

## **Summary of the doctoral dissertation entitled: Information warfare in the foreign policy of the Russian Federation towards Poland in 2010-2022.**

Information warfare is closely associated with Russian political culture and the foreign policy pursued by the Kremlin. It has enduring features developed over decades, which have been perpetuated in the political system of the Union of Soviet Socialist Republics and are now evolving in the system of the Russian Federation. The subject of the dissertation's research is the Russian Federation's use of information warfare as an instrument of its foreign policy towards Poland. The tools that Russia uses are asymmetrical in nature. With their help, it carries out actions on an unprecedented scale in the offline dimension, but above all in the online sphere. In this respect, they are based on information warfare, which involves simultaneously influencing online audiences with propaganda techniques and launching cyber-attacks on ICT infrastructure. The Kremlin's information warfare poses an increasing threat to Poland's security, both nationally and internationally.

The main research objective of the dissertation is to determine the conditions, nature and implications of the information war of the Russian Federation against Poland in the years 2010-2022. The dissertation seeks first of all to identify and characterise its conditions and the direct and indirect goals that the Russian Federation pursues through it. Furthermore, the dissertation aims to identify the instruments it uses for this purpose, as well as to indicate the most important implications of the above actions. It should also be noted that, within the framework of this dissertation, Russian information warfare is seen both as a propaganda impact on online audiences and as activities conducted in cyberspace by launching cyber attacks. Therefore, the purpose of the thesis is to discuss the propaganda tools and techniques that are used in pro-Russian information channels on the Internet, in messages concerning Poland and Polish-Russian relations, as well as to present the characteristics of Russian attacks on Poland in cyberspace.

Within the framework of the dissertation, the following main research hypothesis was verified. Information warfare as an instrument of foreign policy conducted by the Russian Federation is steadily gaining in importance, which should also be applied to Polish-Russian relations. In its information warfare against Poland, Russia employs propaganda techniques and tools to exert an informational influence on the recipient. These activities are undertaken through Russian information portals. The Russian Federation's information warfare against Poland also manifests through cyber-attacks on Poland in cyberspace. The activities undertaken within the framework of the indicated dimensions are complementary to each other. The

objective of the operations undertaken by Russia is primarily to weaken internal state structures, deepen social cleavages, marginalise Poland's position on the international arena, create a negative image of Poland on the international arena and, above all, pursue its own interests.

The time frame of the research covers the period from 2010 to 2022, owing to the key events in Polish-Russian relations, starting from the Smolensk catastrophe of 2010 to the full-scale invasion of Ukraine by the Russian Federation in 2022. The most important issues of contention during the period under review include, first and foremost, historical policy, diversification of energy sources, security policy in Central and Eastern Europe, NATO security policy, the crash of the government plane carrying the President of the Republic of Poland in Smolensk, the annexation of the Crimean Peninsula and the war in Ukraine, as well as the Eastern Partnership Programme.

The following methodological assumptions were made as within the scope of the dissertation. The Russian English-language news portal Sputnik News International and the website of the government news agency TASS were subjected to research. The research included: identifying the types of content published on the websites of the above entities, determining the frequency of contentious issues in Polish-Russian relations in the articles, identifying the content framing used and identifying the propaganda techniques used. With regard to the research on the activity of the Russian Federation towards Poland in cyberspace, an analysis of source materials was conducted, in particular the reports published by the CERT Polska Team and the CSIRT GOV Computer Security Incident Response Team. As a result, it was possible to characterise Russian activity undertaken against Polish ICT infrastructure.

The research indicates that the Russian Federation uses information warfare as an instrument of its foreign policy towards Poland. The Kremlin's activity boils down to an information influence campaign on the Internet through the Sputnik News International news portal and the TASS news agency website. The Russian Federation carries out hostile activity against Poland in cyberspace by undertaking attacks, primarily on the country's critical infrastructure. The actions taken by the Kremlin in the areas outlined above are complementary to each other. Information warfare in the Russian view is a comprehensive and unlimited instrument. Furthermore, the Kremlin's activities are part of the contentious issues in Polish-Russian relations, thus correlating with the current state of bilateral relations. Internally, the aim of the Russian Federation is to create and fuel socio-political disputes in Poland. In the external dimension, it is undermining Poland's image and presenting Poland as an anti-Russian, unstable and untrustworthy state, primarily in the context of Warsaw-NATO, Warsaw-EU relations. A long-lasting information warfare waged by Russia may lead to deepening social

polarisation, which poses a threat to Poland's internal stability. Furthermore, it can destabilise Poland's relations with its allies, especially in the context of cooperation with the North Atlantic Alliance and the European Union. It is therefore necessary to develop mechanisms to counteract these threats, as well as to continuously monitor them.