Contemporary Security Problems of Poland and the Czech Republic

Edited by

Ewelina Kancik-Kołtun

Maria Curie-Skłodowska University Press

Contemporary Security Problems of Poland and the Czech Republic

Ministry of Foreign Affairs
Republic of Poland

Public task *Polish-Czech perspective on contemporary security problems* financed by the Ministry of Foreign Affairs of the Republic of Poland within the grant competition "Polish-Czech Forum to bring societies closer together, enhance cooperation and foster good neighbourship 2024"

UMCS
WYDAWNICTWO

Contemporary Security Problems of Poland and the Czech Republic

Edited by

Ewelina Kancik-Kołtun

Maria Curie-Skłodowska University Press
Lublin 2024

Reviewer
Prof. JUDr. PhDr. Miroslav Mareš

Editor
Marta Kasprzak

Technical editor
Agnieszka Muchowska

Cover and front page design
Krzysztof Trojnar

Typesetting
Marcin Wachowicz

Cover image: lovephoto (freepik.com)

ISBN 978-83-227-9860-7

Maria Curie-Skłodowska University Press
ul. Idziego Radziszewskiego 11, 20-031 Lublin, Poland
tel. +48 81 537 53 04
www.wydawnictwo.umcs.eu
e-mail: sekretariat@wydawnictwo.umcs.lublin.pl

Sales Department
tel./fax +48 81 537 53 02
Online bookstore: www.wydawnictwo.umcs.eu
e-mail: wydawnictwo@umcs.eu

Contents

PART IV. MIGRATION SECURITY

PART V. WAR IN UKRAINE

PART VI. SECURITY ISSUES AND THREATS

Introduction

Security is perceived as a value through the prism of peace, which occupies the most important place in all contemporary values. Security is therefore the primary human need and concerns not only individuals, but also entire states. Currently, we see many problems in various areas and types of security, both at the state, regional and international levels. Due to the lack of a sense of security, concerns arise among citizens, political players and state institutions, which, based on security threats, have shaped our interests in implementing the topic of contemporary security problems. The publication discusses the dimension of security primarily with the conditions of researchers from Poland and the Czech Republic.

The situation after the beginning of the Russian aggression against Ukraine significantly affected both Poland and the Czech Republic and security in the region in almost every respect in the socio-political sphere, but also internal and international security. These changes can be seen at the political, security, economic, media, communication and technology, and military levels.

The book consists of six parts. The first part, entitled "Geopolitics and Diplomacy", contains two articles. The first one, authored by Marek Pietraś, entitled *Global Geopolitical Space of Poland and the Czech Republic*, presents a proposal for a new approach to the polarity of the international system, taking into account the functioning of Poland and the Czech Republic in the global geopolitical space, which has entered a period of accelerated changes, growing rivalry and a new form of international turbulence. The second article by Ewelina Kancik-Kołtun – *Diplomacy of Security – Outline of the Issues* – is an attempt to define the concept of security diplomacy in the context of the importance of security in international relations. The article presents the issues of diplomacy in the context of realizing national and international interests in the area of security. The second part of the book, devoted to disinformation, begins with an article by Jakub Olchowski entitled *Russia's Disinformation as a Threat to the Security of Poland and the Czech Republic*. The article examines the threat that Russian disinformation poses to the security of Poland and the Czech Republic and emphasizes the need for both countries to strengthen their resistance to disinformation threats through coordinated actions in the field of cybersecurity, public awareness, and international cooperation. The next article – *Disinformation in Poland – Diagnosis, Combating, Counteracting* – by Agnieszka Demczuk is an analysis of contemporary public discourse, which is infused with disinformation and conspiracy narratives, which have become fundamental elements of influence

campaigns conducted by various propagandists in democratic systems. The author draws particular attention to the fact that the conglomerate of disinformation reinforced by IT automation systems enables the growth of content harmful to democratic institutions and values, such as discourse, human rights, the rule of law and security, extremely effectively and on an unprecedented scale, which is why education, moderation, regulation, as well as a new media policy based on proactive ethics in combating and preventing disinformation are needed. The next article by Ondřej Filipec – *What States Shall Do (Not) to Counteract Disinformation. The Inspiration from the Czech Republic* – describes actions aimed at counteracting disinformation and propaganda at the state level by presenting a broader picture and experiences with proposals and adopted measures in the Czech Republic. The last article in this part – *Strategic Communication (StratCom) as a Tool to Counter Disinformation. Its Advantages and Limits* – by Tomáš Kolomazník discusses strategic communication as one of the tools to eliminate disinformation narratives in society, and its aim is to present strategic communication, especially in the Czech context.

The section on media and security opens with an article by Piotr Celiński – *Communication Security: Between Biomedia and Biopolitics* – in which the author undertakes an initial analysis of selected communication security issues. Taking biomedia technologies as a starting point, he focuses on the political and social ways of designing, implementing and using communication technologies that come into close contact with sensory organs and the body. In the next article – *Medical Data Security in the Digital Era* – Justyna Kięczkowska discusses the main aspects of medical data security, paying particular attention to technical, organizational and regulatory protection measures to effectively secure medical data. The last article in this section – *TikTok as a Security Threat? A Challenge for Political Actors in the Czech Republic* – by Daniel Šárovec focuses on TikTok from a security perspective, as information from several state authorities indicates that this application poses a particular risk of compromising security. The researcher, thus, tries to answer the question of whether it is appropriate to choose the path of partial bans and restrictions on this application.

The next part of the book is devoted to migration security. It begins with an article by Michal Klíma – *The Migration Crisis of 2015–2024 and Its Impact on European Security* – in which the author discusses a new security threat, namely the migration crisis facing Europe and Western democracies. The article *The Limits of Technocratic Decision-Making: The 2015 European Union Relocation Policy and the Blind Spot Theory*, by Katarzyna Marzęda-Młynarska presents the EU's relocation policy through the prism of the "blind spot" theory, which emphasizes the organizational and cognitive limitations in decision-making processes. The author points out that despite the EU's comprehensive migration management system, the relocation policy failed due to a narrow technocratic approach that ignores the

socio-political and cultural dimensions of the crisis. The penultimate part of the book is devoted to the war in Ukraine. Adrian Szumowski in his article *Critical Infrastructure Importance during the War in Ukraine 2022–2024*, analyzes the war in Ukraine from the perspective of causing a renewed interest in the destruction and protection of critical infrastructure nodes in a specific region of space. The author wonders whether the network of critical infrastructure, especially at the global level, is dense enough to transmit waves of its destruction strong enough through the transnational social space to trigger mutual defense mechanisms and be the cause of global war. Another article by Zdeněk Rod – *Reconstruction Roadmap: Current Perspectives on Ukraine's Post-Conflict Recovery* – analyzes considerations and expectations regarding the reconstruction of Ukraine after the conflict, shedding light on key aspects of this complex problem. The last part of the book is devoted to security problems and includes three articles. The first article by Miroslav Plundrich, entitled *How Foreign Activities of Hamas Strengthen Its Capacity Against Israel*, examines the critical role of foreign diplomatic and financial support in the operational and political strengthening of Hamas from 2006 to October 7, 2023. In turn, using the concept of anti-diplomacy, it analyzes how non-state actors, such as Hamas, engage in foreign policy activities similar to those of states. In their article, *Taiwan: One of the Most Dangerous Places in the World*, Agata Wiktoria Ziętek and Elizabeth Freund Larus analyze Taiwan's security. Sarah Cernikova, in her latest article, *Drugs and Organized Crime as a Non-Traditional Threat to National Security*, addresses the topic of drugs and organized crime as an unusual threat to the national security of the Czech Republic.

PART I

Geopolitics and Diplomacy

MAREK PIETRAŚ

MARIA CURIE-SKŁODOWSKA UNIVERSITY, LUBLIN

The Global Geopolitical Space of Poland and the Czech Republic

Abstract: Poland and the Czech Republic operate in a global geopolitical space which has entered a period of accelerated changes, growing rivalry and a new form of international turbulence. These changes – without a crystallized form of the international order following the end of the Cold War – accelerated after Russia's aggression against Ukraine and began to be identified as a turning point in the functioning of the global international system. In this context, the subject of the analysis is the polarity of this system in a period of change. The objective of the article is, firstly, to propose a new approach to the polarity of the international system. It was recognized that the previous approaches were static and single-level, referring to the relative surplus of power of one, two or more states at the level of the global international system. In place of such thinking, a dynamic approach was proposed – without denying the importance of relative power – focused on geopolitical strategies, i.e. functional thinking, and on two-level polarity taking into account the global international system and regional systems. The second objective, referring to the proposed dynamic and two-level approaches to polarity, is to analyse the cases of selected global powers and polarity at the regional level. In this context, the geopolitical strategies of Russia, China, the United States, and the regional level of the Global South were synthetically analysed.

Keywords: international system; polarity; dynamic and two-level model of polarity; Russia's aggression against Ukraine; geopolitical strategies of Russia; China; the United States; Global South

Introduction

The geopolitical space of the international system, in which Poland and the Czech Republic operate, is changing, and an important feature of these changes is their acceleration. On the one hand, it is the result of an ongoing long-term change conditioned by the collapse of the bipolar system, the end of the Cold War, which was compounded by globalisation processes with a synergistic effect. On the other hand,

changes at the level of the international system, its geopolitical space, were accelerated by an "extemporary" factor, well capable of producing long-term consequences, which is Russia's aggression against Ukraine. The ongoing change in the structure and functioning of the global international system does not seem to be a temporary crisis, but a permanent change in the geopolitical space, sometimes perceived as a turning point. The awareness of radicalism and profound nature of the emerging changes is not accompanied by a vision of their direction. In contrast to the change in the international system that took place after the end of World War II in 1945, or the Cold War at the turn of the 1980s and 1990s, when there existed a "creator", a "director" of the emerging new international order, it is now difficult to indicate a global "architect". The international order appears to be "adrift", in a direction difficult to identify clearly, perhaps with the exception of increasing instability and unpredictability.

For the purposes of the analysis, it was assumed that a key feature of contemporary international relations is the growing importance of changes at the level of the international system, which determine the foreign policies of states. The changes being in progress today, create a geopolitical space in which Poland and the Czech Republic function. The uniqueness of these changes is often referred to as a turning point in the functioning of the global international system, identified as the end of the post-Cold War period and a new phase of international turbulence. Adam D. Rotfeld called this period marked by the lack of a crystallized form of the international order in the wake of the Cold War conclusion, an "inter-epoch" already in 2008 (Rotfeld, 2008, p. 15).

In the geopolitical space, in which Poland and the Czech Republic operate, structural and functional changes are taking place. The former are related to the polarity of the international system in terms of the structure of power concentration and are associated with the growth of geopolitical competition, the reconstruction of the geopolitical map of the world and the shift of the existing dividing lines. A new and significant element of this process is the growing geopolitical importance of the Global South, which is no longer a mere background for the rivalry between superpowers. Many states are reorienting their geopolitical strategies and re-evaluating previous priorities.

Functional changes, in turn, denote, primarily, a new quality of social processes in which structural changes take place. These include, for example, the growing importance of artificial intelligence, the emergence of cyberspace, a new quality of international interdependencies, the increasing asymmetry of globalisation processes with their limitation at the economic level and the continuation of global human mobility, circulation of information, shrinkage of time and space, or the activity of non-state entities also becoming carriers of power.

Being aware of the complexity of the changes determining the geopolitical space of Poland and the Czech Republic, the subject and the objective of the analysis will

be to identify the specificity of the emerging structural changes with a proposal of a model for their perception and identification of the geopolitical strategies pursued by the main states whose potentials determine the polarity of the international system. The geopolitical strategies of Russia, the United States, China and the Global South will be analysed, regardless of the awareness of the deficient cohesiveness in the latter. In other words, the subject of the analysis will be: 1) structural changes, i.e. the polarity of the international system; 2) geopolitical strategies of the main actors in the international system.

In the methodological terms, according to the concept of David Singer's levels of analysis (Singer, 1961, pp. 77–92), changes at the level of the international system are treated as an independent variable, a global context, creating the international environment of Poland and the Czech Republic. An assumption was also made according to which the importance of the so-called systemic determinants of the foreign policy of states is increasing. Systemic determinants – as Kenneth Waltz emphasised – imply the focus on how the whole determines the parts thereof (Waltz, 1979).

The change in the polarity of the international system

The polarity of the international system refers to a kind of structure for concentrating the power of states or their group, at a given historical moment of a polyarchic, decentralised international environment. It results from the relative surplus of the power held by a state or a group of states compared to others. It is analysed primarily in relation to the global international system, although one can imagine its use in the analysis of regional systems. Neorealism contributed significantly to the spread of such a mindset. Waltz qualified the polarity of the international system as one of the three elements in the analysis of its structure (Waltz, 1979). The structure of polarity is a historical process, which means that it changes with the shift in the relative power of states (Kennedy, 1994). In the literature on the subject and in the context of the historical variability of the polarity of international systems equated with the relative surplus of the power of specific states, three types of them were identified: unipolar, bipolar and multipolar. Richard Haass, suggesting the lack of a relative surplus of power in the international system, or the mutual balancing of power potentials, drew attention to the fact that the world had entered the stage of lack of polarity or zero-polarity after the period of unipolar dominance of the United States (Haass, 2008).

For thousands of years, the structure of power distribution, the so-called polarity of the world understood as the existence of dominant states and empires, was an important factor determining the functioning of the international order, creating its geopolitical space of other states' behaviours. After the collapse of the bipolar

order specific to the Cold War period, the polarity of the post-Cold War order is a dynamic process of *ad hoc* and transitional solutions, which means the lack of permanent form development. At the same time, the process of accelerating the change in the relative power of superpowers, and other states as well, was initiated. In other words, the relative resources of states' power, viewed in comparison to other states, began to change quickly, causing variability in assessments on the polarity of the order, also resulting from the difficulty of its identification. In past eras, the change of the dominant power, and thus also of the structure of the order, took place over a long period of time (Gałganek, 1992; Modelski, 1987).

An important element in the analysis of the polarity of international systems was the discussion on the cause-and-effect relationship between the polarity structure and the stability of the system (Kondrakiewicz, 1999). Views on this subject are not only diverse, but also contradictory. The main axis of the dispute during the Cold War period was the assessment of the stability of the bipolar system and the multipolar system. Waltz believed that the bipolar system was more stable, because under the conditions of two power centres it allows for controlling the subordinate areas of influence and reduces the likelihood of a bipolar confrontation (Waltz, 1964, p. 881 ff; Waltz, 1979, pp. 170–171). After the end of the Cold War, John Mearsheimer was a supporter of the stabilising usefulness of the bipolar system (Mearsheimer, 2014, pp. 14–15; Mearsheimer, 1990, pp. 5–56). In a polemic with Waltz, Karl Deutsch and David Singer formulated arguments in favour of greater stability achieved by the multipolar system. They claimed that although the likelihood of conflict is greater, the freedom of interstate association and of selecting allies in the multipolar system, stabilises this arrangement (Deutsch & Singer, 1964, p. 390 ff). After the end of the Cold War confrontation and in the conditions of the hegemonic position of the United States, an argument in favour of the stabilising properties of the unipolar system appeared, clearly inspired by the concept of hegemonic stability theory (Keohane, 1984) formulated by Robert Keohan and the belief that the hegemon can provide common goods. It is a system in which one state has a surplus of power and is not balanced by other states or their coalition (Wohlforth, 1999, pp. 5–41).

The ways of defining the polarity of the international system proposed in the literature were distinguished by two features. First of all, these are static definitions with a focus on the relative power surplus of a state or states at a given moment in the historical process. The number of centres – most often states – in which the relative power surplus is concentrated (one, two or several) determined the structure of the international system, its polarity (Krzyżanowska-Skowronek, 2024, p. 97 ff). Secondly, these are single-level approaches with a focus on the structure, the number of centres of power accumulation at the level of the global international system.

Meanwhile, the shift in the relative power of states and the resulting change in the geopolitical space of the globe are significantly accelerated (Pietraś, 2021, p. 412 ff).

After the collapse of the former USSR, it seemed that Russia, as its successor, entered the period of post-superpower position, losing previous opportunities to influence the international environment. However, the period of Vladimir Putin's government has been primarily a restoration of Russia's military might, which has become an instrument of neo-imperial policy, attempts to regain spheres of influence and intimidation of the international environment. There are many indications that after the aggression against Ukraine, Russia's relative position in the changing global balance of power will be weakened (Pietraś, 2024).

After the end of the Cold War and the collapse of the former USSR, the United States became "by leaps and bounds" a multidimensional, complex hegemonic power with no possibility of having their position balanced in the 1990s or at the beginning of the 21st century. There were even talks of the unipolar, hegemonic stability of the international order dominated by them. However, the country began to lose its relative power surplus as a result of the so-called war on terrorism and military interventions in Afghanistan and Iraq, the global financial crisis which began in 2008, but above all the already cited phenomenon called "the growth of the rest of the world", which reduces the relative deficit of power in relation to the United States and other Western states as well. This was clearly due to the processes of globalisation, which relatively weakened the West and relatively strengthened the rest of the world. A counterweight for the United States is being created, and this means that the system has ceased to be unipolar and is entering a period of instability (Wohlforth, 1999).

Since the beginning of the 21st century, the largest relative change in power has occurred between the United States and China. For example, in the economic sphere, China's GDP was 2.5 times smaller than that of the United States in 2010, but in 2019, China's GDP attained two thirds of the United States' GDP. In this context, in 2017, Chinese President Xi Jinping said at the Davos Economic Forum that China is a superpower, ready to take the central spot on the world political scene and be a leader. The economic penetration strategy called "Belt and Road Initiative" became an element serving this purpose (Wohlforth, 1999, pp. 416–417). The US national security strategy of October 2022 recognised that China is a country that wants to change the international order and has the resources to do so (White House, 2022).

