ARTIFICIAL INTELLIGENCE AND (COUNTER)TERRORISM

Opinion Paper

Luka Lesko, University of Applied Sciences in Security and Safety, Zagreb, Croatia, Swiss School of Business and Management Geneva, Switzerland, luka@ssbm.ch

Mario Silic, Swiss School of Business and Management Geneva, Switzerland, mario@ssbm.ch

Abstract

Security is one of the basic human needs so it is therefore important to study phenomena like terrorism, that significantly threaten security. Artificial intelligence as the simulation of human intelligence processes by machines, especially computer systems, can be a useful tool in the malicious activities of terrorists, and on the other hand, it enables new solutions in the fight against terrorism. The opinion paper summarizes the usefulness of artificial intelligence in both mentioned domains. Further research should focus on technological development of using AI for counter-terrorism purposes, on AI knowledge among national security organizations and continuous improvement of AI related policies among alliances and individual countries.

Keywords: Security, Cyberterrorism, Intelligence, Attack.

1 Introduction

According to Maslow’s hierarchy of needs (Maslow, 1954), security is one of the basic human needs in which various phenomena like terrorism play a significant role and consequently, may have an important effect on security and a feeling of security. Terrorism is a consequence of a multifaceted combination of historical, political, social, cultural, ideological, religious, economic and psychological factors (Friedman, 2003). In a broader sense, it implies the use of violence to achieve political goals. During counter-terrorism activities, countries use a variety of instruments: police, criminal law, military, intelligence, political, civil, sometimes even amnesties to suppress terrorist activity (Jones and Libicki, 2008), while the fight against terrorism often requires international cooperation. The rapid growth of cyberspace as well as the artificial intelligence (AI) solutions in the modern era have deepened potential threats. Nowadays, terrorism has become highly digital with the rise of threats such as cyber-crime networks.

Terrorist organizations are well-organized while their managerial members are often highly educated, which makes the prevention more complex. They have a defined structure and decision-making processes, recognized leaders in positions of formal authority, develop functionally differentiated roles and collective goals that they achieve as a unity with collective responsibility (Gunaratna and Oreg, 2010). They have units for political or military issues, information, planning and preparation of operations, intelligence, counter-intelligence, logistics, training, financing, technology, etc. Every terrorist organization has its own value structure and specific modus operandi. Thus, their motivation becomes rational and can be observed within the concept of axiological rationality (Tosini, 2007). Counter-terrorism, as a rule, is significantly more expensive than terrorism. For example, the total cost of Al-Qaeda’s operation on 9/11/2001 was between 300.000 and 500.000$ (Bilandžić, 2019). An important policy implication of historical and sociological research concerns what Chaliand and Blin (2007) describe as the need to avoid terrorism while claiming to fight it. In the fight against terrorism both physical and online, the importance of building instruments to prevent radicalization and effective international cooperation are emphasized.

Artificial intelligence as the simulation of human intelligence processes by machines, especially computer systems, can be a useful tool in the malicious activities of terrorists, and on the other hand, it enables new solutions in the fight against terrorism.

2 The use of artificial intelligence for terrorist purposes

Terrorist organizations have opportunities for faster mobility of people, funds and weapons than national organizations bound by international regulations (Shiraz and Aldrich, 2013), with soft targets being an increasingly common choice of security threats compared to hard-defended targets such as military facilities, embassies, etc. One of the most demanding challenges of counter-terrorism is in detecting lone-wolves attacks, who may or may not be members of a terrorist organization, and who generally do not leave a trace of communication during the preparation of the attack (Bilandžić and Leško, 2019). They can independently carry out a terrorist act, inciting publicly announced calls by terrorist groups to commit an attack. The nature of terrorist attacks has changed significantly over time in connection with technological developments (Herbert, 2002). Such threats are further complicated by the emergence of artificial intelligence. In that term, the United Nations Office of Counter-Terrorism (2021b) specifically points to the following AI-driven threats: autonomous vehicles, drones with facial recognition, genetically targeted bio-weapons. Also, other numerous threats to information security in the cyberspace as human error or failure, information extortion, theft, espionage, software attacks, etc., may provide space for malicious activities of terrorists. Additionally, different cyber security laws among countries make the fight against terrorism in the cyber sphere more difficult.

