry out operations on an unprecedented scale, and that the technologies available for their use have evolved more rapidly than those needed to counter them. Wagner highlights the need for timely access to terrorist communications and the ability to interdict weapons shipments and logistics as crucial aspects of effective counter-terrorism measures. The article also suggests that new laws and technologies may be required to address these challenges, and provides insights into the current technology base used by terrorists and potential areas for future technological development.

According to James Johnson (2019), recent advancements in artificial intelligence (AI) have the potential to significantly impact military power, strategic competition, and global politics. While the initial literature on AI was characterized by broad speculation, Johnson's article seeks to provide much-needed specificity to the ongoing debate. Johnson argues that if left unaddressed, the uncertainties and vulnerabilities that arise from the rapid proliferation and diffusion of AI could become a major source of instability and great power rivalry. The article identifies several AI-related innovations and technological developments that are likely to have significant implications for military applications, from tactical battlefield scenarios to strategic-level decision-making.

Weimann (2015) examines the challenges posed by the internet to counterterrorism efforts, including the use of the internet by terrorist organizations for recruitment, propaganda, and communication. The author evaluates the effectiveness of responses by governments and other actors and provides recommendations for policymakers and counterterrorism practitioners to address these challenges.

After reviewing the research background, it is evident that no specific scientific investigation has been conducted on the topic of the ramifications of artificial intelligence and its related technologies on the anti-security operations of terrorist organizations. Additionally, no studies have been identified regarding the impact of ChatGPT on international security and counter-terrorism domains.

Cyberterrorism and Artificial Intelligence: The Impact of ChatGPT

There is no consensus on a legal or academic definition of the derivative term “cyberterrorism,” which was introduced by Barry Collin in 1997 (Collin, 1997). As for terrorism, there is debate over the basic definition of the scope of cyberterrorism, depending on motivation, targets, methods, and centrality of computer use in the act. Cyberspace involves both military and civilian security, as governments rely on the Internet and telecommunication systems for a wide range of critical services (US Department of Defense, 2015).

Artificial intelligence and the capabilities of ChatGPT can create new opportunities for cyberterrorism and its tactics. Terrorists can leverage these technologies to launch attacks that disrupt computer networks and cause widespread consequences, especially on personal computers connected to the internet. Some possible tactics include using computer viruses, worms, phishing scams, and hacking into computer systems. As AI technology advances, it is important for security experts to stay vigilant and be prepared for new threats that may emerge.

It is also crucial to note that ChatGPT can inadvertently assist individuals who seek to disrupt computer systems for political or malicious purposes by providing them with training and answers to their questions. This technology may be particularly helpful for amateur hackers who lack the necessary skills and knowledge to carry out cyberterrorism tactics effectively. Therefore, it is necessary to monitor the use of ChatGPT and other AI tools to prevent them from being misused for harmful purposes. Security experts should remain aware of the potential for AI to be used in cyberterrorism and take proactive measures to prevent such misuse.

In addition to traditional cyberattack methods, victims' online information can be used to automatically generate custom malicious websites, emails, or links that they would be likely to click on. These attacks can be sent from addresses that impersonate their real contacts and use writing styles that mimic those contacts. As AI continues to develop, convincing chatbots may be able to elicit human trust by engaging people in longer dialogues and potentially masquerade visually as another person in a video chat. Therefore, it is necessary for security experts to anticipate and develop strategies to counter such threats (Brundage et al., 2018).

The Dangers of Fragmented and Secondary Information for Violence and Sabotage Operations

Political violence is considered as the root cause of issues such as terrorism and violent conflicts in the world (esmailzadeh, 2020: 347).When considering terrorism, the Internet, and their combined effect, one thing becomes clear: both have catastrophic consequences from the local to the international and global levels (LaFree, 2017). Following the rise of ISIS and their activities in recent years, online training has become increasingly popular for individuals seeking to learn how to create explosives, use explosive precursors, and conduct lone wolf operations. However, the use of new technologies such as Chat GPT has created limitations on the dissemination of information that can facilitate violent and sabotage operations. While these technologies may restrict access to certain parts of these trainings and their associated steps, they may still provide valuable information to researchers and other interested parties.

The Internet could be useful to the would-be terrorists in their plotting, in particular for obtaining information about potential targets (Mueller and Stewart, 2015: 179). Online terrorist training programs have become a serious concern for law enforcement and counterterrorism experts due to the ease with which individuals can access information on how to conduct violent and sabotage operations. However, the quality and accuracy of the information disseminated in these programs is often questionable, with much of it consisting of fragmented or secondary information that may be incomplete or misleading. This is particularly true for lone wolf operations, which are often planned and executed by individuals who lack the training and resources of more organized groups.