When analysing the changes in the relative capabilities of the largest powers, one cannot forget about the changes in the relative strength of regional powers with consequences for the global international system. This seems to be an element of the new quality displayed by the polarity of the international system and the way of understanding it in the form of mutual conditioning of the potential possessed by regional and global powers. This means that the concentration of power in the international system, probably no longer adequately called its polarity, has become a two-level phenomenon in relation to states (not to mention non-state actors as carriers of power), including

the mutually determinant relative potentials of global superpowers and regional powers. Russia's aggression against Ukraine confirms the autonomy of foreign policies pursued by regional powers such as Turkey (Smoleń, 2020), Brazil, Saudi Arabia with their consequences for the global international system. Saudi Arabia's involvement in multilateral diplomacy aimed at a peaceful termination and resolution to Russia's aggression against Ukraine, being an attempt to take on roles "reserved" for the existing global superpowers, seems to confirm this tendency.

In order to generalise the previously analysed phenomenon of regional powers gaining an autonomous position with its consequences for the global international order and treating this phenomenon as the regularity of the shift in the modern international system, it is justified to draw on the analyses contained in the *SIPRI Yearbook* in 2005. It was then found that at the level of states in the global international system, there are simultaneously occurring processes of power concentration and diffusion, which are contradictory in their logic (Bailes, 2005, p. 4). From the perspective of the global international system, diffusion of power is the outcome of its concentration by regional powers, which may sound paradoxical. "The growth of the rest of the world", being a confirmation of the concentration of power by individual states, is at the same time an element of power diffusion from the perspective of the global international system. When we include non-state actors who are power brokers, the clear trend of change at the level of the global international system is the diffusion of power, which does not mean in any way the "democratisation" of this system. Apart from the relative increase in the strength of many countries, which is decisive, this is also due to an increase in the complexity and multifactor nature of the phenomenon of power in contemporary international relations, encompassing, among others, the economy, armed forces, technologies, demographic resources, cultural attractiveness, etc., but also to strategic thinking on how to use this potential in action in the face of the changing international environment (Pietraś, 2024).

Bearing in mind the above-mentioned trends of change at the level of the international system, a new model of capturing its polarity is proposed. One of the important premises for its structuring is – firstly – the assumption that for the structure, but also the functioning of the geopolitical space of the international system the "mere" surplus of the relative power of states ceases to be a decisive factor. "Asymmetrical powers" become a problem for stability – as the case of Russia demonstrates – meaning states endowed with lesser potential compared to many Western states but posing a significant threat to them. This means – without ignoring the importance of the potential – that the geopolitical strategy of applying this potential, including the strategic culture of a given state, is important and requires analysis. In this context, in addition to the structural approach, which is a derivative of the power concentration structure, a functional approach to polarity is proposed, identified as the strategy of the main players, which is to be referred to as geopolitical rationality.

Secondly, it was assumed that in conditions of simultaneous concentration and diffusion of force, the analysis of polarity only at the level of the global international system does not reflect the complexity of this phenomenon, especially when the importance of regional powers is growing. For this reason, it is proposed that the polarity of the international system be analysed as a two-level phenomenon, taking into account the level of the global system and global powers and the level of regional systems and their respective regional powers. This second level is useful in order to include the Global South states in the reflections on the current polarity of the international system. These assumptions are important for answering the question about the structure of the geopolitical space in which Poland and the Czech Republic function.

Geopolitical strategies of the main actors of the international system

The global international system has entered a period of change in the relative strength of global superpowers, but also of regional ones, as well as other states. This affects the structure of this system in the sense of "shifting" the centres of power concentration. Russia's aggression against Ukraine, accelerating this process, is seen as a turning point (White House, 2022) in the organisation, structure and functioning of the international order. There are several features of the aforementioned turning point (Pietraś, 2024), meaning that the geopolitical space of Poland and the Czech Republic is changing rapidly.

First of all, geopolitical rivalry is intensifying, accompanied by an increase in protectionism, economic fragmentation and curbing the importance of international institutions. However, this does not equate to the disappearance of international interdependencies, and common global problems such as climate change are on the rise. All of these factors create a previously unknown environment. On the one hand, it shows increasing geopolitical rivalry, and on the other hand, the persistence of interdependency and common problems, the solution to which requires cooperative behaviours. This is a previously unknown challenge for the rationality of geopolitical strategies of states.

Secondly, the states of liberal democracy are experiencing a specific "recurrence of history" – re-emergence of something that was considered a thing of the by-gone Cold War era. The perception of liberal democratic states by authoritarian/totalitarian states as ideological enemies (Stelzenmüller, 2023) "reinforced" by the formula of a civilisational enemy, familiar from the period of the bipolar order, has raised its head again. Vladimir Putin considered the West to be decadent, immoral, and self-corrupting (Kotkin, 2022).

Thirdly, the process of changing division lines at various levels of the social life organisation was set in motion. These lines run within states, but also at the level

of the international system with increasing conspicuousness. In the context of the latter, the division into democratic and authoritarian or totalitarian states is clear. The Global South stands out as an important geopolitical actor. There is no doubt that political values carry a geopolitical significance. They organize the space of social life and change the division lines. However, in the current conditions of geopolitical rivalry, an important question arises for Western countries about the strategy towards countries that selectively apply the principles of democracy, and to from which China or Russia do not require complying with these principles in their geopolitical strategy (Rhodes, 2024, pp. 8–23). This stems from the fact that the ties of alliances are shifting. Russia is seeking allies, for example, in Iran, Syria, North Korea and is receiving support from a "perplexed" China (Chatham House, 2023). The United States is intensively recruiting allies in the Indo-Pacific region (e.g. AUKUS, Quad), linking this region with the Middle East (I2U2), and surveying Africa with ever growing interest. Regional powers with aspirations for a global gameplay play a significant role. Amongst the new players with such aspirations one can see, e.g. Turkey, Saudi Arabia and Brazil. The attitude towards values "in the remaining part of the world" is becoming an important geopolitical dilemma for Western states.

Fourthly, summing up the elements of the analysis of the turning point in conditioning the structure of the international system, one should ask whether the Russian war in Ukraine can be seen as a conflict with consequences for the international order in Europe, or whether it is important for the global order. Could Russia's aggression against Ukraine create conditions for a new international order, as it took place after the end of World War II in 1945? (Feltman, 2023). Answers to these questions vary. In the case of the former, there should be no doubt that the war in Ukraine has consequences for the global international order, also changing the one in Europe, for example as a result of Finland and Sweden's membership in NATO. However, there is – with regard to the second question – no such distinctive global leader, general political climate and weakened opponents as was the case in 1945, or in 1989 or 1990 after the collapse of the bipolar order. The countries of Western and Central Europe must take greater responsibility for their own security (Logan & Shifrinson, 2024).

In the context of the identified trends of shifts in the global (but also regional) international system, the main elements of geopolitical strategies of Russia and China as states creating a challenge and an alternative to a rules-based order will be analysed. The geopolitical strategy of the United States as a state defending a rules-based order will be studied. The subject of a separate analysis will be the Global South, which, having been a background for geopolitical rivalry for the last few centuries or a space in which this rivalry took place, is now becoming an autonomous geopolitical player. These analyses are understood as a focus on the

structure of international order in functional terms, i.e. a focus on the geopolitical strategies of the actors listed and their geopolitical rationality in the changing international system.

Russia's geopolitical strategy

Russia is a country focused on rejecting a rules-based order with the dominant position of the United States and Western countries. It aspires to enjoy exclusivity of political, economic and cultural influence in the post-Soviet area. Such priorities – in general terms – determine the geopolitical rationality of this country. In order to reconstruct it, three elements will be analysed: 1) the asymmetry of Russia's power; 2) the awareness components of Russia's strategy; 3) the operational layer of Russia's strategy. It was recognised that, in addition to the historical past, they determine the current strategic culture of Russia, meaning – without going into its evolution – a state-specific way of thinking about the international environment, existing security threats and the way of responding to them (see Haglund, 2011, pp. 494–516; Snyder, 1977; Gray, 1999, pp. 49–69).

The asymmetry of Russia's potential, which is much smaller than what the United States or China hold, not to mention the comparison of Russia's resources with the states of the entire Euro-Atlantic area or European Union Member States. It was assumed that the asymmetry of Russia's potential significantly determines the manner of implementing the geopolitical strategy, e.g. the use of hybrid instruments. According to the World Bank data, the Russian GPD at the end of 2022 amounted to USD 2,266 billion, and at the end of 2023 to USD 2,021.4 billion, while the GDP of the United States was, USD 25,744.1 billion and USD 27,360.9 billion, respectively. This disproportion is increasing in favour of the United States. In 2022, it was 1:11.3, and in 2023 it increased to 1:13.5. According to SIPRI data, US military spending in 2023 amounted to USD 916 billion, which accounted for 37% of the military spending worldwide. In the case of Russia, these figures were USD 109 billion and 4.5% for 2023, respectively. For comparison, in the case of China it is USD 296 billion and 12% (SIPRI, 2024). Despite such disproportions, Russia is challenging the West and poses a geopolitical challenge.

Awareness elements in the context of geopolitical rationality and related strategic culture determine, above all, the way in which Russia and its decision makers perceive the world, as well as the way in which they think about it. First of all, Ukraine has a special cultural, historical and geopolitical significance for Russia. Kyiv was the first capital of Russia (or more specifically of its parent state called Ruthenia), which does not accept the separate statehood of Ukraine, or its culture and spiritual space (Lebow, 2022, p. 128; Reid, 2022).

Secondly, under the conditions of the autocratic political system of Russia and the historical traditions of the cult of personality, the argument about the "personalisation" of the formation of Russia's strategic culture by the figure of Vladimir Putin shaped in the environment of KGB intelligence officers seems justified. The view that the modern geopolitical rationality of Russia equates to Putin's rationality appears to be justified. The latter is perceived as a person utterly terrified by democracy, having a sense of historical mission, considering himself a continuator of the achievements of Lenin, Stalin and the tsars, especially Peter the Great, intended to make Russia a great superpower (Lebow, 2022; Curanovic, 2021, p. 72).

Thirdly, an important feature of the strategic culture of Russia and the rationality of actions towards the international environment is the inheritance of the imperial style of foreign policy regardless of the political system, be it tsarist, Soviet or Putin's. The imperialism of actions, thinking in terms of spheres of influence, striving to regain the ones lost after the Cold War and, to this end, questioning the established international order and thinking about the 19th-century concert of superpowers (Borowik, 2022, p. 41), belong to the elements of historical continuity in the foreign policy of Russia.

Fourthly, with regard to the "awareness layer" of the geopolitical rationality of Russia, it seems justified to argue that there is a relationship between the authoritarian political system, invoking the cult of personality and the ability to adequately assess reality. The personification of geopolitical rationality combined with the authoritarian political system, the specific circulation of information, creates the premises for incorrect assessments, such as those in the context of the aggression against Ukraine in 2022, underestimating the political cohesion of the West (Lebow, 2022, pp. 130–131).

The operational layer of the geopolitical rationality of Russia and the related strategic culture of this state concerns the effectiveness of its actions. In the conditions of aggression against Ukraine, it is possible to identify several of its elements. First of all, strength and fear occupy the central position in Russia's geopolitical strategy (Kimmage & Notte, 2023). Despite the norms of international law, including the principles of the Charter of the United Nations and the prohibition of the use of force (Karta Narodów Zjednoczonych), when attacking Ukraine, Russia referred to the original motive for the use of force in history, which is the restoration of the empire (Lebow, 2022, p. 113).

Secondly, it is possible to identify several features of the Russia-specific style of using force against the international environment, and not only military force. The first one is the way of thinking about power as a compound, complex phenomenon, resulting from the synergy of various elements, e.g. conventional, nuclear, hybrid ones, including disinformation, and targeted pressure of refugees (Seely, 2023). The second feature is flexibility and gradation of pressure in the use of force. The full-scale

war became next stage of exerting pressure on Ukraine after a hybrid war. The third feature of the use of force is not only to defeat the enemy, but also – and perhaps above all – to maintain the ability to influence and control specific states or regions.

The third element of Russia's geopolitical rationality in the operational layer and the related strategic culture is the global context of the actions taken, their impact on the global geopolitical space. When conducting the aggression against Ukraine, Russia, first of all, hopes to change the global international system, and more specifically, the balance of power to the disadvantage of the states upholding liberal democracy. Secondly, it aims to open a new chapter in the structure of its global ties, a peculiar restructuring of them, striving to strengthen relations with non-Western states of the Global South.

Geopolitical strategy of China

The geopolitical rationality of China, similarly to the case of Russia, is determined by the desire to change the liberal international order supported by Western states, especially the United States. However, there is a significant difference between China and Russia. The United States national security strategy of 2022 recognised that China is currently the only state with the potential and strategy of changing the international order and conditioning the future of the geopolitical space of liberal democracies (White House, 2022). Therefore, it is important to analyse this potential and the international position of China (static component) and its geopolitical rationality strategy (dynamic component).

Firstly, the international position of China and the factors which it is determined by are a dynamic process. This means that the relative strength of China compared to other superpowers has changed rapidly in its favour in recent decades, but in the last two years have witnessed a clear decline in its economic growth dynamics. According to World Bank data, in 2023, the GDP of China decreased slightly compared to 2022, falling from USD 17,881.8 billion in 2022 to USD 17,794.8 billion in 2023. It is unclear to what extent this is the result of the draconian "zero COVID" policy, and to what degree a result of structural conditions and overproduction resulting from them (Zoe Liu, 2024). Secondly, the factors underlying China's changing potential seem to coincide with the factors that currently, as well as in the future, are and will be decisive for the relative change in the concentration of power in the global international system. These are the economy, technology and demographic situation. An opinion is formulated according to which the change in the relative geopolitical position of China is taking place as a result of geo-economic change combined with demographic potential (Golden, 2019, pp. 14–20). China is also boosting its military strength.

China's share in the global GDP has increased significantly. In 1980, at the beginning of the economic reforms initiated in 1978, it amounted to 1.6%. In 2014, it was 13.25%, in 2018 – 16.27%, and in 2022 – 17.86%. China has reduced its distance to the United States, whose share in the global GDP in 1980 was 21.3%, in 2014 – 22.20%, in 2018 – 24.04%, and in 2022 – 25.32%. The demographic potential of China in 2021 was 18.02% of the global population and was relatively in decline, amounting to 18.88% in 2014. In the case of the United States, in 2021, the share of the population in the global demographic potential was 4.24% and was also relatively decreasing, amounting to 4.38% in 2014. China's military expenditure has increased significantly in recent years. In absolute terms, it amounted to USD 196.5 billion in 2020, USD 258 billion in 2015, and USD 296 billion in 2023. US military expenditure was significantly higher, amounting to USD 633.8 billion in 2015, USD 778.4 billion in 2020, and USD 916 billion in 2023 (Global Economy, n.d.; SIPRI, 2024).

The analysis of China's power components clearly demonstrates that their relative power, i.e. the resources with which they can change the international system, is increasing, regardless of the limitations that have appeared in recent years. An additional motivation is China's desire to regain its hegemonic position still held at the beginning of the 19th century. The loss of this status is still accompanied by a sense of historical, humiliating injury. In 1820, China generated more than 30% of the world's GDP, with Europe and the United States combining to generate less than 25% during that period. In 1949, China generated less than 5% of the global GDP, and the United States and Western Europe achieved more than 50% (Golden, 2021).

The increase in China's relative power is accompanied by the strategy of striving to change the liberal international order to an alternative one, consistent with China's preferences. In this context, the former Foreign Minister of China, Qian Qichen, formulated the view that diplomacy is an extension of the domestic policy of the state (Callick, 2021). One may conclude from this that the feature of China's geopolitical strategy is to be the comprehensiveness and cohesion of an international model of social life, which is an alternative model to liberal democracy and the liberal order, both at the level of the interior of the state and at the level of the international system. An opinion has been formulated, that under the leadership of Xi Jinping, China became more authoritarian internally and more inclined to use force at the level of the international system (Chen Weiss, 2022, p. 42). These efforts are captured by the symbolic formulas of the "Chinese dream" and the "Chinese model".

An international order alternative to the liberal international one is implemented by China as part of four programs. The oldest one is the Belt and Road Initiative launched in 2013. It focuses on supporting the development of the infrastructure of emerging or middle-income economies, while serving to solve the issue of excess production of the Chinese economy. In 2021, the Global Development Initiative was launched. The category of development holds particular significance

for China's geopolitical thinking, which aspires to be a global leader in development processes. Development seems to be an alternative to the Western preference for human rights. The third program is Global Security Initiative launched in 2022. It is supposed to promote "Chinese wisdom" about "Chinese solutions", rejecting unilateralism and the policy of military blocs. In 2023, the Global Civilisation Initiative was launched, emphasizing the diversity of civilisational models and highlighting the absence of a single, universal model of human rights protection (Economy, 2024, p. 10). These initiatives mean that China is not a country interested in retaining the existing global geopolitical *status quo*, but rather in changing it. It is a "revisionist" superpower, seeking to reduce the importance of the liberal international order and has a strategy to do so, including the preference for the use of force.

China's geopolitical strategy aimed at an alternative change and the preferred way of its implementation are distinguished by several features. First of all, economic penetration is an important element of this strategy, identified with the Belt and Road Initiative. More than 150 countries have joined this initiative, and it marks a change in the way power is projected through a dispersed, infiltrating action of the economic sphere inside various states, creating "bridgeheads" of political influence. The "Belt and Road" program, therefore, holds a geopolitical importance. It serves to expand China's economic influence, and through it, its political influence (Loh, 2021, p. 167 ff).

Secondly, an important element of China's geopolitical strategy is to increase its military capabilities, both conventional and nuclear ones, as well as its capabilities to operate in space and cyberspace. It is expanding naval forces, including the number of aircraft carriers and naval bases; probably to protect supply and export routes.

Thirdly, an important element of China's geopolitical strategy is the support of the multipolar international system and, among others, development of cooperation with the states of the Global South and encouraging cooperation between these states. The multipolar system is intended to replace the hegemonic position of the West, as well as of any region in the emerging international order (Golden, 2021).