SARS-CoV-2, which has boosted online activities in terms of digital transactions, has additionally deepened the potential for terrorist activities. During the COVID-19 pandemic, for instance, such terrorists or violent extremists created and amplified misleading content on a largescale, by taking advantage of vulnerabilities in the social media ecosystem and by manipulating people through conspiracy narratives and fake news to inter alia undermine trust in the government and, at the same time, reinforce non-state actors' extremist narratives and recruitment strategies (UNICRI, 2020).

Summarized, the cyber activities driven by artificial intelligence, including the online gaming platform, have become a useful tool for terrorist organizations to:

- create cover identities;
- research for decision-making purposes in the context of terrorism;
- surveillance;
- (encrypted) communication;
- spread propaganda (ISIL have been using bots on social media to automate the dissemination of propaganda);
- inspire like-minded people;
- recruit new members;
- spread disinformation and deception;
- acquiring funds;
- money transactions between terrorist branches, cells, etc.
- buy weapons and other logistics supplies;
- manage and perform the attacks (physical);
- manage and perform the attacks (online - DDoS, Malware, Ransomware, password cracking, encryption/decryption);
- live stream of the attack for the purpose of virally spreading terror and a general feeling of insecurity;
- claim responsibility for conducting attacks;
- easier dissemination of information about the demands of a terrorist organization.

In terms of preserving security, both small and large governmental and non-governmental organizations should pay attention to strategic planning for security, including contingency planning. According to Whitman and Mattord (2018) contingency planning implies the actions taken by senior management to specify the organization's efforts and actions if an adverse event becomes an incident or disaster, which includes business impact analysis, incident response plan, disaster recovery plan and business continuity plan. In the context of cyber terrorism penetration into organizations of different types, it is important to train employees in adequate reactions. More applicable for that purpose, Silic and Lowry (2020) proposed a recontextualized kernel theory from the hedonic-motivation system adoption model that can be used to assess employee security constructs along with their intrinsic motivations and coping for learning and compliance, while they have concluded that fulfilling users' motivations and coping needs through gamified security training can result in statistically significant positive behavioral changes.

3 The use of artificial intelligence for counter-terrorism purposes

The rapid improvement of information and communication technologies facilitates the collection and analysis of increasing amounts of data in shorter periods of time, making dragnet surveillance a viable and appealing alternative to targeted surveillance (Verhelst et al., 2020). In that term, AI-driven solutions may be capable of supporting some phases of the counter-terrorism intelligence cycle such as initial demand setting, collection of data and information, as well as intelligence analysis and reporting. According to the United Nation's Office on Counter-Terrorism (2021a) AI can be a powerful tool in counter-terrorism, enabling law enforcement and counter-terrorism agencies to realize game-changing potential, enhancing effectiveness, augmenting existing capacities and enabling them to manage with the massive increase in data. AI can support law enforcement and counter-terrorism agencies, for example, by automating highly repetitive tasks to reduce workload; assisting analysts through predictions of future terrorist scenarios for well-defined, narrow settings; identifying suspicious financial transactions that may be indicative of the financing of terrorism; as well as monitoring internet spaces for terrorist activity at a scale and speed beyond traditionally available human capabilities. Over the past years, governments have increased their use of AI for the collection and evaluation of data in efforts to ensure national security, for example SIGAD US-984XN (PRISM) implemented by the National Security Agency of the United States. According to McKendrick (2019) AI allows higher volumes of data to be analysed, and may perceive patterns in data that would, for reasons of both volume and dimensionality, otherwise be beyond the capacity of human interpretation. The impact of this is that traditional methods of investigation that work outwards from known suspects may be supplemented by methods that analyse the activity of a broad section of an entire population to identify previously unknown threats.