One major challenge in addressing the dangers of fragmented and secondary information in online terrorist training is the rapid pace at which new technologies are emerging, making it difficult for law enforcement to keep up with the latest threats. As mentioned in the previous paragraph, technologies such as ChatGPT have created new limitations on the dissemination of information, but they have also opened up new avenues for individuals to access training materials and connect with other like-minded individuals. To address these challenges, law enforcement agencies must work to stay ahead of the curve by leveraging the latest tools and technologies to monitor and disrupt online terrorist activity, while also promoting public awareness of the risks associated with online training programs. By doing so, they can help to mitigate the dangers of fragmented and secondary information, and keep our communities safe from the threat of terrorism.

Terrorist organizations and Lone wolf terrorists can use the scattered information available on the internet, particularly through the use of technologies such as ChatGPT, to conduct violent operations and create explosive devices. By piecing together bits of information from various sources, they can learn how to make bombs, obtain explosive precursors, and plan tactics for lone wolf operations. This makes it challenging for law enforcement agencies to track and disrupt online terrorist activity, as much of the information exchanged in these forums may be encrypted or otherwise difficult to intercept.

To counter the use of scattered information in online terrorist activity, it is critical for law enforcement agencies to focus on the supply chain of information, including identifying the sources of information and working to shut them down. This can include monitoring online chat rooms and forums to identify and disrupt networks of individuals who are sharing information related to violent operations, as well as working with internet service providers to remove content that promotes terrorism and violent extremism. Additionally, public awareness campaigns can help to educate individuals about the risks associated with online terrorist training, including the potential for fragmented and secondary information to lead to violent and destructive outcomes. By taking a multi-pronged approach to countering the use of scattered information in online terrorist activity, law enforcement agencies can help to prevent attacks and keep our communities safe.

Technologies such as ChatGPT may provide valuable information to terrorists and lone wolves seeking to make explosive devices or other weapons of terror. For example, ChatGPT could be used to obtain information on the different stages of making explosive materials, including how to source the necessary precursors, how to mix and handle the materials safely, and how to assemble the device. Such information could be pieced together from different sources, including online forums and training materials, and could be used to create a functional explosive device.

In addition to information on making explosives, technologies such as ChatGPT could also be used to obtain information on the construction and use of other weapons of terror, such as firearms and improvised weapons. For example, ChatGPT could be used to obtain information on the different types of firearms and their components, as well as how to modify or manufacture these components to make them more lethal. Similarly, ChatGPT could be used to obtain information on the construction and use of improvised weapons, such as pipe bombs or car bombs, which could be used in terrorist attacks. It is worth noting that accessing and piecing together this information is not necessarily easy, as it requires a certain level of technical expertise and specialized knowledge. However, with the help of technologies such as ChatGPT, terrorists and lone wolves may be able to overcome some of these barriers and access the information they need to carry out attacks. While technologies such as ChatGPT have the potential to provide valuable insights and support research efforts, it is also important to consider the risks associated with the use of these technologies for nefarious purposes.

Overall, the availability of information on the internet, including through technologies such as ChatGPT, poses a serious threat to public safety and national security. Law enforcement agencies must remain vigilant in monitoring and disrupting online terrorist activity, while also promoting public awareness of the risks associated with online training programs and the use of scattered information in terrorist activity. By doing so, they can help to prevent attacks and keep our communities safe from the threat of terrorism.

Artificial Intelligence & Future Threats: Implications for International Security

Although most of the contemporary debate on AI is related to regulation, innovation and the digital market, the development of AI is tied to the history of warfare and security. The concept of AI builds on Turing's pioneering work "Can Machines Think?" (Turing 1950). Since Turing's work on AI, the latest advancement in the field reflects the recently acquired access to "big data", developments in machine learning approaches, and increased computer processing power. Today, AI consists of a set of elements including data, sensors, algorithms, actuators, and machine learning, that can emulate human cognition in reasoning, learning and autonomously taking actions as a response (Calderaro & Blumfelde, 2022: 421). These latest progresses in AI have and will continue to have enormous impact on international security. Therefore, due to the digital, physical and political security threats arising from the competition between AI in military applications, private digital innovations and scientific development (Johnson, 2019), normative and legal frameworks are seen as crucial to sustain international stability (UNIDIR, 2019).

Undoubtedly, terrorism is an important player in the international arena today today (Esmailzadeh, 2023: 55). In the past decade, researchers have achieved major milestones in the development of artificial intelligence (AI) and related technologies, and world leaders have been quick to recognise the transformative potential of AI as a critical component of national security. The uncertainties and risks surrounding the proliferation and diffusion of dual-use AI technology could worsen international security in several ways: exacerbate existing threats, transform the nature and characteristics of these threats, and introduce new (and potentially accidental prone and unsafe) threats to the security landscape (Johnson, 2019: 148-149).