Fourthly, an important component of China's geopolitical strategy is the ability to learn about the changing world associated with the pragmatism of turning this knowledge into the implementation of defined interests. China has become the largest beneficiary of globalisation processes. It has developed a strategy of "playing" with interdependencies as a feature of these processes, striving to "decouple" elements of dependence on the West and to exploit the sensitivity and susceptibility of Western states to economic ties with China. It has learned to take advantage of the geopolitical errors of the West.

Geopolitical strategy of the United States

Despite the relative surplus of the United States' power after the period of its unipolar hegemony, the world is entering the "post-American period". Fareed Zakaria wrote about it at the end of the first decade of the 21st century (2008). A significant challenge for the United States – also bearing in mind the limited predictability of the domestic political scene – is the geopolitical strategy of leadership in the world of post-American hegemony. An opinion is formulated that Russia's aggression against Ukraine in 2022 and China's growing geopolitical assertiveness have created an opportunity for a "geostrategic awakening" of the United States (Sullivan, 2023). One of its manifestations is the role of the leader for the states supporting Ukraine after Russia's aggression, but also a kind of diplomatic offensive in various regions of the world. These actions appear to reflect the new geopolitical strategy of the United States, an important feature of which is a change in the approach to the understanding and use of force in international relations. It was recognized that this strategy requires to be founded on economic potential, technological innovation, and the effectiveness of application in the international environment requires cooperation with other countries and its institutionalisation, including – after Donald Trump's presidency – "repair" of relations with allies (White House, 2022). The regional geopolitical priorities of the United States have also been clearly defined. Attention is drawn to the complexity of the approach to international cooperation, combining its bilateral and multilateral forms, various areas such as the economy, diplomatic relations, armed forces, new technologies, etc. and various spatial scopes identified with geographical regions, but also intercontinental operations. Multilateralism – after the period of *America First policy* – is being rebuilt in the foreign policy of the United States.

Russia's aggression against Ukraine has not changed the United States' priority interest taken in the Indo-Pacific region and strengthening alliance ties in Asia. This shows – especially in the context of China or Russia – a relatively wide range of diplomatic possibilities in terms of acquiring cooperation partners. Among the forms of multilateral dialogue one can find AUKUS (USA, Australia, United Kingdom). This structure was created in 2021 mainly to coordinate defence industries. It complements the QUAD dialogue resumed in 2017 (USA, Australia, India, Japan) focused on non-military areas of cooperation such as technology, climate, health care and marine environment. At the economic level, in May 2022, the United States initiated cooperation of 14 Indo-Pacific countries (Australia, Brunei Darussalam, Fiji, India, Indonesia, Japan, South Korea, Malaysia, New Zealand, the Philippines, Singapore, the USA, Thailand and Vietnam) under the "Indo-Pacific Economic Framework for Prosperity". The purpose is to contribute to cooperation, stability and development of the regions, and these countries produce more than 40% of the world's GDP (USTR, n.d.). The trilateral cooperation of the United States, Japan and South Korea on security

issues with a focus on deterring North Korea is being consolidated. A summit of these states was held at Camp David in August 2023 (Pietraś, 2024). India is a clear priority in bilateral relations. The Philippines and Vietnam are important.

While making the Indo-Pacific region a geopolitical priority, the United States is not neglecting partners in other geographical regions by initiating regional but also transcontinental multilateral structures. As regards regional structures, in addition to the obvious presence in Europe, for example, within NATO, multilateral ties are being developed with African and South American countries. In December 2022, the first US-Africa Leaders Summit was organized since 2014 (U.S. Department of State, 2024a), proposing a framework agreement for a free trade zone. In relation to South America, the USA initiated the Americas Partnership for Economic Prosperity in 2022 in order to reduce development disparities, accelerate regional integration and strengthen democracy (U.S. Department of State, 2024b). Regarding transcontinental structures, in July 2022 the United States initiated cooperation with India, Israel and the United Arab Emirates referred to as I2U2. Together with 31 states from North and South Americas, Africa and Europe, the Partnership for Atlantic Cooperation was established in September 2023. Cooperation on cybersecurity was initiated with the participation of 47 states (Sullivan, 2023).

After the experience of the strategy pursued by Donald Trump's administration, the actions of the Joe Biden administration in the international system, which is characterized by the growing rivalry of superpowers, are a consciously implemented geopolitical turnaround. There is an apparent awareness of the importance of strength, relative power and its complexity in connection with the ability to cooperate, build a network of partners on a global scale and preserve international leadership as well as its style of implementation. An image is being built of a responsible leader who is involved in solving common problems of humanity such as climate change, environmental problems and at the same time avoidance of military interventions. Foreign interventions are not excluded in the new geopolitical strategy, but without a long-term commitment binding military and economic forces. Preparing for a new era of strategic rivalry, deterring and responding to the aggression of other superpowers are a priority (Sullivan, 2023). There are issues related to the lack of a cohesive strategy towards China and even more so to the response to actions taken by China, which has an alternative international order strategy.

Global South as a geostrategic space

The term "Global South" emerged in 1969. Over the years, its understanding also has changed in the conditions of the changing international system. The main criterion for delineating the division line between the Global North and the Global

South is the level of development. It is a group of highly diverse states, and it is difficult to talk about their cohesion. Nevertheless, one can formulate a view arguing that one of the most significant changes after Russia's aggression against Ukraine, one with long-term effects, is the geopolitical autonomy of the Global South, which can be seen as a space for the emergence of regional powers and regional level of polarity. On the one hand, it is becoming a specific geopolitical player of low cohesion, but on the other hand, it is becoming a geopolitical space. In both senses, the Global South has ceased to be a mere background for the earlier rivalry for hegemony between superpowers.

The response of the Global South to Russia's aggression against Ukraine has contributed to an accelerated realisation on the part of the global superpowers that geopolitical value lies in the space beyond their borders. In this context, an opinion is formulated according to which the Global South exists more as a geopolitical fact than an organized group, aware of clearly formulated and common priorities (Shidore, 2023). This means that the geopolitical space of the global international system is determined not only by the relations between the United States, China and Russia, but also by the actions of medium-sized and smaller states (Shidore, 2023). This creates the premises for the egress of the Global South from many decades of marginalisation conditioned by the international system polarity. The bipolar system, and after its collapse, the unipolar dominance of the United States, were not conductive to the strategic autonomy of the Global South. Nowadays, the cooperation of the Southern states gradually balances the earlier asymmetrical relations of the North and the South analysed in terms of central and peripheral systems (Galtung, 1971, p. 89).

One of the ways in which the geopolitical autonomy of the Global South manifests itself is through applying the power of refusal, a behaviour other than the realised expectations of the superpowers. This is confirmed by the voting on the issue of Russia's aggression against Ukraine in the UN General Assembly (Resolution adopted by…). Out of 193 member states, 141 voted in favour of the resolution, 35 abstained, 5 were against and 12 did not participate in the vote.

Does the result of the vote mean that some of the states of the Global South are against the international rules-based order? Many of them have a pragmatic approach to this order. The critical attitude and disappointment towards the states of the North, and more specifically the West, is definitely significant. It is conditioned by the experiences of the colonial past, the lack of expected and promised support in solving the global problems of climate change or debt. The COVID-19 pandemic exacerbated this disappointment. The propensity of the United States to intervene militarily is met with critical assessment. As a consequence, in the context of Russia's aggression against Ukraine, paradoxically, many states of the Global South harbour resentment not towards the aggressor, but towards Western states supporting Ukraine as a victim of aggression. Many states of the Global South are

convinced that the rules-based order has not served their interests in the best way, having protected the *status quo*, in which the Western superpowers – depending on the historical moment – dominated them. Hence, the behaviour of many countries of the Global South is not conditioned by fidelity to norms and values, but by the pragmatism of interests (Miliband, 2023).

In summary, the global geopolitical space of Poland and the Czech Republic is undergoing dynamic changes. These changes were accelerated by Russia's aggression against Ukraine, contributing to the intensification of geopolitical rivalries. In the context of accelerating the changes in the global international system, the polarity of this system was selected as an important subject of analysis, proposing a new way of thinking about it. Firstly, it was found that in the current tradition of studying the polarity of international systems in the discipline of "international relations", the focus was on the static and single-level perception of polarity as the result of the relative surplus of the power of one, two or more states at the level of the global international system. Secondly, a dynamic and two-level approach was proposed. Its dynamic nature stems from the focus on the geopolitical strategy of a power with strength resources, and, thus, on what it does with these resources. It is a two-level approach since the level of the globe as a whole and of the group of global superpowers was taken into account, as well as the level of regions and regional powers, especially from the Global South. In the context of such research assumptions, the geopolitical strategies of Russia, China, the United States and the Global South were subjected to synthetic analysis. They create a space in which Poland and the Czech Republic function.

References

Bailes, A. (2005). Introduction. Global security governance: A world of change and challenge. In *SIPRI Yearbook 2005, Armaments, Disarmament and International Security*. Oxford University Press.

Borowik, B. (2022). *Kultura konfliktu. Polityka Federacji Rosyjskiej wobec Ukrainy i Zachodu na łamach „Newsweeka Polska" i „Polityki" (2013–2015)*. Wyd. UMCS.

Callick, R. (2021). *Xi Jinping lanches a New Era for China and the World*. https://revistaidees.cat/en/xi-jinping-launches-a-new-era-for-china-and-the-world/

Chatham House. (2023). *Seven ways Russia's war on Ukraine has changed the world*. https://www.chathamhouse.org/2023/02/seven-ways-russias-war-ukraine-has-changed-world

Chen Weiss, J. (2022). The China trap. U.S. foreign policy and the perilous logic of zero-sum competition. *Foreign Affairs*, *5*(101), 42.

Curanovic, A. (2021). *The Sense of Mission in Russian Foreign Policy. Destined for Greatness!* Routledge.

Deutsch, K., & Singer, D. (1964). Multipolar power system and international stability. *World Politics*, *3*(16).

Economy, E. (2024). China's alternative order. And what America should learn from it. *Foreign Affairs*, *3*(103).

Feltman, J. (2023). *War, peace, and the international system after Ukraine*. https://www.brookings.edu/articles/war-peace-and-the-international-system-after-ukraine

Galtung, J. (1971). A structural theory of imperialism. *Journal of Peace Research*, *2*(8), 89.

Gałganek, A. (1992). *Zmiana w globalnym systemie międzynarodowym. Supercykle i wojna hegemoniczna*. Wyd. UAM.

Global Economy. (n.d.). https://www.theglobaleconomy.com/

Golden, S. (2019). New paradigms for the New Silk Road. In C.A. Mendes (Ed.), *China's New Silk Road. An Emerging World Order* (pp. 14–20). Routledge.

Golden, S. (2021). *China's role in the construction of a new geopolitics in Asia and the world*, https://revistaidees.cat/en/chinas-role-in-the-construction-of-a-new-geopolitics-in-asia-and-the-world/

Gray, C.S. (1999). Strategic culture as context: The first generation of theory strikes back. *Review of International Studies*, *25*, 49–69.

Haass, R. (2008). The age of nonpolarity. What will follow U.S. dominance. *Foreign Affairs*, *87*(3).

Haglund, D. (2011). 'Let's call the whole thing off'? Security culture as strategic culture. *Contemporary Security Policy*, *3*(32), 494–516.

Karta Narodów Zjednoczonych. https://www.bb.po.gov.pl/images/Prawa/PNZ/KNZ.pdf

Keohane, R. (1984). *After Hegemony. Cooperation and Discord in the World Political Economy*. Princeton University Press.

Kimmage, M., & Notte, H. (2023, September 1). How Russia globalized the war in Ukraine. The Kremlin's pressure-point strategy to undermine the West. *Foreign Affairs*.

Kondrakiewicz, D. (1999). *Systemy równowagi sił w stosunkach międzynarodowych*. WSPiA.

Kotkin, S. (2022, May 31). *What Putin Got Wrong About Ukraine, Russia, and the West*. Interview by Daniel Kurtz-Phelan, Foreign Affairs.

Krzyżanowska-Skowronek, I. (2024). System międzynarodowy jako przedmiot badań w stosunkach międzynarodowych. In E. Haliżak (Ed.), *Encyklopedia stosunków międzynarodowych* (p. 97). Scholar.

Lebow, R. (2022). International relations theory and the Ukrainian war. *Analyse & Kritik*, *44*(1).

Logan, J., & Shifrinson, J. (2024, August 9). A post-American Europe. It's time for Washington to Europeanize NATO and give up responsibility for the continent's security. *Foreign Affairs*.

Loh, D.M.H. (2021). The 'Chinese Dream' and the 'Belt and Road Initiative': Narratives, practices, and sub-state actors. *International Relations of the Asia-Pacific*, *21*(2).

Mearsheimer, J. (1990). Back to the future: Instability in Europe after the Cold War. *International Security*, *15*(1), 5–56.

Mearsheimer, J.(2014). *The Tragedy of Great Power Politics*. W.W. Norton & Company.

Miliband, D. (2023, May/June). The world beyond Ukraine The survival of the West and the demands of the rest. *Foreign Affairs*.

Modelski, G. (1987). *Long Cycles in World Politics*. Palgrave Macmillan.

Pietraś, M. (2024). Globalna przestrzeń partnerstwa strategicznego Polski i Ukrainy. In M. Pietraś, W. Baluk, & H. Perepełycia (Eds.), *Partnerstwo strategiczne Polski i Ukrainy w warunkach zmiany systemu międzynarodowego. Punkt widzenia Polski i Ukrainy* (pp. 27–60). Wyd. UMCS.

Pietraś, M. (2021). Pozimnowojenny ład międzynarodowy. In M. Pietraś (Ed.), *Międzynarodowe stosunki polityczne* (p. 412). Wyd. UMCS.

Reid, A. (2022). Putin's war on history: The thousand year struggle over Ukraine. *Foreign Affairs*.

Resolution adopted by the General Assembly on 2 March 2022. ES-11/1. Aggression against Ukraine, A/RES/ES-11/1, 18 March 2022.

Rhodes, R. (2024). A foreign policy for the world as it is. Biden and the search for a new American strategy. *Foreign Affairs*, *103*(4), 8–23.

Rotfeld, A.D. (2008). Dokąd zmierza świat? Determinanty zmian w systemie międzynarodowym. In A.D. Rotfeld (Ed.), *Dokąd zmierza świat?* (p. 11). PISM.

Seely, S. (2023, November/December). The Russian way of war. Moscow wants to weaken NATO in Ukraine, not just win battles. *Foreign Affairs*.

Shidore, S. (2023, August 31). The return of the Global South. Realism not moralism drive a new critique of western power. *Foreign Affairs*.

Singer, D. (1961). The level-of-analysis problem in international relations. World Politics, *14*(1), 77–92

SIPRI. (2024). https://www.sipri.org/sites/default/files/2024-04/2404_fs_milex_2023.pdf

Smoleń, K. (2020). *Geostrategiczne położenie Turcji w XXI wieku*. Wyd. UMCS.

Snyder, J. (1977). *The Soviet Strategic Culture: Implications for Nuclear Options*. RAND.

Stelzenmüller, C. (2023). *The Return of the Enemy: Putin's war on Ukraine and cognitive blockage in Western security policy.* https://www.brookings.edu/articles/the-return-of--the-enemy

Sullivan, J. (2023). The sources of the America power. A foreign policy for a changed world. *Foreign Affairs*, *102*(6).

U.S. Department of State. (2024a). https://www.state.gov/africasummit/

U.S. Department of State. (2024b). https://www.state.gov/americas-partnership-for -economic-prosperity/

USTR. (n.d.). https://ustr.gov/trade-agreements/agreements-under-negotiation/indo-pacific -economic-framework-prosperity-ipef

Waltz, K. (1964). Stability of bipolar world. *Deadalus*, *93*(3).

Waltz, K. (1979). *Theory of International Politics*. McGraw-Hill.

White House. (2022, October). *National Security Strategy*. https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy -10.2022.pdf

Wohlforth, W. (1999). The stability of a unipolar world. *International Security*, *24*(1), 5–41.
Zakaria, F. (2008). *The Post-American World*. W.W. Norton & Company.
Zoe Liu, Z. (2024). China's real economic crisis. Why Beijing won't give up on a failing model. *Foreign Affairs*, *103*(5).

EWELINA KANCIK-KOŁTUN

MARIA CURIE-SKŁODOWSKA UNIVERSITY, LUBLIN

Diplomacy of Security – Outline of the Issues

Abstract: The high dynamics in international relations, the growth of threats in the field of security, have led to a significant decrease in the level of global and regional security. Tense situations require advanced and multi-level diplomatic actions for security, and security diplomacy is currently becoming one of the main trends in foreign policy. The article is an attempt to define the concept diplomacy of security and is a contribution to further discussion on the issue, in particular in the context of the importance of security in international relations. The article presents the issue of diplomacy in the context of realizing national and international interests in the area of security, taking into account the reason for the actions taken, which is the war in Ukraine and the implementation diplomacy of security activities by the Polish state.

Keywords: diplomacy of security; Poland; Russia's war in Ukraine

Introduction

The military conflict in Europe, namely Russia's war in Ukraine, has caused the destruction of the generally understood infrastructure, including critical infrastructure and has undoubtedly contributed to the cessation of economic activity, investments and the normal functioning of Ukrainian citizens. The war caused many casualties among the Ukrainian civilian population, but also a wave of migration from Ukraine, in particular to neighboring countries. Europe is facing a major challenge and threat to its security. The outbreak of the full-scale Russia-Ukraine conflict reminded us that the war in Europe has not disappeared and that the continent has only temporarily remained free from armed conflict. Diplomacy plays a significant role in ensuring security both at the regional and global levels. The areas of diplomatic activity are constantly expanding, going beyond the political plane, distinguishing them into scientific, trade, economic and defense diplomacy. "The catalogue of international issues that are of interest to diplomacy has significantly expanded, including problems related to human rights, refugees or humanitarian interventions, ecological issues, financial flows, development issues and intellectual property matters" (Drab, 2019, p. 83).