Terrorists are aware of the work scope of the intelligence agencies, so the number of members of a terrorist organization is often limited to carrying out attacks until just before the attack, with strict control over the disclosure of information in mutual, often encrypted communication (Pillar, 2011). Accordingly, breaking even the highest levels of their management does not necessarily mean disclosing information about local cells, especially in decentralized organizations (Bilandžić, 2014). Also, the value of quality information in the field of terrorism is short-lived, which requires timely responses (Byman, 2014). Terrorists typically attack when they are fully confident in the effectiveness of an act, so even less information gathered from the national intelligence may lead them to give up (Clarke, 2004). Although Gerges (2011) found that the US National Security Agency collected about 1.7 billion records of controlled communications daily, in reality the agencies are often faced with a shortage of key information about terrorist networks (Gerecht, 2001). This is best confirmed by the fact that CIA’s estimates in August 2001 indicated possible Al-Qaeda attacks on US interests and targets abroad, but not on US soil (Bilandžić, 2014). In the real world of intelligence agencies, great discoveries are the result of hard work, slow gathering of facts, each of which seems ambiguous, but as the whole helps to make assumptions (Panetta and Newton, 2014). However, AI has the potential for identifying terrorists (and potential terrorists) as well as the timing and location of attacks. According to Huszti-Orbán and Ní Aoláin (2020) biometric markers may be related to a person’s physiological characteristics, such as finger or palm prints, DNA, and facial, iris, or retina recognition (i.e. biological biometrics), while the potential of biometrics in the area of preventing and countering terrorism has received increased and sustained attention in the aftermath of the 9/11 attacks.

According to Deloitte and UOB Group (2018) machine learning can assist in enhancing effectiveness, efficiency and accuracy of processes within a bank’s core and terrorist financing risk detection and reporting system. Traditional systems detect very specific typologies that can be circumvented. Furthermore, the results from these models contain more noise than ‘signals of risk’ as the net is often cast wide in order to not miss a potentially suspicious activity. Monitoring online behaviour can also be used to predict terrorist activities. AI-driven solutions can help automated takedown of (suspiciously) terrorist content. As a step forward, according to the United Nation’s Office on Counter-Terrorism (2021a) predictive models informed by statistics from online sources that have been thoroughly anonymized or at least pseudonymized to protect user privacy could be used to identify trends or forecast the future behaviour of terrorists. This analysis based on aggregated data can be helpful to support security and intelligence agencies, prioritizing scarce resources as operational support, making strategic decisions or providing warnings to the competent authorities.

4 Conclusion: double-edged sword and challenges

As always throughout history, every innovation is useful to humanity as much as it is used for ethical purposes. Artificial intelligence as the simulation of human intelligence processes by machines, especially computer systems, can be a useful tool in the malicious activities of terrorists, and on the other hand, it enables new solutions in the fight against terrorism. As terrorist organizations have opportunities for faster mobility of people, funds and weapons than national organizations bound by international regulations, they are sometimes one step ahead and they have a lot of benefits from the AI solutions. Some other challenges, like societal effects of mass surveillance or lack of AI expertise within governmental organizations, even within the most developed countries, sometimes make the fight against terrorism in cyberspace more difficult. Also, the human rights issues according to McKendrick (2019): lack of well-established norms for the use of AI technology, inherent disproportionality, an expanding but weakly regulated private sector role, or lack of redress; stands as the important segments related to counter-terrorism activities. Further research should focus on technological development of using AI for counter-terrorism purposes, on AI knowledge among national security organizations and continuous improvement of AI related policies among alliances and individual countries.

References

Bilandžić, M. & Leško, L. 2019. Sport i nacionalna sigurnost [Sport and national security]. Zagreb: Despot infinitus.

Bilandžić, M. 2014. Sjeme zla: uvod u studije terorizma. Zagreb: Despot infinitus.

