Ladies and Gentlemen!

I am pleased to be able to recommend the latest issue of the "Internal Security Review". In this issue, we have devoted a great deal of attention to the activities of various uniformed services in Poland. Our authors write, among other things, about specialist rescue operations in the State Fire Service, issues relating to human resources policy in the Border Guard and the Polish Armed Forces, as well as about difficult experiences of soldiers and officers who were guarding our country's eastern border in 2021 during the Russian-Belarusian operation 'Sluice'.

The geopolitical situation in Central and Eastern Europe, which is heavily influenced by the armed conflict in Ukraine, is creating new demands on threat response systems, including CBRNE (chemical, biological, radiological, nuclear and explosive). CBRN mobile laboratories, with which the State Fire Service has been equipped play an important role in ensuring safety in Poland. Grzegorz Bugaj, PhD Eng., analysed operational effectiveness of these laboratories in accordance with the relevant legislation and the principles of the National Firefighting and Rescue System. He also identified the challenges and limitations associated with their use. One such challenge is recruiting and retaining the highly skilled staff needed to operate such technologically advanced solutions.

Radosław Wiśniewski, PhD and Denis Tomala write about the need to ensure that uniformed services have an optimal number of well-trained personnel, enabling them to carry out their tasks to a sufficiently high standard. They present the results of research into Border Guard officer retention. The researchers sought answers to questions regarding the extent to which individual and organisational factors influence whether officers leave or remain in the service, and what solutions might not only increase interest

in a career in the Border Guard – and in uniformed services in general – but also optimise the conditions for serving for many years. Having experienced staff on the team, among many other benefits, ensures that the staff succession process runs smoothly. The insights gained from the research presented enable us to refine our internal human resources practices and enhance the stability of our formation, as well as state security. It is well worth reading.

The article by Major Mariusz Domżalski, PhD, deals with the issue of human resources policy, but within the Polish Armed Forces. He discusses matters relating to the prohibition on undertaking paid employment and carrying out business activities by a professional soldier. It should be borne in mind that the labour market is becoming increasingly complex and new forms of employment are emerging. As the author rightly points out, this may require a clearer definition of the concept of paid employment and the adoption of implementing regulations concerning occupational restrictions for persons serving in uniformed formations.

Norbert Łucarz describes the operation 'Sluice' and the migrants instrumentalisation practice in the policies of the Russian Federation and the Republic of Belarus. As a result of this operation, Polish uniformed services guarding the Polish-Belarusian border became the target of aggression from migrants and Belarusian officers supporting them. The operation 'Sluice' was accompanied by hostile propaganda and disinformation activities – narratives emerged in which Polish security services were presented in an extremely negative light. The result of these actions was growing polarisation among the Polish society. One expression of opposition to these events was the 'United behind the Polish uniform' campaign. Its aim was to express support for people who, in the course of their duties, had to cope with intense physical and mental strain.

Agata Rytel also writes about attacks on the integrity of the Polish border with Belarus, addressing the issue of hybrid operations carried out by the Russian Federation, which in 2021 – 2024 were directed at the Polish information sphere and cyberspace. The author shows that these events were directly linked to the war in Ukraine and constituted deliberate interference by Russia and Belarus. This is yet another example of the complex nature of modern cyberattacks, in which the attacker combines various types of activities and carries them out across multiple domains.

One of the most common targets of attacks is financial sector. Associate Professor Kamil Mroczka and Paweł Piekutowski write about enhancing the digital resilience of entities in this sector in light of the obligations arising from the DORA (Digital Operational Resilience Act) regulation. They point to TLPT (threat-led penetration testing) tests, as an effective method of strengthening this resilience. The aim of these tests is to replicate real-world attack scenarios as closely as possible, in order to precisely identify vulnerabilities in an organisation's cyber security system and improve its ability to detect cyber threats. The authors believe TLPT tests are essential, as they enable the verification not only of technical measures but also of staff behaviour.

The issue of resilience testing also features in Klaudia Maciata's article on offshore wind farms, which are vital to the country's energy security. Their specific location increases their vulnerability to hybrid threats, including in cyberspace. It is therefore necessary to conduct multi-faceted resilience testing of these farms. In the cyber domain, this will include, among other things, red teaming exercises, i.e. simulated attacks that replicate the tactics and techniques used by cybercriminals. According to the author, legal, technological and organisational measures must be combined in order to improve the safety of wind farms.

The emergence of artificial intelligence has a significant impact on the development of cyber threats. This is discussed in an article by Jakub Gajecki. Advances in AI and machine learning have made threats more complex, dynamic and difficult to detect. In this context, the author analyses and evaluates the existing defence strategies. He points to the role of international cooperation in combating cybercrime and the need to keep regulations up to date. Most of them were developed at a time when AI technologies were not yet being used in cyber operations on such a large scale.

This issue also features a topic of significance for crisis management and defence of the Republic of Poland concerning the safeguarding of the continuity of state functioning.

In the 'Competition entries' section, we present the text by David Cybulski on the government connectivity and communication in the event of a national security threat. The implementation of the System of Secure State Communication supervised by the minister responsible for internal affairs is expected to lead

to a reduction in response times of the administration and security services, as well as to improve rescue in crisis situations.

'Internal Security Review' is a periodical of a counterintelligence-oriented special service, it could hardly omit a reference to issues revolving around Article 130 of the Criminal Code. Tomasz Safjański, PhD, reviewed for us the monograph entitled *Szpiegostwo. Studium kryminologiczne* (Espionage. Cryminology study). Its author, Associate Professor Piotr Chlebowicz, undertook a comprehensive criminological analysis of the phenomenon of espionage in Poland between 1990 and 2022. This publication is a summary of his many years of research based on file and archival research, informal interviews and literature on the subject. According to the reviewer, this is outstanding work and should become required reading for criminologists, criminal lawyers, analysts, as well as politicians and others responsible for national security. I also encourage you to read this unique book!

To conclude, I would like to thank the authors, reviewers, members of the Academic Editorial Board and the editorial team for co-creating the journal I lead. It is both a pleasure and a responsibility for me. I believe that the topics we address are interesting to you, and that our contribution to the popularisation of security issues is both needed and recognised.

Editor-in-Chief
Daria Olender, PhD