As terrorism has emerged as a significant actor in the international arena, it is imperative for other actors, such as governments and international organizations, to play their role in countering security threats. Security actors are committed to considering the global impact of their choices (esmaizladeh emamqoli & tajari, 2017: 1).The latent hazards of AI-augmented capabilities can be classified into three overarching domains: (1) cyber security (2) physical security; and (3) political security. Understanding and addressing these security concerns is crucial for the safe and responsible development and deployment of AI systems in various domains, from healthcare to defense.

Conducting Psychological War against Targets

Psychological warfare (PSYWAR) is the mix of psychological operations (PSYOP) with the achievement of political objectives, using unorthodox measures (this term coined by the British in World War II): "What we are talking about, then, when we speak of 'psychological warfare' is the use of symbols to promote policies—i.e., politics. Propaganda is politics conducted by the symbolization of events." (Celeski, 2019: 351). As a crude explanation, efforts to influence opinion and, by extension, impact decision making is the aim of psychological warfare (Dheeraj, 2020: 558). Terrorism is widely acknowledged as propaganda by deed. Terror and violence are tactics adopted by terrorist groups to achieve their strategic goals. Hence, an act of terror has a psychological objective directed at a set audience. The target audience in psychological operations can be divided into three groups: domestic audience, adversarial audience and international audience; each with distinct roles. Domestic audience, the section of population over whom the terrorist group assumes representation, is the primary target audience. In success, the terrorist groups instil a sense of confidence among the supporters, which is critical in sustaining a steady recruitment pool and raising the morale of the community. The adversarial or enemy audience are the main targets of terror groups. A successful terrorist attack makes the victim population insecure, threatened; lose faith in political and security establishment and transform public opinion against the respective government. In some cases, terrorist groups also seek to subvert public opinion and develop sympathisers for the terrorist's cause. The third audience is international public opinion. The aim of targeting the international community is to convey a sense of determination of the terrorist group's cause and thereby, seek interference through application of pressure on the enemy to accommodate the demands of the terrorists (Ganor, 2017). Notwithstanding the acts of terror as propaganda, terrorists use other platforms to communicate with their target audience. In the case of domestic audience, where recruitment and support is sought, public execution of informers and dissenters is accompanied by dissemination of literary material both in print as well as online platforms. Osama Bin Laden's call for jihad against Americans, Westerners, Jews and Non-Believers through release of fatwas is a case in point.Footnote5 Internet and mass media are effective platforms for terrorist propaganda. Besides spreading fear and intimidation, mass media and internet serves as a medium for Islamic terrorist groups to battle for 'hearts and minds' using victimisation narratives (Bilgen, 2012). The proliferation of the internet has facilitated terrorist groups in legitimizing their actions, promoting their leaders as heroic figures, and disseminating fabricated narratives and misinformation to expand their sphere of influence.

ChatGPT has access to numerous and diverse datasets on various topics worldwide and possesses knowledge of public opinion and different societal strata and groups. As a result, it can provide fundamental data and essential strategic information to terrorists and masterminds, which poses a significant threat to national security.

One of the ways terrorists can abuse ChatGPT is by preparing fake news and creating rumors with the aim of creating social, cultural, political, and economic divisions in public opinion. By manipulating public opinion, they can create chaos and instability, making a country appear weak to its own people and other nations. In today's world, terrorism is led by designers and creative minds who strive to create significant challenges for countries, their national security, and their objectives, particularly in the area of psychological operations. Given the significant role that technology and artificial intelligence play in modern-day terrorism, it is imperative to consider the potential risks and dangers associated with AI models like ChatGPT. The use of AI models for malicious purposes can cause significant harm, and it is crucial to implement measures to prevent its abuse. Therefore, it is essential to establish proper safeguards and regulations to ensure that AI models like ChatGPT are not used to facilitate terrorist activities.

Conclusion

After ChatGPT's introduction, it seems to exhibit substantially more capability and expertise compared to the chatbots that people used before. The development of artificial intelligence (AI) and related technologies has a significant impact on international security. The use of AI in military applications, private digital innovations and scientific development can potentially exacerbate existing threats, transform the nature of these threats, and introduce new threats to the security landscape. AI-augmented capabilities can lead to cyber security, physical security, and political security threats. In particular, the use of ChatGPT technology can create new opportunities for cyberterrorism and its tactics, which can potentially be used to disrupt computer networks and cause widespread consequences. Additionally, fragmented and secondary information in online terrorist training programs can provide valuable information to researchers and interested parties, which can be used to facilitate violent and sabotage operations.

To address these risks, it is crucial to develop legal and normative frameworks for the safe and responsible development and deployment of AI systems. Security experts should stay vigilant and take proactive measures to prevent the misuse of AI and ChatGPT technology for harmful purposes, and anticipate and develop strategies to counter potential threats. Furthermore, it is necessary to monitor the use of ChatGPT and other AI tools to prevent them from being misused for political or malicious purposes. In summary, the potential risks of ChatGPT technology and AI in general should be taken seriously by policymakers, security experts, and the public. While AI has enormous potential for innovation and growth, it is essential to address the security concerns that arise from its development and deployment to ensure international stability and security.