Security diplomacy and all its activities from the point of view of Russia's ongoing war in Ukraine are becoming very important, not only by the countries participating in the conflict, but also by the neighboring and transit countries that provide the hinterland for Ukraine. The war in Europe has significantly affected the sense of security of citizens in individual European countries. In countries bordering the area of armed conflict, the sense of security has significantly decreased.

The sense of security accompanies a person at every stage of life from fetal life to death, with the need for security intensifying in new, sudden and existence-threatening situations (Sygit, 2017, pp. 300–301) and one of such threats is Russia's war in Ukraine. The aim of the article is to analyze the impact of the war in Ukraine on security diplomacy. The article is an attempt to define the concept of security diplomacy and is a contribution to further discussion on the issue, in particular in the context of the importance of security in international relations. The article presents issues in the field of diplomacy in the context of realizing national and international interests in the area of security, taking into account the reason for the actions taken, which is the war in Ukraine, and the implementation of security diplomacy activities by the Polish state.

The war in Ukraine and security

There are many definitions of security, and, thus, they concern many areas of security: social, political, cultural, ecological, military, cyber, energy, or climate. Security is often perceived as a value through the prism of peace, life or health, which occupy the most important place of all known values in the European cultural sphere (Kancik-Kołtun, 2021). A very important condition for security is the occurrence of a threat. Thus, new categories of security are created. We can divide security into four areas, taking into account threats: global security, international security, regional security and national security.

Ensuring internal and external security is extremely important from the point of view of the functioning and continuity of each state. The period of peace and stability in Central and Eastern Europe after the political transformation was undoubtedly conditioned by the accession of the countries belonging to the former communist bloc to the European Union and NATO. Membership in the indicated international organizations changed relations between states, strengthening cooperation in almost every area of the functioning of states and the lives of citizens. In order to maintain international security, actions were taken related to the peaceful resolution of disputes. With the end of the Cold War, the number of states became increasingly open, and security became something obvious in a globalizing world in which we dealt with the dissemination of democracy, the free flow of trade, services, technology,

investments and people. Connections related to the dependence of transport, IT, service and energy infrastructure were gaining increasing importance in Europe. Security is a basic condition for the economic and political development of states. The escalation of the aggression of the Russian Federation against Ukraine, committed on February 24, 2022, a war that had been ongoing since February 2014, was a very big challenge for European countries, and, at the same time, a threat to security, peace and stability in Europe. Before the start of a full-scale war, Russia had previously demanded an end to further NATO enlargement and a reduction of the military potential of the North Atlantic Alliance in Central and Eastern Europe to the state before 1997. Russia's main goal was undoubtedly to prevent Ukraine from integrating with the EU and NATO. Ukraine's aspirations to change the system, an attempt to join the EU and NATO and "the possible success of Ukraine's democratic transformation, its adoption of European standards and political and economic integration with Western structures, the Kremlin perceived and perceives as a serious threat not only to the security of the Russian Federation, but also to the stability of the authoritarian Putin regime" (Menkiszak, 2021, p. 1). The war in Ukraine is therefore a fight for democracy against an authoritarian regime, hence Western countries should help Ukraine, because its fall will be the fall of democracy and may have an impact on triggering World War III, in the longer or shorter term (Kancik-Kołtun, 2023, p. 74). The countries and citizens of the former USSR are particularly at risk, and, thus, those directly bordering Ukraine and Russia, such as Poland, Slovakia, Romania or the Baltic states. Specific decisions developed and established at the diplomatic level, actually translate into authentic actions. It would be worth paying attention to the actions of aid packages for Ukraine or sanction packages imposed on Russia. Ukraine connects Asia and Europe, and is therefore very important geopolitically for Russia, because without Ukraine, Russia will not be a global empire. In turn, the United States cannot allow Ukraine to once again find itself in the Russian zone of influence, because it would infect their hegemony of influence in Europe. It is worth noting that Russia is aware that the expansion of NATO eastwards to Russia's borders will increase the US influence in Europe and, thus, reduce Russia's. Thus, in the case of the war in Ukraine, we are dealing with a rivalry of powers on a global scale and the distribution of zones of influence between Russia and the United States, with the outcome of the Russian-Ukrainian conflict creating a European security architecture. The broader geopolitical contact presented by Štefan Danics shows that Ukraine is guided primarily by its national interests in the war, with the interests of not only Russia as a land power, but also the United States as a naval power visible in a transaction about a zero-sum geopolitical game, which is dangerous for Ukraine, because both Russia and the USA are trying to draw Ukraine into their zone of powerful influence, which threatens its territorial integrity, but also its independence (Danics, 2023, p. 37).

Diplomacy and its types

According to Marian Wilk, "the process of economic, political and cultural globalization as well as new threats to international order and security in the form of armed conflicts and pathologies such as terrorism, illegal migration or drugs, pose new challenges to the foreign service of each state" (Wilk, 2002, p. 5). Krzysztof Domeracki stated that "the contemporary world and international relations are characterized by great dynamics, and thus the rapid technological (civilizational) development, which is a product of globalization, determines the growth of political activity of societies and significantly affects the relations between individual security entities in international relations" (Domeracki, 2019). In this localized world, diplomatic activities seem to be extremely real.

The concept of the definition of diplomacy is very broad, and, thus, it concerns many areas, such as: politics, science, culture, ecology, economics and defense, and therefore it can be understood and defined in many ways, as evidenced by the rich literature on the subject. Diplomacy is one of the mechanisms in international relations and is often identified with foreign policy. As Beata Surmacz states, the concept of diplomacy is explained in two perspectives,

> in the macro perspective, where diplomacy means a global process of communication between actors, in which a solution to a conflict is sought through negotiations while avoiding war, and in the micro perspective understood as the behavior of actors in international relations, where diplomacy is an instrument of foreign policy or a mechanism of representation, communication and negotiation through which international actors pursue their own interests. (Surmacz, 2013, pp. 7–8)

In turn, Ziemowit J. Pietraś defines diplomacy as "official activity of the state directed outward, implemented by state bodies and aimed at achieving the assumptions of foreign policy through conducting negotiations and concluding international agreements" (Pietraś, 1978, p. 14). Surmacz lists four basic functions of diplomacy:

1) "It must define its goals, taking into account the availability of actual and potential power necessary to achieve it.

2) It must assess the goals of other states and the power that is actually and potentially available to achieve them.

3) It must determine to what extent these goals can be stimulated.

4) It must use appropriate means to achieve its goals" (Surmacz, 2015, p. 41).

At present, there have been changes in the international environment, which are called in the literature "the late Westphalian order" and are characterized by the impact of globalization on international relations, in which there have been changes in the functioning of diplomacy at the European level due to the blurring of state

borders in the international space and undoubtedly the development of new communication and information technologies, especially the Internet.

Along with the phenomenon of globalization, new categories of international problems have also emerged, in the field of human rights, humanitarian law, and migration and refugee law. During the evolution of the subject scope of diplomacy, we are dealing with, among others: political diplomacy, cultural diplomacy, economic diplomacy, ecological diplomacy, climate diplomacy, migration diplomacy, scientific diplomacy, historical diplomacy and defense diplomacy. Defense diplomacy is therefore located in the scope of international relations, in foreign policy. As Lech Drab notes, "defense diplomacy, as one of the most important instruments of foreign security policy, covers many areas in which it performs tasks related to ensuring the security of the state" (Drab, 2019, p. 84). The main areas of Crown diplomacy should be considered: humanitarian aid, military aid, military education and training, arms control and disarmament, defense industry, missions and operations, historical cooperation, intelligence cooperation, military exercises, legal and legislative cooperation, cooperation in international organizations, bilateral and multilateral cooperation (Drab, 2019, p. 85). It seems that a more broad term is the term "security diplomacy", which includes both defense diplomacy and military diplomacy. Security diplomacy should be understood as an instrument of conducting foreign policy focusing on security areas, and, thus, it is a process and the entire system of communication of state governments in the international arena in order to pursue national interests, by changing behaviors, positions, negotiations and developing common solutions by the international community in security issues. Security diplomacy is implemented at three levels, which are:

1) Actions of political actors and their involvement in shaping international security and peace, such as: presidents, prime ministers, chancellors, monarchs, ministers.

2) Actions of military entities and their involvement in shaping international security and peace.

3) Actions of non-governmental organizations and their involvement in shaping international security and peace.

Security diplomacy can be conducted in various areas (global, international, regional, national) and security fields (military, ecological, economic, political, physical, social, IT, cultural, health, energy) and many others, divided into further categories of given fields.

The importance of security diplomacy in Poland

Since the beginning of the regular war between the Russian Federation and Ukraine, attention should be paid to the diplomatic efforts of the Polish government,

namely the growing importance of security diplomacy in diplomatic activities. Undoubtedly, the war between Russia and Ukraine has to some extent united politicians of different political parties in the matter of a common direction of actions in order to maintain the security of Poland and the region. Since the beginning of the sub-Nazi war in Ukraine, diplomatic activities have been and are taking place at various levels of international politics. It is necessary to note the activities of President Andrzej Duda's security diplomacy. Since the beginning of the escalation of the war in recent years, President Duda has been conducting his international talks and meetings, which have focused on the subject of security in the region, including in the context of the situation in Ukraine. Figure 1 presents in detail the diplomatic activities, talks and meetings with specific foreign politicians (presidents, heads of government, representatives of the UN, NATO, EU) of various countries conducted by the President of the Republic of Poland. Numerous activities in the field of security diplomacy were also undertaken by the Prime Minister, but also by the Ministries of Foreign Affairs.

Figure 1. Security diplomacy

Source: Oficjalna strona Prezydenta Rzeczypospolitej Polskiej. https://www.prezydent.pl/aktualnosci/wydarzenia/dyplomacja-bezpieczenstwa-plen,48626

Analyzing the last exposé of the Minister of Foreign Affairs Radosław Sikorski from April 2024, we find information that the tasks of Polish foreign policy will be focused on ensuring the security of the state understood as the certainty of survival and development. The Minister stated that "diplomacy is the first line of defense of the Republic of Poland". Sikorski touched on many topics that were important to Poland. The exposé mentioned, among others, relations with Ukraine, the European Union, Russia, Belarus, the USA, Germany, China, Israel, as well as economic issues. Throughout the exposé, the Minister devoted much attention to security issues, thus, emphasizing several times the importance of diplomacy in matters of ensuring security. The Minister stated that "Poland is already facing various forms of hybrid aggression, such as disinformation, cyberattacks, the use of energy dependencies, or the instrumentalization of migration pressure". The Minister considered Poland's security to be the first priority of foreign policy:

> Poland is safe. The Polish *raison d'état* requires us to develop our own defence resources and the ability to deter aggression, shared with our allies. It also requires us to provide Ukraine with maximum military and political support. It is in Poland's obvious interest to keep the aggressor as far away from our borders as possible. Therefore, sovereign Ukraine must win this war, and peaceful international order in Europe must be restored. The foundation of Poland's security remains the transatlantic Alliance with the leading role of the United States. Our goal is to maintain and strengthen American involvement in Europe, and, at the same time, strengthen the European pillar of the Alliance, in the spirit of strategic harmony of NATO and European Union activities. (Exposé of the Minister of Foreign Affairs Radosław Sikorski)

This is undoubtedly an important topic, because the sense of security of a given citizen is a multidimensional phenomenon, and the perception of threat by citizens depends on many conditions, such as the geopolitical location of the Polish state, socio-cultural and economic conditions. In the further part of the exposé, in his long speech, Minister Sikorski referred to improving Poland's security by taking such actions as:

– "expansion of the military potential of the North Atlantic Alliance,

– guarantees of new defense plans of the Alliance, covering the eastern flank of NATO,

– strengthening the transatlantic community as one of the priorities of the Polish Presidency of the Council of the European Union,

– effective coordination in three areas: assistance to Ukraine, improvement of security and sanctions on Russia and Belarus,

– development of military cooperation and continued presence of American troops in our Republic of Poland,

– improving the effectiveness of defense cooperation of Europeans,

– development of the defense industry and inclusion of Polish enterprises in international supply networks,

– creation of European rapid reaction forces,

– the Three Seas Initiative will be successful to the extent that it contributes to the development of the transport, energy and digital infrastructure of the region stretching from Estonia to Greece" (Exposé…).

The indicated examples of actions of representatives of the Polish government show how important security diplomacy is in the current geopolitical situation, which is becoming one of the main diplomatic areas due to the military conflict in Ukraine, which borders Poland. The tense situation in the region requires advanced and multi-level diplomatic actions for security.

Conclusions

We are currently dealing with a very dynamic situation in the matter of security in the global and regional aspect, and it is precisely diplomacy that should effectively implement national interests, through changing behaviors, positions and negotiations, along with the development of common solutions by the international community in matters of security and peace in the global and regional area. It should be noted that diplomacy is constantly taking action to find new solutions to conflicts, and the effectiveness of its actions in maintaining the state of security depends on the political will, cooperation of entities of international law and their determination (Hyb, 2016, p. 113).

It is worth noting that predictability in the context of security is currently decreasing, which is conditioned by changing trends and factors. The sources of threats are of a different nature – state, non-state and supranational, and the trends are asymmetric – thus, strengthening the potential of threats that will cause weakness, conflicts and tensions in different regions of the world. Interestingly, one can get the impression that threats to internal and external security are delving into each other, amending the differences. The combination of all these circumstances and dependencies means that they have a very large impact on security. Therefore, a comprehensive approach to the need to ensure security is needed, combining diplomatic, military, civil, economic and legal instruments and measures to prevent infections or mitigate their effects. The problem is also the readiness to respond quickly and effectively to sudden threats. Andrzej Szeptycki notes that the countries of Eastern Europe and the South Caucasus (Ukraine, Belarus, Moldova, Georgia, Azerbaijan, Armenia) are fragile states, where their development and guarantees of security and protection of human rights are lacking, where institutions are ineffective and corrupt, and society does not create a real community; and in addition, it is very likely that armed conflicts will break out

there in the near future (Szeptycki, 2021, p. 293). Undoubtedly, this zone of powerlessness will be the source of security threats in the form of rapid border changes, terrorism, extremism, organized crime, illegal migration, or military/army conflict. It is therefore worth noting that security and stability in the areas neighboring Europe are decreasing and a direct threat to the territory of some NATO and EU member states can no longer be completely ruled out, because both the ongoing hybrid war and the possibility of a traditional military conflict are threats to security. Miroslav Mareš defines hybrid war as a conflict conducted with the use of both violence and non-violence instruments in situations where there is no regular armed clash between rivals in war, the aim of which is to destabilize and demotivate the opponent, forcing its center of power to implement such a policy that is in the interest of the attacker; hybrid war is linked to conflict and the potential use of direct violence is not excluded, but the dominant influence is primarily the loss of ability and the lack and will to resist (Mareš, 2023, p. 70). Hybrid threats are not necessarily immediately visible and can weaken an enemy system in the long term, preparing the ground for its collapse or conventional war (Danics & Smolík, 2023, p. 127).

References

Danics, Š., & Smolík J. (2023). Czech security policy in the context of the hybrid warfare in Ukraine. In E. Kancik-Kołtun (Ed.), *30 Years of the Visegrad Group. Volume 3: The War in Ukraine and the Policy of the V4 Countries*. Wyd. UMCS.

Danics, Š. (2023). Ukrajina – prostor pro geopolitickié hry mocnosti. In J. Smolík (Ed.), *Region v rozvoji společnosti 2023: Sborník příspěvků z 11. mezinárodní vědecké konference 5.–6. května 2023 Brno* (pp. 69–74). https://doi.org/10.11118/978-80-7509-957-0-0069

Domeracki, K. (2019). Istota bezpieczeństwa dyplomacji. *Zeszyty Naukowe Wyższej Szkoły Zarządzania Ochroną Pracy w Katowicach*, *1*(15), 89–102. https://doi.org/10.32039/WSZOP/1895-3794-2019-07

Drab, L. (2019). Rola dyplomacji obronnej w zapewnianiu bezpieczeństwa międzynarodowego. *Kwartalnik Bellona*, *3*, 83.

Hyb, L. (2016). Dyplomacja jako środek utrzymania bezpieczeństwa. In D. Nowak, A. Zagórska, & M. Żyła (Eds.), *Si vis pacem, para bellum – Dyplomacja czy siła?*. Akademia Sztuki Wojennej.

Kancik-Kołtun, E. (2021). Poczucie bezpieczeństwa zdrowotnego obywateli podczas pandemii COVID-19 w państwach Grupy Wyszehradzkiej. *Rocznik Instytutu Europy Środkowo-Wschodniej*, *1*(19), 214. https://doi.org/10.36874/RIESW.2021.1.12

Kancik-Kołtun, E. (2023). Polish aid to Ukraine and its citizens during Russia's war against Ukraine. In E. Kancik-Kołtun (Ed.), *30 Years of the Visegrad Group. Volume 3: The War in Ukraine and the Policy of the V4 countries*. Wyd. UMCS.

Mareš, M. (2023). Česká republika v hybridní válce: Bilance a perspektivy. In J. Smolík (Ed.), *Region v rozvoji společnosti 2023: Sborník příspěvků z 11. mezinárodní vědecké konference, 5. – 6. května 2023 Brno* (pp. 69–74). https://dx.doi.org/10.11118/978-80-7509-957-0-0069.

Menkiszak, M. (2021). *Ukraiński dylemat Rosji: strategia Moskwy wobec Kijowa*. Ośrodek Studiów Wschodnich. https://www.osw.waw.pl/sites/default/files/komentarze_416.pdf

Pietraś, Z.J. (1978). *Dyplomatyczna misja specjalna jako instytucja prawa międzynarodowego*. Wyd. UMCS.

Surmacz, B. (2013). Wstęp. In B. Surmacz (Ed.), *Nowe oblicza dyplomacji*. Wyd. UMCS.

Surmacz, B. (2015). *Ewolucja współczesnej dyplomacji. Aktorzy. Struktury. Funkcje.* Wyd. UMCS.

Sygit, M. (2017). *Zdrowie publiczne*. Wolters Kluwer.