Bilandžić, M. 2019. Nacionalna sigurnost - prognoziranje ugroza. Zagreb: Despot infinitus.

Byman, D. 2014. The Intelligence War on Terrorism. Intelligence & National Security. Routledge: Taylor & Francis Group.

Chaliand, G. & Blin, A. 2007. Introduction. In: Gerard Chaliand and Arnaud Blin (eds.), The History of Terrorism: From Antiquity to Al Qaeda (Berkeley: University of California Press), 1-11.

Clarke, R. 2004. Against all Enemies: Inside America's War on Terror. New York: Free Press.

Deloitte and UOB Group. 2018. The case for artificial intelligence in combating money laundering and terrorist financing: A deep dive into the application of machine learning technology.

Friedman, A. 2003. Terrorism in Context. In: Terrorism: Concepts, Causes and Conflict Resolution. Advanced Systems and Concepts Office, Defense Threat Reduction Agency and Working Group on War, Violence and Terrorism. Institute for Conflict Analysis and Resolution, George Mason University. Fort Belvoir, Virginia.

Gerecht, M. R. 2001. The Counterterrorist Myth. http://www.theatlantic.com/past/docs/issues/2001/07/gerecht.htm (accessed June 20th 2023)

Gerges, F. A. 2011. The Rise and Fall of Al-Qaeda. Oxford University Press.

Gunaratna, R. & Oreg, A. 2010. Al Qaeda's Organizational Structure and its Evolution. Studies in Conflict & Terrorism 33, 12, 1043-1078.

Herbert K. Tillema. 2002. A Brief Theory of Terrorism and Technology. In T. K. Ghosh (Ed.), Science and Technology of Terrorism and Counterterrorism.

Huszti-Orbán, K. & Ní Aoláin, F. 2020. Use of Biometric Data to Identify Terrorists: Best Practice or Risky Business? Human Rights Center. University of Minnesota.

Jones, S. G. & Libicki, M. C. 2008. How Terrorist Groups End: Lessons for Countering al Qa'ida. Santa Monica: RAND Corporation.

Maslow, A. H. 1954. Motivation and personality. New York: Harper and Row.

McKendrick, K. 2019. Artificial Intelligence Prediction and .Counterterrorism. The Royal Institute of International Affairs Chatham House. London.

Panetta, L. & Newton, J. 2014. Worthy Fights: A Memoir of Leadership in War and Peace. USA: Penguin Publishing Group.

Pillar, P. R. 2011. Intelligence and U.S. Foreign Policy: Iraq, 9/11, and Misguided Reform. Columbia University Press.

Shiraz, Z. & Aldrich, R. J. 2013. Globalisation and Borders. In: Dover, R.; Goodman, M. S.; Hillebrand, C. 2013. (ed.) Routledge Companion to Intelligence Studies. Routledge.

Silic, M. & Lowry, P.B. 2020. Using design-science based gamification to improve organizational security training and compliance. Journal of management information systems 37, 1, 129-161.

Tosini, D. 2007. Sociology of Terrorism and Counterterrorism: A Social Science Understanding of Terrorist. Sociology Compass 1, 2, 664–681.

UNICRI. 2020. Stop the virus of disinformation. Accessible at http://unicri.it/sites/default/files/2021-01/misuse_sm_0.pdf

United Nations Office of Counter-Terrorism. 2021a. Countering Terrorism Online with Artificial Intelligence.

United Nations Office of Counter-Terrorism. 2021b. The malicious use of artificial intelligence for terrorist purposes.

Verhelst, H.M., Stannat, A.W. & Mecacci, G. 2020. Machine Learning Against Terrorism: How Big Data Collection and Analysis Infuences the Privacy-Security Dilemma. Science and Engineering Ethics 26, 2975-2984.

Whitman, M.E. & Mattord, H.J. 2018. Management of Information Security. Cengage Learning; 6th edition.