References

Ali, S. S. & Shukla, S. (2021). Terrorism and encrypted communication: Issues and challenges for law enforcement. *International Journal of Cyber Warfare and Terrorism*, 11(1), 45-57.

Berger, J. M. & Morgan, J. (2015). *The ISIS Twitter census: Defining and describing the population of ISIS supporters on Twitter*. The Brookings Institution.

Bilgen, A. (2012). *Terrorism and Media: A Dangerous Symbiosis*, E-IR (22 July 2012)http://www.e-ir.info/2012/07/22/terrorism-and-the-media-a-dangerous-symbiosis/.

Brundage, M. et al. (2018). *The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation*. Oxford: Oxford University.

Calderaro, A. & Blumfelde, S. (2022). Artificial intelligence and EU security: the false promise of digital sovereignty, *European Security*. 31(3), 415-434, DOI: 10.1080/09662839.2022.2101885.

Celeski, J. D. (2019). *Psychological Operations—A Force Multiplier, Alabama: Air University Press*. https://www.jstor.org/stable/resrep19555.19.

Collin, B,. (1997). The Future of Cyberterrorism. *Crime & Justice International Journal*, 13(2), 15-27.

Dheeraj P. C. (2020). India's PSYWAR Against Islamic Terrorism: A Trident Strategy, *Terrorism and Political Violence*, 32(3), 558-581.

Esmailzadeh, Y. (2020). Organizing the concept of legitimacy-based political violence by focusing on the views of Habermas and Weber 1. *Political Sociology of Iran*, 3(1), 347-362. doi: 10.30510/psi.2021.307008.2379.

Esmailzadeh, Y. (2023), Towards the emergence of the fifth wave of terrorism in the world. *The Iranian Research letter of International Politics* 11(2). doi: 10.22067/irlip.2022.71990.1138.

Esmaizladeh E.Y., and Tajari, S. (2017). Ethical and Ontological Frameworks in Security Cosmopolitanism. *Iranian Research letter of International Politics* 5(2), 1-19. doi: 10.22067/jipr.v5i2.52952.

Ganor, B. (2017). *Terror as a Strategy of PSYWAR*, International Institute for Counter-Terrorismhttps://www.ict.org.il/Article/827/Terror%20as%20a%20Strategy%20of%20Psychological%20Warfare

Hu, K. (2023). *ChatGPT sets record for fastest-growing user base - analyst note*. Reuters. https://www.reuters.com/technology/chatgpt-sets-record-fastest-growinguser-base-analyst-note-2023-02-01/.

Johnson, J. (2019). Artificial intelligence & future warfare: implications for international security. *Defense & Security Analysis*, 35(2), 147-169, DOI: 10.1080/14751798.2019.1600800.

Kshetri, N. (2018). Can blockchain strengthen the internet of things?. *IT Professional*, 20(4), 68-72.

LaFree G. (2017). Terrorism and the Internet. *Criminol Public Policy*, 16(1):93–98.

Mueller, J. & Stewart, M. G. (2015). Terrorism, counterterrorism, and the Internet: The American cases. *Dynamics of Asymmetric Conflict*, 8(2), 176-190. http://dx.doi.org/10.1080/17467586.2015.1065077.

Nakashima, E. (2021). *U.S. indicts North Koreans, accuses them of stealing millions in cryptocurrency*. The Washington Post.

Rudolph J, Tan S, Tan S. (2023). ChatGPT: bullshit spewer or the end of traditional assessments in higher education? *J Appl Learn Teach*. 6(1): 1–22.

Schindler, H.-J. (2021). Emerging challenges for combating the financing of terrorism in the European Union: financing of violent right-wing extremism and misuse of new technologies. *Global Affairs*, 7(5), 795-812. doi: 10.1108/JMLC-06-2020-0063.

Turing, A.M., (1950). Computing machinery and intelligence. *Mind*, *LIX* (236), 433–460.

US Department of Defense. (2015). *The Department of Defense Cyberstrategy*, https://www.defense.gov/Portals/1/features/2015/0415_cyberstrategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.

Wagner, A R. (2007a). *Meeting the terrorist challenge: Coping with failures of leadership and intelligence*. New York, NY: Harper-Collins.

Wagner, A. (2007). Intelligence for Counter-Terrorism: Technology and Methods. *Journal of International Affairs*, 2(2), 48-61.

Weimann, G. (2010). *Terror on the Internet, he New Arena, the New Challenges*. United States, United States Institute of Peace Press.

Copyrights