Szeptycki, A. (2015). Europa Wschodnia i Kaukaz Południowy: strefa niestabilności. *Rocznik Strategiczny*, *16*.

Wilk, M. (2002). Wstęp. In M. Wilk (Ed.), *Dyplomacja*. Wyższa Szkoła Studiów Międzynarodowych.

PART II

Disinformation

JAKUB OLCHOWSKI

MARIA CURIE-SKŁODOWSKA UNIVERSITY, LUBLIN

Russia's Disinformation as a Threat to the Security of Poland and the Czech Republic

Abstract: The paper examines the threat posed by Russian disinformation to the security of Poland and the Czech Republic. Despite differing geographical, demographic, and economic conditions, as well as distinct strategic cultures shaped by historical experiences and national identities, both countries face a common threat from Russia. This includes Russian disinformation and propaganda, crucial elements of Russia's hybrid warfare strategy against the West. While the instruments, channels, and target groups for these disinformation campaigns are similar in both countries, differences in societal susceptibility influence the content and emphasis of the campaigns. Russian disinformation, deeply rooted in the country's historical use of manipulative tactics, aims to exploit societal tensions, undermine trust in factual information, and polarize public discourse. The Kremlin employs narratives tailored to specific audiences, such as Euroscepticism and anti-Ukrainian sentiments in Poland and the Czech Republic, to weaken support for Ukraine, diminish trust in state institutions, and foster anti-EU and anti-NATO sentiments. The paper highlights the sophistication of Russian disinformation efforts, which leverage advanced communication technologies and exploit vulnerabilities in information environments of democratic states. The strategic goals of these campaigns are to weaken Western cohesion, disrupt internal stability, and influence political decisions. The study underscores the necessity for Poland and the Czech Republic to strengthen their resilience against such threats through coordinated efforts in cybersecurity, public awareness, and international cooperation.

Keywords: security; disinformation; hybrid warfare; Russia; Poland; Czech Republic

Introduction

Poland and the Czech Republic have different conditions when it comes to security and threats. This is due to various factors: geographical, demographic, economic. The strategic culture of both countries is also different, i.e. the way they think about their national security, resulting from historical experiences, mentality, specific

culture and national identity, etc. However, both countries are not only neighbors in the geographical sense – they share a civilizational affiliation, a specific history of the entire Central European region, cultural affinity and, finally, institutional ties, especially membership in the European Union and NATO.

The threats to their security are also largely common. First of all, in both cases, the main source of threat is Russia. The similarities concern every dimension of security, including Russian disinformation and propaganda, which are of fundamental importance from the point of view of Russia's hybrid war against the West. In the case of Poland and the Czech Republic, instruments, channels and target groups are similar. The strategic goals of Russian actions are similar, but the differences concern the distribution of content and emphasis in disinformation campaigns. This is due to the differences between Polish and Czech societies, which make them susceptible to certain narratives to varying degrees. In this context, it can be noted that this regularity was aptly described by Ladislav Bittman, deputy chief of the Czechoslovak intelligence service's disinformation department in the 1960s. He pointed out an important rule: in order to succeed "every disinformation message must at least partially correspond to reality or generally accepted views" (Legucka, 2022).

Russia at war

Russian disinformation activities have already been described very widely, and this problem has finally, although perhaps too late, begun to be noticed not only in terms of an academic curiosity. In general, let us recall that such actions are part of the imperial strategy of *divide et impera*, consistently implemented for centuries, not only by Russia. In the case of the latter, however, it is of a specific nature – these activities have been raised almost to the rank of art, and extensive instruments and know-how have resulted in the appearance of the so-called active measures (Rus.: *активные мероприятия*). The term appeared during the Cold War, it does not exist officially, but actual references to it ("special means of influence", "informational-psychological impact") can be found in official documents, such as the national security strategy or war doctrine.

It is a broad concept, referring to many different forms of impact on the international environment. They can be defined as all activities of a diverse nature (manipulative, disinformation, agentic, destabilizing, polarizing, etc.) and used using various instruments and techniques (influence operations), the aim of which is to induce opponents in the international environment to behave and act in accordance with the interests of the USSR/Russia. After the end of the Cold War, "active measures" continued to be used, but thanks to the development of communication

technologies, new instruments and opportunities emerged – which were immediately and successfully used.

This success was possible largely because, as mentioned, Russia has vast experience and dedicated resources: human, financial, institutional and technological. The roots of this know-how run deep: disinformation, manipulation, and propaganda activities have been undertaken by Russia's secret services in all of its iterations: Third Department, Okhrana, Cheka, OGPU, NKVD, KGB, GRU, SVR, and FSB. The theoretical foundations are developed:e.g. decades ago, Evgeny Messner formulated the concept of *subversion* or *mutinous* wars (Rus. *мятеж войны*), which has now been modified, developed and enriched with new elements based on information technologies, becoming the foundation of today's "hybrid warfare" (Olchowski, 2022). Obscuring the image of reality in order to confuse the opponent, which is nothing new in the history of conflicts and diplomacy, has become the hallmark and basic method of operation of the Russian secret services, commonly known as *maskirovka* (disguise). Technological development and civilizational changes, which accelerated unprecedentedly in the 21st century, have only changed the scale of this phenomenon. As Mark Galeotti aptly put it, in the past wars there were 80% combat and 20% propaganda, today there are 80–90% propaganda and 10–20% combat – the Russians are aware of this and are able to exploit it, using all available instruments: diplomacy, secret services, state and parastatal institutions, social media, influence agencies and, finally, ordinary "useful idiots" around the world (Galeotti, 2019). Finally, authoritarian states, such as Russia or China, have a fundamental systemic advantage over democratic states in the information domain – they can fully control the information flow and their own infosphere, thus, using information as a weapon against which the West – with its inherent features, i.e. freedom words and pluralism of opinions – is largely helpless, and dictatorships realize this.

Tailoring

Kremlin disinformation is often tailor-made. There is used a set of narratives that work as templates for particular stories and can be adapted to a target audience. This can be analyzed and patterns identified in various ways. The East Stratcom Task Force, the European Union body dealing with combating Russian disinformation, identifies five general narratives (EUvsDiSiNFO, 2019):

1. The Elites vs. The People: "Evil elites" are out of touch with the needs of "ordinary people". This populist trope is especially useful during elections, when it is deployed to attack the political establishment and offer voters easy solutions (and scapegoats) to complex problems. It is also often connected to conspiracy theories and operates on the basis of emotions and faith rather than facts.

2. Threatened Values, or "the rotting West". This shows Western attitudes to the human rights, minority rights, etc. as an evidence of a decadence and a moral decay, while Russia is presented as a haven of traditional values, based on "decency", "common sense", "Christianity", "purity", etc.

3. Lost Sovereignty or Threatened National Identity: Western states and societies are no more sovereign and independent, they are directed by external forces that want to destroy them (be it the USA, big corporations, immigrants, Israel, Islam, LGBT conspiracy, Big Pharma, etc.).

4. Imminent Collapse: The West is going to collapse soon, it is on the verge of the civil war. This narrative framework is very useful as it addresses, exploits and ignites societies' fears connected to economy, migration, terrorism, etc.

5. "The Hahaganda Narrative": jokes, sarcasm, ridiculing, derogatory descriptions and mockery in reference to individuals (e.g. leaders), Western states and values (democracy) – in fact it is a way to disguise lies and deception (*maskirovka*).

As mentioned, different narratives, in different configurations, are used to refer to different audiences. For example, a whole range of anti-Ukrainian narratives has been consistently used against Poland for years, exploiting strong emotions in Polish society related to tragic events from the past (such as the Volhynia massacre). In Germany, pro-Russian narratives feed on German trauma and guilt related to World War II, while emphasizing the need to maintain good relations with Russia, which supposedly determine German prosperity and economic development (hence, among others, German support for Nord Stream II, presented to Germany as an economic project beneficial for them). Czech citizens, however, are fed with anti-American, anti-NATO, anti-EU and anti-Israel narratives (Tatarenko, 2023b).

Generally, everything that has the potential to generate and deepen social tensions and conflicts is used. Russia is trying to inspire and fuel them – but also create them. Therefore, any social phenomenon that can cause tension and fear (which became particularly visible and important after the Russian invasion of Ukraine in 2022) is a platform for Russia's disinformation activities. All kinds of conspiracy theories are a convenient tool; narratives about the Illuminati, Davos, Jews, globalists, Satanists, the Bilderberg Group and, of course, fascists are successfully used.

The COVID-19 pandemic was actually a special opportunity to strengthen social fears and the radical circles and conspiracy theories that feed on them. It was also used by Russia – in numerous narratives, the COVID-19 pandemic was linked to everything, e.g. NATO and its "plots". Anti-vaccine groups have significantly strengthened, and often "accidentally" also presented pro-Russian opinions. This turned out to be very useful after the invasion of Ukraine – anti-vaxxers suddenly became fierce enemies of Ukraine and one of the main propagators of Russian theses about "Nazi Ukraine" and "Western aggression against Russia" (Demczuk, 2023).

In general, the specific goals of Russia's pandemic-related disinformation campaign have included undermining trust in objective facts and credible information sources concerning pandemia. According to a study by the Oxford Internet Institute, COVID-19 propaganda materials published by Russian and Chinese state media reached a larger audience on social media in France, Spain and Germany than information from their state media. To illustrate the impact of disinformation related to the COVID-19 pandemic, in October 2020, around 43% of Moldovans believed that the coronavirus was developed by "World Government" to control humanity (Legucka, 2022).

We must also bear in mind that disinformation is a growing threat in the modern world also due to rapidly occurring civilization changes, the consequences of which include: 1) increasing disagreement among people and societies about facts and analytical interpretations of facts and data; 2) blurring of the line between opinion and fact; 3) the increasing relative volume, and resulting influence, of opinion and personal experience over fact; 4) declining trust in formerly respected sources of factual information (Legucka, 2022).

As a result, disinformation can become a very powerful, destructive and divisive tool. It exploits ethnic, religious, regional, social and historical tensions and conflicts, and promotes anti-systemic attitudes, extending their reach and giving them an appearance of legitimacy (Lucas & Pomerantsev, 2016).

Evolution

Narratives can be combined and modified based on current events and changing social attitudes. This was visible after Russia's invasion in 2022, when new threads appeared. Despite this evolution the general narratives are still similar and their strategic goal is also coherent with Russia's story about the world – it is to convince people that "Ukrainian crisis" was a result of NATO expansion", "the West prolongs the war by providing Ukraine with weapons" and "Ukraine should negotiate with Russia".

Obviously, there are many modifications, depending on actual events. After Finland and Sweden joined NATO, pro-Kremlin outlets claimed the both states' leaders "surrendered the countries to NATO slavery", turned them into a "colony of the Empire" to "start a world war". Not asking "ordinary people" about their opinions, naturally. And "NATO expansion" is a part of a plan to encircle and destroy Russia – which is also, by the way, the reason for "the current bloodshed in Ukraine" (EUvsDiSiNFO, 2024).

It is therefore not surprising that in the face of the upcoming elections in Moldova and the beginning of this country's accession negotiations with the European

Union, the Russian propaganda machine has targeted Moldova, taking action in every dimension, including at the cognitive level – it is the "Moldovan leaders" who "dangerously" want to join the Alliance – "the citizens of Moldova want calm, peace, and neutrality".

In every case, the Russian authorities try to havean indirect influence on internal Western countries processes. The goals are diversified – currently weakening democratic institutions around the world and taking advantage of international and internal crises serves, for example, to lift sanctions against Russia and discourage support for Ukraine.

As a side note, it can be added, although this is a topic for a broader discussion, that the assessment of the effectiveness of Russian disinformation depends, among others, on "disinformation resilience" which is defined as an "adaptability of states, societies, and individuals to political, economic, and societal intentional pressure and falsehood spread in various formats of media (including social media) in order to influence political and economic decisions" (Yeliseyeu & Damarad, 2018). The Disinformation Resilience Index (DRI) is based on three indicators. The first indicator concerns population exposure to Kremlin-backed media. It is based on Russian media popularity and trust ratings among the country's population. The second one, the quality of systemic responses, defines a state's preparedness, i.e. institutional design in the sphere of information security, legal framework comprehensiveness as well the quality of countermeasures by the media community and civil society. The third indicator, vulnerability to digital warfare, concerns the prevalence and counteraction to masked sources of disinformation (mainly social media and the Internet).

Poland and the Czech Republic

To put it briefly, it is necessary to point out similar narratives in pro-Russian narratives addressed to Poles and Czechs. Disinformation activities during the pandemic were undoubtedly similar, but this applies to many countries. Currently, the dominant themes include supporting Eurosceptic or openly anti-EU opinions, arousing resentment towards Ukraine and Ukrainians residing in Poland and the Czech Republic, and attempts to interfere in the internal situation (on the occasion of elections, but also by polarizing public discourse).

This basically has three goals: the first of them results from the current international situation and is to weaken support for Ukraine, including by distracting public opinion from the conflict. Secondly, Russia is trying to build and strengthen hostility towards the EU and NATO in the long term in order to weaken Western cohesion (which is Russia's strategic goal). Thirdly, the aim is to sow distrust towards state authorities and institutions as well as the mainstream media (Tatarenko, 2023a).

In both states, there is a growing awareness of the threats related to Russian disinformation and pro-Russian propaganda. Both Poland and the Czech Republic claim that Russia is waging a hybrid war against them, in which disinformation activities are important. Both countries are also targets of cyberattacks, which increased after February 2022 and after Russia's invasion of Ukraine (Tatarenko, 2023b). Occasionally, there are spectacular events – in Poland, these were agricultural protests that swept across the country at the turn of 2023/24, largely anti-Ukrainian in tone and strongly inspired by pro-Russian circles.

In the Czech Republic, at the beginning of 2024, there was much talk about the disclosure of espionage and pro-Russian activities of the Voice of Europe portal and the investigation into the explosion in ammunition depots. As a result, structures and institutions are being created in both countries and their activities focus not only on cybersecurity in the strict sense, but also on activities aimed at limiting Russian influence. These are not only public institutions and entities, the activities of the third sector (civil society) are also of great importance. Coordination of activities at the state level is needed, actions are being taken in this area.

This is necessary, again from the point of view of both countries, for at least two reasons. Firstly, Poland and the Czech Republic are among the countries where Russian influence threatens social cohesion, political stability and foreign policy. The Russian disinformation and propaganda machine should not be underestimated. It works coherently, professionally and quickly, and can effectively use opportunities to attack Ukraine, Poland and the West, discrediting them and stimulating divisions. Importantly, complex information operations may be almost impossible to identify from the perspective of an average information recipient.

Examples from Poland prove this. Recently, pro-Russian circles have been closing ranks and striving to play a greater political role. They do not formally articulate a pro-Russian position (in Poland this is a political suicide), hiding behind the façade of "anti-war" movements and groups, using at the same time strongly anti-Ukrainian and anti-Western rhetoric. They also question the policy of the Polish government, deepening the already significant polarization of society (in this case, the aim of Russia's actions, as in other countries, is to change the shape of the political scene so that anti-Ukrainian/pro-Russian formations come to the fore).

Here it is worth paying attention to the elements of continuity and change – "anti-war movements" inspired by Moscow are not new. They were used by the Soviet Union during the Cold War. Anti-Ukrainian rhetoric addressed to Poles is also nothing new. However, it is evolving. Permanent threads devoted to historical events are currently accompanied (summer 2024) by narratives intended to discourage involvement in helping Ukraine under the pretext of caring for Poland's peace and security – hence the slogan "it's not our war". According to this narrative, the Polish government wants to involve Poles in a war against Russia on the orders of the US, i.e. not in the interests

of Poland, but additionally in defense of Ukraine, which is hostile towards Poles and Poland. Until recently, the dominant narrative was about the "Ukrainization" of Poland by refugees living at the expense of Polish society and the state.

Secondly, it has a broader dimension. Both Poland and the Czech Republic are Central European countries, with all the baggage specific to this region: the legacy of remaining under the yoke of foreign powers, with the memory of decades of Soviet domination and many painful systemic transformations (political, economic, social, territorial). Currently, independent and sovereign states of Central Europe are becoming more and more important actors (just like the region itself) in international relations. However, this is only possible if they are not subject to the influence of Russia which did not and does not recognize the existence of Central Europe as an independent entity, because it is in contradiction with its imperial ambitions (Olchowski, 2024).

The attitude of some countries in our region is, however, worrying. While Poland and the Czech Republic rightly diagnose the threat from Russia, both in the short term and strategically, the situation is different in the case of Hungary and, to an increasing extent, Slovakia. They do not treat Russia's actions as a threat, but on the contrary – Russian (like Chinese) influence in these countries is constantly growing. At the same time, this is also a challenge for Poland and the Czech Republic and should lead to closer relations between them.

References

Demczuk, A. (2023). *COVID-19-Related Infodemic in Poland*. Wyd. UMCS.

EUvsDiSiNFO. (2019, April 2). *5 Common Pro-Kremlin Disinformation Narratives*. https://euvsdisinfo.eu/5-common-pro-kremlin-disinformation-narratives/

EUvsDiSiNFO. (2024, June 25). *Three Kremlin disinformation narratives about NATO enlargement*. https://euvsdisinfo.eu/three-kremlin-disinformation-narratives-about-nato-enlargement/

Galeotti, M. (2019). *Russian Political War: Moving Beyond Hybrid.* Routledge.

Legucka, A. (2022). Russian disinformation: Old tactics and new narratives. In A. Legucka & R. Kupiecki (Eds.), *Disinformation, Narratives and Memory Politics in Russia and Belarus* (pp. 22–42). Routledge.

Lucas, E., & Pomerantsev, P. (2016). *A Report by CEPA's Information Warfare Project in Partnership with the Legatum Institute*, https://cepa.org/comprehensive-reports/winning-the-information-war/

Olchowski, J. (2022). How to weaponize information: Russian patterns. In A. Legucka & R. Kupiecki (Eds.), *Disinformation, Narratives and Memory Politics in Russia and Belarus* (pp. 50–64). Routledge.

