Terrorism – Studies, Analyses, Prevention, 2026, no. 9: 477–482

https://doi.org/10.4467/27204383TER.26.021.23804

Review

Tomasz Wróblewski, Rola Sztucznej inteligencji w zapobieganiu atakom terrorystycznym[1]

Tomasz Michalak

IDEAS Research Institute,
Faculty of Mathematics, Informatics and Mechanics,
University of Warsaw

https://orcid.org/0000-0002-5288-0324

In the third decade of the 21st century, developments in the field of artificial intelligence (AI) have accelerated at an unprecedented rate, a phenomenon referred to as the AI revolution. In an economic context, this technology forms the foundation of the Fourth Industrial Revolution due to its ability to optimise manufacturing processes. Nevertheless, the potential impact of AI on society is multifaceted and goes far beyond the purely industrial sphere. It encompasses both fundamental changes in the way we interact with information and with one another, as well as

[1] T. Wróblewski, *Rola sztucznej inteligencji w zapobieganiu atakom terrorystycznym* (Eng. The role of artificial intelligence in preventing terrorist attacks), Warszawa 2025, Difin, 178 p. The book is available only in Polish.

a profound transformation of the labour market, where the automation of routine tasks is forcing a redefinition of human skills. All of this means that AI brings not only benefits but also many challenges. For example, the implementation of smart systems in medicine, education and public administration offers an opportunity to significantly increase the efficiency and personalisation of services, but at the same time raises critical questions about privacy, algorithmic ethics and accountability for decisions made autonomously by computer systems.

The multifaceted nature of AI's impact on reality is reflected in the realm of national security, as we are witnessing a revolution in the military. The ongoing war in Ukraine has become both a driving force and a testing ground for algorithmic warfare, in which superiority is determined not only by human resources and heavy equipment but also by the ability to rapidly fuse and analyse data from drones, military satellites and other available sources, including open-source ones. The analysis of massive datasets is one of the most important applications of AI algorithms, which are capable of performing advanced inference and identifying correlations and relationships of such high complexity that they are practically impossible for a human to identify. On the battlefield, shortening the decision-making cycle to near real time makes AI a key force multiplier. Furthermore, it should be emphasised that the development of AI not only pertains to the field of software but is also a main catalyst for the advancement of autonomy in weapons systems and robotics. All these trends define the battlefield in Ukraine, it can therefore be concluded that AI plays a very significant role in the ongoing processes of reshaping the global geopolitical architecture.

Technological progress based on AI extends beyond the military sphere. It also has an impact on internal security, ranging from crime prevention to counter-intelligence, counter-terrorism, and hybrid threat mitigation. In all these areas, AI algorithms are used for merging and analysing large datasets, as well as for extracting knowledge from information noise and drawing conclusions based on that knowledge. The development of autonomous systems and robotics is also extremely important in the context of internal security, as these technologies can greatly expand the capabilities of security services. Of course, we must also consider the other side of the coin – AI technologies and developments related to AI can be extremely dangerous in the hands of terrorists.

The potential of artificial intelligence in combating terrorism was highlighted in the publication of Tomasz Wróblewski entitled *Rola sztucznej inteligencji w zapobieganiu atakom terrorystycznym* (Eng. The role of artificial intelligence in preventing terrorist attacks), which was published in 2025 by Difin Publishing and runs 178 pages. Before proceeding with a substantive analysis of this publication, it is necessary to provide a brief overview of the author in order to avoid the misconceptions that are common in the public sphere. The author of the reviewed publication, Tomasz Wróblewski, PhD – a researcher and academic with extensive expertise in the field of defence and internal security – should not be confused with the journalist and publicist of the same name. He is a graduate of the National Defence Academy (currently the War Studies University). He has held leadership positions in the Polish Armed Forces and has many years of service at the Central Investigation Bureau of Police (CBŚP).

The book under review is divided into an introduction and four chapters. The first chapter, entitled *The basics of terrorism and AI technology*, is introductory and contextual. The author defines terrorism, presents the fundamental trends in the evolution of this phenomenon, and describes the goals and methods of contemporary extremist groups. He defines key concepts in the field of AI, with particular emphasis on deep learning and machine learning.

