Ladies and Gentlemen!

The next issue of the "Internal Security Review" comes at a time of serious crisis in the international security system. The war in Ukraine, which is threatening the very foundations of the country's existence in its current form; the conflict in the Middle East, which could escalate into a regional war with the potential to involve nuclear powers; the increasingly fierce rivalry between the US and the People's Republic of China; global climate change with its devastating effects on the environment and, finally, dangerous technological developments capable of dramatically changing the nature of all socio-political processes – all these events destabilise the international order, forcing the search for new paradigms for the operation of special services in changing geopolitical realities. At the same time, the adaptation to the new challenges has to be effective and fast, in a situation where the Doomsday Clock, for the first time since 1947, already indicates only one and a half minutes to midnight, understood as the atomic self-destruction of mankind.

I hope that the new issue meets the demands of turbulent times. Thus, we offer you an article devoted to the use of analytical models of *cyber threat intelligence* in combating disinformation in the broadest sense; a legal analysis of issues related to counterintelligence shield of the Republic of Poland; interesting reflections on: forms of financing terrorist attacks based on the attack on Crocus City Hall; search tools used in web-based open source intelligence; provocation as a tool of Russian hybrid policy and, finally, a polygraph research in the work of special service.

In addition, we offer a practical summary of the identifiers of Russian sabotage and diversion groups developed by Ukrainian services, which I feel could prove a useful tool in a situation where

Russian GRU and FSB are carrying out kinetic operations in Europe that have long since crossed the threshold of a "hot" conflict.

Also of interest are the report of the debate "Global cybersecurity in a the face of a new cold war" and articles based on the winning competition entries dealing with energy security in Europe and the development of cryptocurrencies.

I think that themes in this issue are up to date and will prove useful to both academics and practitioners trying to adapt the way the special services operate to threats unseen for decades.

Editor-in-Chief
Marek Świerczek, PhD