Olchowski, J. (2024). Zmiana środowiska regionalnego systemu Europy Środkowej. In M. Pietraś, W. Baluk, & H. Perepełycia (Eds.). *Partnerstwo strategiczne Polski i Ukrainy w warunkach zmiany systemu międzynarodowego* (pp. 61–78). Wyd. UMCS.

Tatarenko, A. (2023a). Dezinformacja w Republice Czeskiej: działania władz i społeczeństwa obywatelskiego. *Komentarze IEŚ*, *844*(92). https://ies.lublin.pl/komentarze/dezinformacja-w-republice-czeskiej-dzialania-wladz-i-spoleczenstwa-obywatelskiego/

Tatarenko, A. (2023b). Jak Czechy radzą sobie z cyberbezpieczeństwem i dezinformacją po rozpoczęciu wojny w Ukrainie. *Komentarze IEŚ*, *1011*(259). https://ies.lublin.pl/komentarze/jak-czechy-radza-sobie-z-cyberbezpieczenstwem-i-dezinformacja-po-rozpoczeciu-wojny-w-ukrainie/

Yeliseyeu, A., & Damarad, V (Eds.). (2018). *Disinformation Resilience in Central and Eastern Europe*. PRISM. http://prismua.org/wp-content/uploads/2018/06/DRI_CEE_2018.pdf

AGNIESZKA DEMCZUK

MARIA CURIE-SKŁODOWSKA UNIVERSITY, LUBLIN

Disinformation in Poland – Diagnosis, Combating, Counteracting

Abstract: The contemporary public discourse is infected with disinformation and conspiracy narratives, which have become basic elements of influence campaigns conducted by various propagandists in democratic systems. An information war has been going on in cyberspace for years – also in Poland – the face of which is the fight for the "rule of the souls and minds" of voters. The disinformation conglomerate reinforced with IT automation systems enables the growth of content harmful to institutions and democratic values, such as discourse, human rights, the rule of law and security, highly effectively and on an unprecedented scale. What is needed is education, moderation, regulation, as well as a new media policy based on proactive ethics, pluralism, inclusion, and the responsible use of information freedom in the fight and prevention of disinformation.

Keywords: misinformation; disinformation; propaganda; fake news; fact-checking; cyberspace; Internet; ICT; Poland

Introduction

Democratic societies have lost the ability to differentiate between truth and falsehood. The democracy and the fundamental values vital for an equal and just society are at serious risk. Disinformation and conspiracy theories are harmful factors to undermine and destroy public security and other common democratic values, such as human rights and freedoms, public discourse, democracy and the rule of law. Disinformation erodes communities and costs lives. For example, in 2020, rumors, stigmas and conspiracy theories about SARS-CoV-2 distributed in the infosphere were recognized by the World Health Organization experts as a new global threat. The researchers from the American Society of Tropical Medicine and Hygiene warned that in the first months of the COVID-19 pandemic (2020), nearly 6,000 people around the world were admitted to hospitals as a result of disinformation

distributed on social media. More than 800 people have died from drinking methanol or other alcohol-based disinfectants (Islam et al., 2020, p. 1622). Disinformation actors (both agents of influence and transmitters): 1) disrupt society by running influence operations, 2) are well resourced due to their use of advanced tech and tactics (*vide* manipulative and black market infrastructure of social media) (Bay & Reynolds, 2018), 3) have an advantage against pro-democratic actors because they are using methods and techniques which are lawless and they are using cyberattacks. So, democracy and the facts are being lost in the battle, and in consequence, defending against both misinformation, disinformation but also malinformation needs coordination on a large scale. Fact-checking and debunking are not effective; as well as protection of individual dignity against hate speech and stigmas is not effective and sufficient. Defenders need to set the agenda in advance; public authorities, experts, civil society, campaigners and communicators are in need of advanced tools to cooperate on a large scale; they are in need of strategic communication, policy and systemic recommendations to fighting and counteracting disinformation.

Online disinformation as a means of hybrid warfare

Both the political class and the civic society in the European Union states, also in Poland, have the problem with democratization of disinformation. The main problem is the democratization of disinformation *à la* the Kremlin. For the pro-Kremlin propaganda centres, every single dispute, every single potential conflict have provided fuel for disseminating polarising and disinformation content for years. The cyberspace has seen hypertrophy and renaissance of the pro-Kremlin disinformation for years. The Russian online disinformation relies on state-sponsored sources and the pro-Kremlin groups who collectively spread false and misleading narratives in multiple languages to play out globally. For years, the Internet Research Agency, the so-called trolls' factory, has been conducting mass propaganda on social media with the main goal of influencing public opinion by disseminating content in multiple languages, consistent with the Russian politics and ideology. Disinformation peddled by Russia is very effective, and has thousands of echo chambers in the European states.

After the annexation of Crimea in 2014 and the emergence of the so-called hybrid warfare in Donbas, the Kremlin intensified propaganda and disinformation directed against the European Union and the United States of America. Anti-refugee, anti-immigrant, anti-Ukrainian and Islamophobic disinformation campaigns; involvement of pro-Russian trolling and botting in the disinformation Brexit campaign or Donald Trump's American election campaign in 2016, as well as climate change denial campaigns, "yellow vests" protests in France in 2018, COVID-related infodemic,

and so on – these are only some of the recent negative examples of manipulative semantic influence carried out by propaganda media outlets which began to target Internet users in democratic systems. The phenomenon of the narrative *à la* the Kremlin is already widely known in 2024, and the involvement of the pro-Kremlin disinformation was also observed in the anti-vaccination discourse connected not only with SARS-CoV-2, but few years before the outbreak of the COVID-19 pandemic (Broniatowski et al., 2018).

The phenomenon of COVID-19-related infodemic has shown all the harmful and destructive effects of the mechanism of information disorder on the quality of public discourse. In the information disorder model created by Claire Wardle, three types of such information were distinguished, based on falseness and harm criteria, i.e. whether the information is false, harmful or both, false and harmful at the same time. It was assumed that (Wardle, 2017): 1) misinformation occurs when false information is shared, but it is not intended to cause harm, 2) disinformation occurs when false information is shared with the intention to cause harm, 3) malinformation occurs when information is either genuine, but shared in order to cause harm, often in violation of the prohibition on disclosure of such information (because it is private or confidential information), or it contains a negative, stigmatising, hateful opinion (hate speech), while it may be partially true. Wardle identified and indicated three elements of information disorder which contribute to the emergence of the mechanism of polluting information ecosystem, i.e. the agent, messages and interpreter, and three phases of the information disorder emergence: creation, production and distribution.

We have to identify the phenomenon of the contemporary disinformation according to Vladimir Volkoff's (1991) disinformation theory. The basic concepts accompanying disinformation include: 1) the client, i.e. a person or a group, which benefits from the disinformation operation (e.g. a commercial entity, a state, a political party, individual politicians, and others); 2) the agent, i.e. an entity that carries out a disinformation dissemination assignment who acts via agents of influence (i.e. disinformation agency and hired agents of influence); 3) supports – events that are the basis of the disinformation activity which do not have to be true, but it is important that they evoke unambiguous associations, e.g. fake news, deep fakes, conspiracy theories; 4) transmitters – media, the following may be the transmitters of a given disinformation in the initial stage: a niche magazine, a local radio station, and then the disinformation is "picked-up" by the mainstream media; 5) the disinformation theme; 6) echo chambers (resonators) – media, both the ones unrelated with agents of influence and the ones related to such agents, whose aim is to introduce information noise, media noise; they also intend to regurgitate theses created by agents of influence, their task is to create an impression (most often unintentionally) that "a given event is being talked about" and to make the topic as widely discussed as

possible. Often it is just ordinary citizens who can also serve as resonators, because they repeat disinformation that was made up beforehand and share it on their social media profiles; 7) target group – a group to which disinformation activities are addressed, including selected social groups, and sometimes the whole society.

Nowadays, the cyberspace has become an ideal transmitter and the place for hundreds of virtual resonators, trolling and botting, being digital agents of influence, where disinformation on selected social, political, economic, health-related topics, and other, is likely to be disseminated by artificial intelligence, endlessly. It is made possible due to the presence of a complex and multi-element disinformation infrastructure, i.e. conglomerate disinformation. Every single and conflict topic is used to disinformation by the Kremlin agents of influence in the context of informational matrices. The Russian Federation and its propaganda focuses on the idea of the weak West, creating disinformation based on geopolitical, conspiracy, Eurasian, Ukrainian, or sovereignty matrices, and it will continue to attack the European Union with information.

It should be noted that for years, non-state actors, from far-right online militias to populist parties, have been adopting the "Putin Playbook" tactics as part of automated influence operations. For example, in the European election times in 2019, there was a shift away from information warfare to "narrative competition" with the promotion of "culture wars" around issues such as migration, Muslims in Europe, family *versus* progressive values, or climate policy. Anti-Semitism, misogyny, and racism were used as weapons in these elections, amplified by automated accounts (Institute for Strategic Dialogue, 2019). But, in 2024, and after Russia's full-scale aggression against Ukraine, we are again dealing with intensification of hybrid activities which has even been referred to as regular hybrid warfare.

Russia's hybrid warfare has been in full swing in recent years, but it did not evolve overnight. The top Russian officials started calling for a comprehensive security doctrine around a decade ago. In 2013, Russia's Chief of the General Staff, General Valery Gerasimov suggested that the country's security policy needed to adapt to the changing nature of conflicts. In an article that has been widely scrutinised in Western policy circles, Gerasimov highlighted the growing role of non-military means for achieving political and strategic objectives (Bilal, 2024). It is worth mentioning that cyberspace, including social media, are breeding grounds for disinformation, and the Russian Federation takes this into account in its strategic calculations. The service EUvsDisinfo maintains a database of tens of thousands of online disinformation samples purportedly linked to the Kremlin, which are verified by the collaborators of the StratCom Task Force (The Disinformation Review). Before 2020, the platform became an important source of information about fake news, conspiracy theories, and manipulations about, e.g.: Ukraine, Brexit, migrants, election in European states and so on; in 2020 – also about COVID-19-related issues. For

example, the number of all pieces of disinformation identified for verification since 2015 increased from 11,052 (as of 20 February 2021) to 17,133 (as of 30 May 2024), demonstrating a dynamic, even exponential annual growth (EUvsDisinfo, 2024).

Diagnosis of disinformation in Poland

Unfortunately, for years, disinformation remained a little-known phenomenon in Poland. Both the political class and the society paid little attention to the problem, maybe except some NGOs, researchers and journalists. Even though it has repeatedly created political negative sentiment in Poland. We have no knowledge of identifying the scale and scope of the activities of Russian or pro-Russian agents of influence on public discourse in Poland. And we do not know which were/are the Russian influence or Polish activities (prepared and disseminated according to "Putin's Playbook" narratives). Instead, we have knowledge (from fact-checkers and media reports) of the scale and scope of hundreds of thousands of various disinformation and malinformation narratives.

For example, in 2015, anti-immigrant narratives – fake news and conspiracy theories known as smear campaign – contributed significantly to the Law and Justice (PiS) party gaining power and election victory, and in 2018, also far-right wing politicians tried the same game against immigrants, and additionally, against LGBT+ in local government election campaign. From 2015 to 2023, there was a smear campaign against the LGBT+, refugees, some striking judges, doctors and teachers, opposition politicians and other groups in Poland. For example, there were many pejorative metaphors and hateful words with fake news addressed in the public debate towards: 1) the LGBT+ community (e.g. "decontamination after the LGBT+ march", "rainbow plague", "child sexualization by LGBT+", LGBT+ as a "homo-lobby", "homo-terror", "homo-propaganda", and "homo-revolution", the Pride March as "a promotion of perversions, deviations and denaturing"), 2) the migrants (e.g. "demographic and social jihad", "refugees spread germs and disease", "every refugee is a terrorist", "refugees murder and rape women and children"), 3) the judges (e.g. "judges who are common thieves"). This means that the Polish authorities and public media, instead of fighting disinformation and hate speech, they spread disinformation and malicious information.

Also, we have knowledge that since 24 February 2022, NASK (National Research Institute) has reported 521 harmful disinformation materials to public administration authorities for urgent response, and has detected 1,592 highly harmful accounts (mainly Facebook and Twitter) (Dąbrowska-Cydzik, 2023b). Media reports showed that 88% of accounts disseminating disinformation discussed topics related to the Russian Federation and Ukraine, and 81% published posts criticizing aid for refugees. We have knowledge that the Internet and Social Media Research Institute showed

that the hashtag #tonienaszawojna was used over 20,000 times in February 2023. Taking into account the nature of the activity of the analyzed hashtags, it can be concluded that they constitute a form of consolidation of the activity of radical or even pro-Russian circles under a common slogan "to nie nasza wojna" ("This is not our war") (Dąbrowska-Cydzik, 2023a). Just as we know that, for example, in 2021, FakeNews.pl fact-checker identified over 30 Polish portals that spread disinformation related to COVID-19, while repeating the Russian narrative (Pawela, 2021).

Over the past eight years, Polish society, authorities and infosphere had the problem with freedom of speech in practice, mainly with the politicisation of public media and their political involvement in election campaigns. After losing the 2023 elections, TVP journalists admitted to spreading government propaganda. That situation did not help to counteract disinformation.

The disinformation crisis in Poland did not change during the COVID-19 pandemic and unfortunately, Polish society has proved to be less resistant to false content. During the pandemic, alt-internet became a perfect place for anti-mask, anti-COVID and anti-vaccine echo chambers, where profiles, fan pages, public and private groups were followed by hundreds of thousands of Internet users, alt-internet content was commented on and liked several tens of thousands of times. Disinformation, rumours and conspiracy theories had penetrated the mainstream of the public discourse in Poland. The COVID discourse in Poland was conducted in the realm of post-truth culture, it was highly emotional and polarised, based on opinions, judgments, and manipulations fulfilling non-informational functions. It was hardly based on facts, scientific evidence and statistics. Official statistics on SARS-CoV-2 infections were flawed with errors resulting from the processing of data provided to the Chief Sanitary Inspector and the Ministry of Health by district sanitary-epidemiological stations, and, thus, they too became a source of misinformation (fact-checking by Michał Rogulski). It should be noted that according to data from the Ministry of Health from March 4, 2024, a total of 6,660,562 people have been infected with coronavirus in Poland from the beginning of the pandemic; 120,573 people died because of COVID-19 infection (Gov, 2024).

The COVID debate, especially when held with the participation of politicians, and dominated by strategies of both denial and trivialisation as well as strategy of discrediting, was largely unsubstantive, and the consequences of conducting the debate in such a way proved to be damaging both in social and health terms because, for example, there was a loosening of the social discipline necessary to effectively deal with the COVID threat. It also introduced unnecessary chaos and information noise, which, in turn, had to prove unfavourable for citizens and entrepreneurs who reorganised their entire private and professional lives and were obliged to close their businesses, in fact on constitutionally dubious legal grounds (Demczuk, 2023). In consequence, Poland remained one of the least vaccinated countries in the EU/

EEA. In 2024, arguments appeared in the public infosphere that If it were not for the ignorance of politicians and anti-vaccination propaganda in Poland, twice as many people could have died from COVID-19 (Klinger, 2024).

Russia's full-scale invasion of Ukraine in 2022 demonstrated the power of the Kremlin propaganda in Poland once again. Thousands of social media accounts have shifted from anti-vaccine narratives to anti-Ukrainian content (Science in Poland, 2023).[1] It was quickly noticed that the accounts that had so far spread disinformation in connection with the COVID-19 pandemic had a large share in the spread of conspiracy theories and false information about Ukraine (Zadroga & Wilczyńska, 2023, p. 3).[2]

In the first period of the war, however, Polish society proved resistant to Russian propaganda against Ukraine. The Kremlin's aggressive narratives were ineffective, and Poles were willing to support Ukraine and provide shelter to refugees (Zadroga & Wilczyńska, 2023, p. 3). However, some politicians such as those from the far-right Confederation Liberty and Independence party spread malicious information about Ukrainian, as well as anti-Ukrainian disinformation and became "useful idiots" of the Kremlin. Kremlin propaganda and disinformation attack in the Ukrainian context are based primarily on fear, uncertainty and playing on emotions. Five main thematic areas are most frequently and widely used: 1) the risk of war on Polish territory, 2) the migration and social crisis caused by Ukrainian refugees, 3) discrediting of Ukraine on the international arena, 4) the energy and economic crisis, and 5) politics of memory (especially massacres of Poles in Volhynia and Eastern Galicia).

However, in 2024, the farmers' protests showed that the economic tensions between Poland and Ukraine caused a renewed rise in anti-Ukrainian sentiment in the first months of 2024 and the use of anti-Ukrainian narratives in politics by some politicians such as the Confederation Liberty and Independence party.

It is impossible to determine how many people shared anti-Ukrainian content with the knowledge that they were duplicating the Russian disinformation. Well-known politicians of the Confederation Liberty and Independence party became famous, among other things, for promoting the slogans "Stop ukrainizacji Polski" (#stopukrainizacjipolski) or "Ukropolin" (#Ukropolin). "Ukropolin" is an evolution of the "Polin" project (another conspiracy theory, is a variation of the so-called world Jewish conspiracy, according to this theory, the Polish government is

[1] But according to Leon Ciechanowski from the Kozminski University, in 2023, only 6.4% of anti-vaccination accounts on X (formerly Twitter) started publishing anti-Ukrainian content after the Russian Federation's attack on Ukraine; it was not easy to prove that we were dealing with an organised propaganda campaign. Also the analysis showed that among those opposed to vaccinations who moved to criticize Ukraine, accounts associated with the far right were the dominant group.

[2] As FakeNews.pl indicated in their report from March 2021, "anti-vaccine/anti-covid" narratives were strongly associated with the Kremlin's centres of influence.

preparing the Poles for the "absorption" of Poland by Ukraine and creation of the "Ukropolin" state).