The second chapter – *Research on the use of AI in the prevention of terrorism* – begins with the author outlining, through a few examples, some areas of research into the use of AI to combat terrorism. The following subchapter briefly describes selected centres and organisations that examine AI from a security perspective, with Wróblewski focusing more on researching the security of AI than on the use of this technology for counter-terrorism purposes. The next subchapter is particularly interesting, as it compares traditional counter-terrorism methods with modern solutions based on AI. It offers a comprehensive overview of the new opportunities that AI offers the security services and the risks posed by this technology. In this light, the previous two subchapters leave something to be desired, as, contrary to the title of the entire chapter, they focus only on a few aspects of this multidimensional issue. The chapter is complemented by an analysis and discussion of the results of the expert opinion survey on the effectiveness of AI tools in combating terrorism. The survey research referred to by the author was conducted in 2022 as part of "Terrorism – Studies, Analyses, Prevention" – the journal of the Internal

Security Agency. Ninety four experts took part in the survey, mostly from the state administration and academic centres. I consider both the findings of the study and the discussion to be valuable, as they demonstrate an active and profound interest in the challenges – posed by the rapid development of AI – on the part of the internal security expert community in Poland.

The third chapter – *Identifying threats using AI* – is the most comprehensive and, in my opinion, the most interesting, as it covers by far the widest range of aspects and examples of how AI-based technologies are used to combat terrorism. The first subchapter relates to data processing and analysis. The second subchapter discusses the use of natural language processing techniques to analyse communication between terrorists. In fact, there is much more to it than that, as a significant portion of the text deals with the risks posed by the development of large language models (LLM), which can be exploited by terrorists in various ways. I consider this analysis to be both very necessary and accurate. The next subchapter focuses on the fundamental issues relating to social media monitoring using AI technology. In it, the author discusses in greater detail the design of predictive models that can be used to identify the intentions of terrorist groups at a relatively early stage. The subchapter 3.4 describes the use of AI solutions for analysing financial data in the context of anti-money laundering and counter-terrorist financing. Wróblewski emphasises the advantage of algorithms over human capabilities when dealing with the sheer volume of data and the complexity of criminal patterns that can be identified from that data. In the next subchapter, the author introduced issues related to image recognition systems, in particular faces. He cites an interesting example of how these technologies were used in 2024 in Berlin by a German female terrorist from the Red Army Faction. The last subchapter is surprising because it deals with the use of AI to support operations in crisis situations that may result from terrorist activities. Research into the use of AI in crisis situations is extremely important, and I believe it is essential to address this issue in the context of terrorism as well.

In the fourth chapter, the author focuses on ethical and social implications of using AI in the context of security. He also analyses the regulatory framework currently being developed at the national and international level.

It should be emphasised that Tomasz Wróblewski took on an exceptionally difficult topic. Artificial intelligence is, in fact, a technology

characterised by an almost unprecedented pace of development, one that permeates many aspects of the lives of individuals and societies. In such a situation, any attempt to provide a comprehensive overview of even a fraction of the available possibilities or directions for the development of AI from the perspective of counter-terrorism efforts is a huge challenge. This becomes even more apparent when we consider the very nature of terrorism – a phenomenon that is extremely complex, multifaceted and constantly evolving. Each attempt to combine these two areas of complexity and to systematically organise this field of research is praiseworthy. The author's interdisciplinary approach to academic interests proved to be extremely valuable in this context.

One of the publication's strengths is its language. Wróblewski avoids excessive use of technical jargon, making the text accessible to non-IT professionals. However, I believe that this book is also very valuable for this group, as it helps them grasp the complexity of issues related both to the existence of technology as such and to its use in society. Another strength of the book is its two-pronged approach to analysing the role of AI in the field of security. On the one hand, the author discusses the use of this technology by government agencies, on the other, he analyses the ways in which the same technologies can be adapted by terrorist groups to plan attacks, spread disinformation or carry out operations in cyberspace. Presenting AI as a tool available to both sides of the conflict is important because it allows the reader to better assess the ever-changing threats.

In summary, Tomasz Wróblewski's work is an important publication that addresses the essence of contemporary threats related to terrorism, which are taking on new forms right before our eyes. The author has succeeded in creating an interesting and valuable compilation of knowledge that serves as a good starting point for a deeper analysis of specific issues.

Assoc. Prof. Tomasz Michalak
Professor of the University of Warsaw

AI Strategy Lab leader at IDEAS Research Institute subordinate to the Ministry of Digital Affairs and the Ministry of National Defence as well as a lecturer at the Faculty of Mathematics, Informatics and Mechanics of the University of Warsaw. Previously, the leader

of the independent 'AI for Security' research team at IDEAS NCBR. He is a graduate of the University of Warsaw. He obtained a PhD at the University of Antwerp and his postdoctoral degree at the AGH University. During his academic career, he conducted research at the Department of Computer Science at the University of Oxford, the School of Engineering and Computer Science at the University of Southampton as well as the Department of Computer Science at the University of Liverpool. From 2024 to 2025, he served as co-director of the 'R-GRID: AI algorithms for Threat Prediction and Power Grid Protection' project, funded by NATO grant, and as an expert on an EU-CIP project concerning the protection of critical infrastructure in the European Union.

Contact: tomasz.michalak@ideas.edu.pl