As mentioned above, there are serious problems with disinformation in Poland but public authorities do nothing (or almost nothing) to counteract them. Poland does not have comprehensive policies to combat disinformation. Polish intelligence services do not have a clear policy for reporting disinformation threats. There are also no clear guidelines for public institutions on counteracting disinformation. There is no general legal act in Poland that would introduce legal solutions regarding disinformation. Anti-fake news law is controversial because its provisions may violate freedom of speech. The prosecution of false information may be based on the accusation of personal rights violation, such as defamation, also lying or providing false information during elections may be prosecuted. The Polish Penal Code includes provisions for protection against hatred of ethnic, religious, or racial groups; but there are no provisions in the law on protection based on gender or sexual orientation or age or disabilities. Finally, new government are preparing amendments in that issue but the individuals are still waiting (on June 2024). There are also provisions prohibiting the promotion of totalitarian regimes, such as fascism or communism. A special provision also applies to Holocaust denial.

In 2021, the then Minister of Justice, Zbigniew Ziobro, tried to introduce a law on the protection of freedom of speech. The new law was intended to protect citizens against attempts by internet corporations to limit public debate. However, concerns were raised that the provisions of this act would lead to abuse by the authorities. Furthermore, it could be used to limit freedom of speech and protect only content that would be favorable to the ruling party.

Fighting and counteracting disinformation in Poland

For years, the fight against disinformation was a task in the hands of NGOs and journalists from private media. There are several organisations, institutions and media that are involved in fact-checking (see Table 1).

Table 1. Countering disinformation in Poland: community of NGOs and media fact-checkers (selected examples)

Fact-checking organisations, and institutions	Fact-checking media
AFP Sprawdzam: Polish branch of the French Press Agency. IFCN member	Fake Hunter: Fact-checking organisation of the Polish Press Agency

Fact-checking organisations, and institutions	Fact-checking media
Wojownicy Klawiatury (Keyboard Warriors): fact--checking initiative engaged in the fight against manipulated content. The Bronisław Geremek Foundation and the Polish Robert Schuman Foundation created the project	OKO.Press: Polish online news and opinion website on political and social issues, mainly focused on investigative journalism and control of government activities
Foundation "Counteracting Disinformation" – FakeNews.pl (2020): second-largest fact-checking organisation in Poland. IFCN member	Konkret24: Group of journalists that work as fact--checkers in TVN, a Polish free-to-air television station, network and a media and entertainment group in Poland
Demagog: the first and largest fact-checking organisation (since 2014). IFCN member	CyberDefence24.pl: portal dealing with the issues of cybersecurity, digitalization and technology, the aim of which is to inform and educate recipients in the field of cybersecurity
StopFake.org is an educational platform, founded by Mohyla School of Journalism at National University of "Kyiv Mohyla Academy", which aims to implement high standards of journalism education in Ukraine	EURACTIV.pl: an independent pan-European media network specialised in EU affairs, established by its founder Christophe Leclercq in 1999
NASK*: a Polish research and development organisation and data networks operator. NASK conducts projects against disinformation and monitors the security of the Polish computer network. The institute operates a computer emergency response team — CERT Polska	

*NASK is a National Research Institute under the supervision of the Prime Minister of Poland. Unfortunately, the former government used Counteracting Disinformation System of NASK to build a system to control the opposition's messages. The team at NASK, instead of protecting Poles against disinformation, followed the entries of the opposition and journalists and informed the Prime Minister Morawiecki about it. From 2024, NASK is under the supervision of the Ministry of Digital Affairs.

Source: Author's own study.

Finally, it is worth mentioning the initiative of almost forty Polish experts who in 2022, jointly prepared a report containing over sixty systemic recommendations regarding counteracting disinformation (Mierzyńska, 2023). This is a grassroots civic initiative, and its purpose is to show how both state and civic society can protect ourselves from the information threat, which is having an increasingly strong impact on Poles.

These are the following key recommendations for specific areas such as:

1) **The state and its institutions**: Strengthening civil society and democracy institutions in the fight against disinformation.

2) **Regulation**, e.g.: introducing EU provisions related to digital services, blocking the possibility of making money online from disinformation, strengthening the National Election Commission and equipping this institution with tools to fight

disinformation; The Digital Services Act and the Digital Markets Act form a single set of rules that apply across the whole European Union. They have two main goals: to create a safer digital space in which the fundamental rights of all users of digital services are protected and to establish a level playing field to foster innovation, growth, and competitiveness. It should be noted that these documents introduce revolution in the ICTs area, but they are also long-awaited legal acts.

3) **National security:** Institutionalizing the fight against disinformation, both structurally and legally, and creating a more active role for the services in building awareness of this threat.

4) **Education:** Media and information literacy is needed, recognizing disinformation as a social threat, creating and integrating media education into the curriculum, enabling people to learn how to handle information.

5) **Information space:** Development of standards for handling information – including verification – in the media, reduce the impact of web traffic on the financial situation of the media, which would result in a reduction in the importance of "fast information".

6) **Sociology and psychology of disinformation:** Polish society needs permanent social dialogue and a long-term campaign to build public awareness of disinformation, securing funding for these activities.

It seems that since 2024, the perspective of perceiving disinformation threats has changed, with the authorities declaring more commitment to combating it, increasing financial resources for fact-checkers NGOs, more active involvement in work with NGOs in order to implement the provisions of the Digital Services Act package (a coordination point was established in the Ministry of Foreign Affairs), and increasing efforts for education and media literacy. There is a public debate about the Russian hybrid threats and the Russian hybrid warfare, which is also something new. Previously, such issues did not appear in the Polish political discourse.

Conclusions

The information space of democratic societies, regularly instrumentalised by pro-Russian propaganda channels and disinformation, has become an integral instrument of foreign policy towards EU states, used by the Russian Federation. It is a part of hybrid warfare. In the coming years, Russian foreign policy will not change this set of informational and psychological influence, trying to systematically shape a negative image of EU and NATO states and institutions, and democratic institutions among UE citizens. The Russian Federation is at war not only with Ukraine, but with the whole West, so every single institution and every single actor of public discourse should take part in counteracting and fighting disinformation,

in accordance to the logic of democratization of disinformation occurring in cyberspace. Systemic solutions are needed.

Polish research related to disinformation studies does not provide an optimistic conclusion about the cyber resilience of Polish society. This challenge needs to be taken up, but, Polish society incorporates distrust of media messages into mass-produced conspiracy theories referring to new technologies, climate, health, and politics. The priority seems to be to direct society towards rational verification of content based on sources consistent with the current state of knowledge and science. But what is needed is a systemic information and media policy in schools, universities, or social campaigns, and positive communication – reduced polarization and fewer smear campaigns in public sphere. It is also necessary to coordinate efforts to systematically detect the network infrastructure of Russian accounts and the social media black market infrastructure. Perhaps it is also necessary to provide the Polish society with information about disinformation (fake news) currently promoted by the Russian propagandists, following the example of ALERT RCB in Poland.

References

Bay, S., & Reynolds, A. (2018). *Countering The Malicious Use Of Social Media. The Black Market For Social Media Manipulation.* NATO Strategic Communications Centre of Excellence. https://www.stratcomcoe.org/black-market-social-media-manipulation

Bilal, A. (2024). *Russia's hybrid war against the West.* NATO Review. https://www.nato.int/docu/review/articles/2024/04/26/russias-hybrid-war-against-the-west/index.html

Broniatowski, D.A., Jamison A.M., Qi, S., AlKulaib, L., Chen, T., Benton, A., Quinn, S.C., & Dredze, M. (2018). Weaponized health communication: Twitter bots and Russian trolls amplify the vaccine debate. *American Journal of Public Health*, *108*(10), 1378–1384.

Dąbrowska-Cydzik, J. (2023a). *„Antywojenne" hasztagi aktywne na Twitterze. „Konsolidacja środowisk radykalnych"*. Wirtualne Media. https://www.wirtualnemedia.pl/artykul/tonienaszawojna-rosja-ukraina

Dąbrowska-Cydzik, J. (2023b). *NASK wykrył prawie 1600 dezinformujących kont w mediach społecznościowych.* Wirtualne Media. https://www.wirtualnemedia.pl/artykul/nask-wykryl-prawie-1600-dezinformujacych-kont-w-mediach-spolecznosciowych

Demczuk, A. (2023). *COVID-19-Related Infodemic in Poland*. Maria Curie-Skłodowska University Press.

EUvsDisinfo. (2024). https://euvsdisinfo.eu/disinformation-cases/

Gov. (2024). *Raport zakażeń koronawirusem (SARS-CoV-2). Koronawirus: informacje i zalecenia.* https://www.gov.pl/web/koronawirus/wykaz-zarazen-koronawirusem-sars-cov-2

Institute for Strategic Dialogue. (2019). *2019 EU Elections Information Operations Analysis: Interim Briefing Paper.* https://www.isdglobal.org/isd-publications/interim-briefing-propaganda- -and-digital-campaigning-in-the-eu-elections

Islam, M.S., Sarkar, T., Khan, S.H., Kamal, A.-H.M., Hasan, S.M.M., Kabir, A., Yeasmin, D., … Seale, H. (2020). COVID-19-related infodemic and its impact on public health: A global social media analysis. *The American Journal of Tropical Medicine and Hygiene*, *103*(4), 1476–1645.

Klinger, K. (2024). *Gdyby nie ignorancja polityków i antyszczepionkowa propaganda w Polsce, na COVID-19 mogło nas umrzeć dwukrotnie mniej*. Gazeta Prawna. https://www.gazetaprawna.pl/wiadomosci/kraj/artykuly/9468266,gdyby-nie-ignorancja-politykow-i-antyszczepionkowa-propaganda-w-polsce.html

Mierzyńska, A. (2023). *Przeciwdziałanie dezinformacji w Polsce. Rekomendacje systemowe*. Forum Przeciwdziałania Dezinformacji. https://ffb.org.pl/wp-content/uploads/2023/02/Raport_Przeciwdzialanie_dezinformacji.pdf

Pawela, M. (2021). *Ujawniamy: skala rosyjskiej dezinformacji o COVID-19 w Polsce*. Fake News. https://fakenews.pl/badania/ujawniamy-skala-rosyjskiej-dezinformacji-o-covid-19-w-polsce/

Science in Poland. (2023). *Researchers investigate whether anti-vaxxers and opponents of Ukraine are in the same propaganda group*. https://scienceinpoland.pl/en/news/news%2C99396%2Cresearchers-investigate-whether-anti-vaxxers-and-opponents-ukraine-are-same

Wardle, C. (2017). *Fake news. It's complicated*. Medium Corporation, https://medium.com/1st--draft/fake-news-its-complicated-d0f773766

Volkoff, V. (1991). *Dezinformacja – oręż wojny*. Delikon.

Zadroga, M., & Wilczyńska, M. (2023). *Disinformation Landscape in Poland*. EU Disinfo Lab. https://www.disinfo.eu/wp-content/uploads/2023/12/20231203_PL_DisinfoFS.pdf

ONDŘEJ FILIPEC

PALACKÝ UNIVERSITY IN OLOMOUC

What States Shall Do (Not) to Counteract Disinformation. The Inspiration from the Czech Republic

Abstract: This article provides insight into the activities to counteract disinformation and propaganda at the state level. It provides a broader picture and experience with proposals and adopted measures in the Czech Republic. These include the introduction of strategic documents and special law addressing the issue, changes in the institutional settings, the introduction of the special coordinator, and a rather limited executive role of the state. The position of the Czech Republic in the fight against disinformation and propaganda is not unique in the European context and especially in post-Communist Central and Eastern Europe, where the effective fight against disinformation and propaganda is limited to high-level politicization of the agenda and rather a hesitant approach of the state to cooperate with the civil society to address the issue.

Keywords: disinformation; propaganda; Czech Republic; countermeasures

Introduction

The development of modern technologies and the fast growth of Internet 2.0 created vital conditions for the spread of disinformation and propaganda. This changing environment poses an urgent challenge to state governments to design tools and measures to protect liberal democracy and secure its vital functioning and development, while not compromising democratic values and suppressing freedom. A situation is usually problematic as any proposal leading to the solution shall be precisely balanced to fit democratic constitutions and respect human rights to avoid concerns of the opposition, which might be – in some cases – linked to the illiberal sphere or even anti-system forces finding support on the disinformation scene. This contribution summarizes (as of May 2024) the experience of the Czech Republic in fighting disinformation, and provides systematic measures that were

taken or abandoned. As a result, it brings valuable policy experience, which might inspire other countries in the fight against disinformation.

There are two principal research questions with exploratory character: 1) What is the Czech government doing in order to counteract disinformation and propaganda?, and 2) What were the main obstacles in introducing and implementing selected measures? Finding answers to both questions will provide valuable information about activities in the Czech Republic that may inspire what measures to introduce in other countries and what mistakes shall be avoided. For analysis, the chapters go as follows: first, the problem of disinformation in the Czech Republic is introduced, providing a broader context to the topic and presenting some important realities to be considered. The second part is dedicated to the specific measures introduced by the government of Petr Fiala, and the analysis focuses on four areas: conceptual, legal, institutional, and executive.

Methodically, the contribution may be considered as an exploratory case study, providing a better context and understanding of the policy associated with the fight against disinformation and propaganda in the Czech Republic. The period covered in the analysis corresponds with the appointment of Prime Minister Petr Fiala into office in November 2021 and ends in May 2024. Because the topic is touching the area of security and governance, three theoretical concepts were found a useful source of inspiration for creating a research design. First, the analysis focuses mainly on the societal sector, which is one of the domains associated with the Copenhagen School of Security Studies (Buzan et al., 1997). This is mainly due to the fact, that disinformation is changing the political preferences of citizens and is having an impact on their identity, loyalty, and support for democracy or its institutions. Second, the analysis focuses on the level of state and the role of central institutions. However, fight against disinformation and propaganda is not only the issue of state as other actors, including NGOs or individuals, are taking part in this struggle. Certainly, there is a space for regional administration under the level of state and international organizations, notably NATO, UN, OBSE or the EU, which are providing valuable tools and guidelines on how to fight disinformation. This perspective of broader links between various levels is close to multi-level governance (Hooghe & Marks, 2003). The analysis focuses only on the level of the state and well develops existing literature.

The analysis of the Czech environment was focused merely on the reaction of the civil society, as the response of the government was to some degree missing (Robbins, 2020; Gierło-Klimaszewska, 2019; Daniel & Eberle, 2018), or the communication channels used by the disinformers, including social network, disinformation webs or chain e-mails (Gregor & Mlejnková, 2021; Kopecký et al., 2021; Hacek & Virostkvá, 2022; Wenzel et al., 2024). Others focused on specific topics including disinformation in the Czech-Russia context (Jacuch, 2024).

Academic contributions focusing on the governmental response are still rather rare, with several noticeable examples. For example, very interesting comparative

perspectives were offered by Marek Rechtik and Miroslav Mareš, who compared Czech and Slovak approaches in the context of rational choice theory (Rechtik & Mareš, 2021). Probably, the most up-to-date analysis reflecting the systemic struggle against disinformation in Czechia is provided by Ladislav Cabada (2022) who considered Russian aggression against Ukraine and the pro-active government of Prime Minister Petr Fiala as the main drivers in the state response towards the challenge of disinformation and hybrid threats in general (Cabada, 2022). This chapter is freely developing trends and ideas mentioned in Cabada's work.

The problem of disinformation in the Czech Republic

False or fake information naturally occurs in the information environment, as a mistake in human communication. Sometimes, untrue information may provoke events with great impact, mobilize the masses, overthrow the governments, and lead to irreversible changes in societies. This is also the case of the famous Velvet Revolution of 1989 in Czechoslovakia, which significantly accelerated after one of the students – Martin Šmíd – was supposedly killed in the police attack on 17 November 1989 (Suk, 2011). The rumour around the death of a fictitious student is thought to have contributed to the end of the communist regime. The above example of misinformation is a rather rare case in which false information leads to a positive outcome. The Czech Republic has a rich negative experience with disinformation and propaganda finding fertile ground in the country, mainly due to the country's history and geopolitical position between the West and Russia, or being sort of a "grey zone" where Russia attempts to export its influence (Baqués-Quesada & Colom-Piella, 2021).

Disillusion with Communism, the fall of the Soviet Union, and the outbreak of hostilities in the disintegrating Balkans led to the political consensus in Czech foreign policy under the motto "return to Europe". While joining NATO in 1999 was considered a solution for security concerns, accession to the EU in 2004 was a milestone in political and economic integration bringing stability into a Central European region. However, at the same time, both milestones provided a natural cleavage, which was used by the opposition, including anti-system parties and pro-Russian forces, in promoting anti-EU and anti-NATO agenda. So far, Czech political institutions and democracy itself have proven resilient, defying illiberal trends in Central Europe associated mainly with Hungary and Poland, or even Slovakia. However, despite the relative stability of political institutions and the absence of some strong ideologically-based movements reflecting the national-religious conservative narrative which is the challenging idea of liberal democracy (Buben & Kouba, 2023), there are present societal segments questioning the pro-Western orientation of the country. These segments are supportive of populist ideologies, illiberal reforms or

anti-systemic turn and represent important targets for pro-Kremlin disinformation and propaganda. It is not surprising, that some segments of society have even problems to recognise the importance of the issue, which is strongly politicized (Eberle & Daniel, 2019). As a result, the society is divided.

For example, in 2023, Ipsos Agency conducted a survey (n = 1,047) that concluded that in total, 23% of Czechs are understanding information war only as a pretext of Western governments (including the Czech one) to suppress freedom of speech and unpleasant media. Moreover, 9% of Czechs claims that the information war is not relevant for the Czech Republic and 28% is not sure, whether information war is relevant for the Czech Republic or not (IPSOS, 2023). It is a sort of paradox, because disinformation in the Czech Republic is spread via approx. 40 disinformation webs, which mirror Russian pro-Kremlin webs (Stětka et al., 2021), via pro-Kremlin politicians and publicists (Břešťan, 2023) or via disinformation chain e-mails forwarded mainly among older people (Kopecký et al., 2018). Other interesting data were presented by GLOBSEC which in the survey (n = 1,000+) found that 24% of Czechs are in favor of the government, where the strong and decisive leader will not have to bother with the parliament or elections, and 20% are not satisfied with their life in Czechia (GLOBSEC, 2020). To sum up, approx. one-fourth of the population may have anti-democratic tendencies and 54% of Czechs are ready to exchange some of their rights and freedoms for better living standards or security (GLOBSEC, 2020).

The relatively dense disinformation ecosystem and illiberal segment of the society already had considerable influence on public attitudes towards the agenda of migration (e.g. relocation mechanism following the 2015/2016 migration crisis), COVID-19 and refusal of vaccination among certain groups of citizens or regularly participation in campaigns (noticeable examples are the 2018 Czech presidential elections when Miloš Zeman defeated Jiří Drahoš, who was labelled by disinformation webs as "migrant welcomer", or elections to the Chamber of Deputies in 2022 in which the Czech Pirate party lost due to disinformation that apartment owner will have to accommodate migrants). The most recent example of disinformation impact is associated with invoking a hostile attitude towards migrants from Ukraine or supporting the pro-Kremlin version of the Russian invasion of Ukraine.

To sum up, despite Czech political institutions and democracy itself have proven resilient so far, disinformation and hybrid threats pose a qualitatively significant challenge to democracy. This is mainly due to new technologies and social networks, which are designed to polarization and conflict, instead of promoting cohesion and solidarity in society (Žanony, 2023). As a result, disinformation and propaganda contribute to the erosion of democracy and endanger the political regime's character, or the regime's stability. In other words, democracy is a system built up from the bottom up and its effectiveness is inherently linked to the quality of democratic inputs. Similarly to Poland, Hungary or Slovakia, also the Czech Republic might be only one

elections far from the problem. That is why it is necessary to develop comprehensive state policy, not only to counteract disinformation and propaganda, but also to create a resilient society strengthening democracy without compromising democratic values.

Measures at the level of state

As noted by Cabada (2022), Czech disinformation ecosystem intensified its buildup after 2015 within the set of crises (mainly the annexation of Crimea and violation of the territorial integrity of Ukraine, later also, the migration crisis) and their securitization. However, until 2021, there was no political will to find a solution at the level of the state, as some persons in the executive belonged to the camp of disinformers (Cabada, 2022). The most visible example was President Miloš Zeman, who repeatedly questioned the involvement of the Russian Federation in the destabilization of Ukraine (Česká televize, 2014) even at times when Vladimir Putin admitted interference of the Russian troops in Crimea (Český rozhlas, 2014). However, even when President Zeman was replaced in 2023 with a pro-western president Petr Pavel, and the populist Prime Minister left office in 2021, the new government under the leadership of Petr Fiala struggled to pass effective measures against disinformation, which was reflected also in the public: according to the MEDIAN survey (n = 1,000), 67% of the citizens claimed that the government fights against disinformation is insufficient (ČTK, 2023).

This public mood was reflected also in the criticism of President Petr Pavel, who in the interview stressed, that "the government is not doing even the minimum to fight disinformation. The fight is frozen" (Pavel, 2024). This criticism was a relatively rare form of disagreement between the president and the government and very soon Miloš Gregor, an advisor to the Prime Minister for information literacy and fight against disinformation, replied that "to claim that the government is not doing even the minimum is too harsh and rather untrue" (Gregor, 2024). These diverging views are an interesting solution that requires further analysis, which is systematically devoted to several domains.

Conceptual measures

The initial step in the fight against disinformation and propaganda is the recognition of the threat in the strategic documents. Countries usually have national security strategies or specific strategies for particular resorts, which are followed by action plans with concrete measures and mechanisms that keep the documents updated. The reference to disinformation and propaganda is missing in the Security

strategy of the Czech Republic from 2003 and 2011, but for the first time appears in the document in 2015 as a part of the hybrid warfare (Ministry of Foreign Affairs 2015). Another important step to recognize the problem of disinformation and propaganda was the National Security Audit conducted in 2016. As noted by Rechtik and Mareš (2021), the National Security Audit assessed the preparedness of the state and for the first time linked the Russian Federation as an actor that employs disinformation campaigns (Rechtik & Mareš, 2021). This is acknowledged also in the 2017 Defence Strategy of the Czech Republic and other strategic documents, including Perspective for Defence 2035 and the Concept of the Czech Armed Forces 2030.

In response to the National Security Audit and ongoing securitization of hybrid warfare, the Government adopted a specialized strategy aimed at the hybrid threats, namely the National Strategy for Countering Hybrid Operations. Despite the absence of any mention of the words "propaganda" or "disinformation", the strategy contains an obligation to build up a system of strategic communication or to strengthen inter-resort cooperation with the aims of achieving "resilient society, resilient state, and resilient critical infrastructure; systemic and whole state approach in the Czech Republic or to achieve the ability of adequate and timely reaction" (Ministry of Defence, 2021). The strategy was followed with the Action Plan for the National Strategy for Countering Hybrid Operations, which is managed under the guardianship of the National Security Council and updated every year. Currently, the action plan contains 15 tasks with allocated responsible institutions (mainly the Ministry of Defense and the Ministry of Interior) and clear deadlines for implementing activities.

Next to the question of whether to adopt a specialized strategy, there is also a question of whether to adopt a special plan to fight disinformation and propaganda. In the Czech Republic, a special "Action Plan to Counter Disinformation" was prepared in 2022 by the team under the leadership of Michal Klíma – a Government executive. Creating the plan was a challenging issue, as the NGOs provided requirements for the plan to fit several criteria, e.g. being in line with human rights and freedom of expression, defining a variety of options, and switching off the web as a last resort option, clear criteria for such steps or strict procedure with appeals and review (Rekonstrukce státu, 2022). Drafting the plan was undermined by information leaks and after presentation, the plan was criticized, due to being incomplete, or, conversely, for going too far in some areas. The Union of Publishers criticized the plan as "false, erroneous, and harmful" (Česká unie vydavatelů, 2023). Among the main points the union criticized the lack of a clear definition of disinformation, the lack of respect for the functioning of the online environment and unclear financing of the media (Česká unie vydavatelů, 2023). As a result of criticism, the plan was abandoned. However, it is important to mention that the open letter from the Union of Publishers raised very important questions touching the very essence of freedoms and democracy, including some legal concerns.

Legal measures

The very essential dilemma is whether countries should have a legal definition of disinformation or not. Any law operating with the term "disinformation" that does not provide a proper legal definition risks being misused as the term can be interpreted differently and in a very arbitrary or selective way. On the other hand, there might be situations of disinformation, that will be not covered by the definition, due to its limited scope. Moreover, disinformation is highly diverse, and creating a definition that fully and accurately reflects the essence of disinformation is probably impossible. The Czech Republic law does not provide any legal definition of disinformation and even the proposal of the Action plan to counter disinformation did not contain any. Instead, the Czech "Act on Disinformation" focused mainly on the conditions for shutting down disinformation networks which became relevant in February 2022. In response to the Russian invasion of Ukraine, the Czech domain operator blocked eight disinformation websites spreading pro-Kremlin propaganda. This unprecedented step invoked a serious debate on the procedural questions.

Another dilemma is whether a special "Act on Disinformation" should be created with new tools and legal instruments, or whether there is no need to create such a *lex specialis*, as the instruments already exist. As mentioned earlier, the Czech Republic does not have any detailed legislation so far and for that reason mainly uses existing instruments. The Czech Penal Code is rich in disinformation-related acts, including § 184 – Defamation, § 357 – Dissemination of an alarm message, § 365 – Approval of a criminal act, § 403 – Establishment, support, and promotion of a movement aimed at suppressing human rights and freedoms, § 403a – Dissemination of work to promote a movement aimed at suppressing human rights and freedoms; § 404 – Expression of sympathy for a movement aimed at suppressing human rights and freedoms; § 405 – Denying, questioning, approving and justifying genocide, or § 407 – Endorsing an offensive war (Law no. 40/2009 Coll. Criminal Code). Despite the above-mentioned paragraphs do not fully cover the issue of disinformation, disinformers often violate some of the paragraphs as a side effect of disinformation. As a result, they might be punished for spreading disinformation in a case, where courts are open to interpreting and apply the above-mentioned paragraphs in a flexible and extensive way. As well noted by Josef Baxa, Head of Czech Supreme Administration Court, on the general purpose of jurisprudence:

> Jurisprudence should show the way to justice, show patterns of behavior according to the law and the consequences of behavior in violation of it, and be a source of knowledge of legal thinking. To be such, it must be actual, understandable, courageous, and dynamic. Judicial decision-making must not deepen the critical state of the legal environment, but to find ways out of it. To reflect the achieved development of social relations, to complete

> imperfect rules, to bridge their contradictions, to find the true meaning of the regulations used and interpreted so that the goal is achieved, and the result of the journey is the finding of justice. (Baxa, 2006)

There are several medialized examples, in which informers were sent to prison or fined. In 2022, the court sent two well-known disinformers to the prison for "hate speech" against Ukrainian refugees (Aktuálně, 2022). In 2022, a woman was sentenced to compensation of CZK 250 thousand (approx. EUR 10 thousand) for spreading fake information about the death of seniors due to vaccination (iRozhlas, 2023). In 2023, another disinformer was sentenced to prison for violating § 365 – Approval of a criminal act when expressing support for Russian aggression against Ukraine (Novinky, 2023). Also, the Czech Police are active and investigate dozens of cases in which people publicly expressed support for Russian aggression of Ukraine. To sum up, the above examples show that disinformation might be fought with existing instruments. On the other hand, the above cases represent only "the top of an iceberg". The positive outcome is that the Czech Republic has experience with similar cases and state authorities are more open to the flexible use of existing instruments to spread a clear message.

Institutional measures

Institutions are key actors in the fight against disinformation and propaganda. From the functional and administrative perspective, it is a principal question 1) whether a special position to coordinate activities is to be created or whether this task will be entrusted to an already existing position (e.g. Minister of Interior, Minister of Defense, Minister of Education, etc); and 2) whether the fight is to be managed by an existing institutional structure or by a specialized institution created for this purpose. When considering the options, it should be considered that the disinformation agenda is closely linked to hybrid warfare, which has a significant security dimension. As a result, the agenda is in practice divided into civilian and military domains, which is also the case in the Czech Republic.

As a result of the Security audit in 2016, which recognized the threat of disinformation and hybrid threats, a specialized institution was created. Since January 2017, the Centre Against Terrorism and Hybrid Threats was created. However, instead of creating new office, the Centre was a transformation of the existing department within the Ministry of Interior. The Centre does not have any executive security personnel, is not active in the public prosecution nor does it work as a security service. Instead, it is merely an analytical and communication unit, which will supply information to the Ministry of Interior, covering a wide range of threats from

migration, through extremism to terrorism and also, disinformation campaigns (Centre Against Terrorism and Hybrid Threats, 2022). Regarding disinformation, it was expected that the Centre would communicate about the most serious pieces of disinformation. To sum up, in the case of the Czech Republic, the change was merely organizational with no significant impact on the powers of the new institution. A similar situation occurs with the coordinating person.

So far there were three people tasked with combating disinformation and propaganda, usually as part of a much greater agenda, including also media literacy. The first person – the government executive – was Michal Klíma who stayed in the office for a year – between March 2022 and February 2023. As mentioned earlier, he created an ambitious plan, which faced strong criticism. His agenda was taken by the "national security advisor" Tomáš Pojar (in office from February 2022 to October 2023) who focused mainly on the security dimension of the agenda linked to foreign interference. The agenda was raised again by the "Prime Minister advisor for disinformation and media education" Miloš Gregor (in the office from October 2023) with the aim of coordinating ministries and state institutions in their activities or coordinating the private/civic sphere. Although Gregor has often been referred to as the "chief censor" in disinformation media, he put it clearly: "I have no executive powers, no budget, and no people. It may raise concern, whether I will be strong enough to change anything" (Forum 24, 2023). Similarly to the above-mentioned Centre, the powers of the advisor are very limited to informal "name and shame". Moreover, the three functions above-mentioned cannot be compared, as they had slightly different tasks, held different positions and changed relatively quickly, which indicates the high sensitivity and politicization in this sphere.

Executive measures

Finally, there is an executive dimension of the agenda, which in the Czech Republic is relatively underdeveloped. It was a team of Helena Langšádlová, the Czech Minister for Science, Research, and Innovations, who tried to conduct a kind of audit of existing activities in the field of disinformation. However, she resigned in the spring of 2024 and the efforts to improve activities were undermined.

There is a question, what could the state do to be more active and effective? The answer is partially provided in the Action Plan for the National Strategy for Countering Hybrid Operations which contains 15 tasks for state institutions, however, a more ambitious and detailed program might be created to enhance cooperation with civil society. It is possible to search for good practices in other countries, that are more advanced in fighting hostile disinformation and propaganda (e.g. Finland, Sweden or the Baltic states), support the partnership between the government,

NGOs, and private sector on a non-controversial basis, promote media literacy and resilience projects aimed at vulnerable groups, develop preventive strategic communication, or conduct training in communication focused on open-source intelligence (OSINT), media analysis, media assessment and rating, etc.

Unfortunately, as a legacy of the communist era, cooperation between state and civil society, including media, is seen in Czechia as problematic and raises concerns that it could be restricted or subjected to state control. However, in an open democratic society, the state could be a partner of the civil sector and support activities that are crucial for the development of civil society and societal resilience. Beyond the security dimension, the state could be active in activities that positively influence media literacy, civic skills, and resilience, including the anchoring of democratic values. This might be done by soft tools and methods on the field of culture or education. Because hybrid threats blur the lines between military and civilian spheres, it is necessary to approach the security of the state in relation to both domains.

Conclusions

Choosing an effective way to fight against disinformation and propaganda is a very complex issue with many questions to be answered before choosing the options. The main dichotomy is between the use and adaptation of existing institutions and instruments or deciding to create new ones. Both decisions may have considerable limits as old institutions and instruments might not be sufficient to fight disinformation powered by new media. At the same time, new instruments or institutions may simply lack legitimacy or misfit the purpose. Moreover, any change will be accompanied by protests from those, who will feel endangered by new measures, including disinformers themselves or actors gaining profits from the disinformation scene.

Due to its geographic position, history, and strong commitment to helping Ukraine, the Czech Republic is among the first-line targets of Russian hybrid warfare, and due to the high politicization of the issue and relatively dense disinformation ecosystem, including politicians in top state positions, the Czech response to disinformation and propaganda has been rather limited to individual projects. Changes at the highest levels of Czech politics, together with negative experiences with disinformation, opened a unique window of opportunity to create a complex and comprehensive approach to fighting disinformation and propaganda. Despite some attempts by the Fiala government, the potential for changes was not fully met, and the next elections may (again) close this opportunity and undermine all the achievements if populists change the agenda. Yet, the Czech experience hopefully provides inspiration to other countries, on how (not to) counteract disinformation and propaganda at the state level. After

analysing the key areas, it can be concluded that the Czech state has mainly developed analytical potential, while the executive dimension has considerable limitations, especially in relation to close coordination with the civil sector.

References

Aktuálně. (2022, October 26). *Nevěřím tomu, dělám to pro peníze, hájil se dezinformátor. Soud ho poslal do vězení*. https://shorturl.at/wDO67

Baqués-Quesada, J., & Colom-Piella, G. (2021). Russian influence in the Czech Republic as a grey zone case study. *Politics in Central Europe*, *17*(1), 29–56. https://doi.org/10.2478/pce-2021-0002

Baxa, J. (2006). *Judikatura a právní argumentace. Teoretické a praktické aspekty práce s judikaturou*. http://www.auditorium.cz/judikatura-a-pravni-argumentace.php

Břešťan, R. (2023, July 7). *Užiteční idioti Vladimíra Putina. I v Česku je jich víc než dost*. https://hlidacipes.org/uzitecni-idioti-vladimira-putina-i-v-cesku-je-jich-vic-nez-dost/

Buben, R., & Kouba, K. (2023). How Czech democracy defies the illiberal trend. *Current History*, *122*(842), 108–114. https://doi.org/10.1525/curh.2023.122.842.108

Buzan, B., Waever, O., & Wilde de, J. (1997). *Security. A New Framework for Analysis*. Lynne Rienner Publishers.

Cabada, L. (2022). Russian aggression against Ukraine as the accelerator in the systemic struggle against disinformation in Czechia. *Applied Cybersecurity & Internet Governance*, *1*(1), 1–16. https://doi.org/10.5604/01.3001.0016.0916

Centre Against Terrorism and Hybrid Threats. (2022). https://www.mvcr.cz/chh/clanek/centrum-proti-terorismu-a-hybridnim-hrozbam.aspx

Česká televise. (2014, September 4). *Bildt Zemanovi: Máte tajné služby? Zeptejte se jich na Ukrajinu!*. https://ct24.ceskatelevize.cz/clanek/svet/bildt-zemanovi-mate-tajne-sluzby-zeptejte-se-jich-na-ukrajinu-336760

Česká unie vydavatelů. (2023). *Otevřený dopis Unie vydavatelů k odmítnutí postupu přípravy a obsahu Akčního plánu pro čelení dezinformacím, který bude vládě předložen vládním zmocněncem pro oblast médií a dezinformací*. https://shorturl.at/uzIX7.

Český rozhlas. (2014, April 17). *Putin přiznal, že na Krymu působili neoznačení ruští vojáci*. https://www.irozhlas.cz/node/5925649

ČTK. (2023, July 9). *Téměř dvě třetiny Čechů míní, že vláda nedostatečně bojuje s dezinformacemi*. https://www.ceskenoviny.cz/zpravy/2388031

Daniel, J., & Eberle, J. (2018). Hybrid warriors: Transforming Czech security through the 'Russian hybrid warfare' assemblage. *Czech Sociological Review*, *54*(6), 907–932. https://doi.org/10.13060/00380288.2018.54.6.435

Eberle, J., & Daniel, J. (2019). "Putin, you suck": Affective sticking points in the Czech narrative on "Russian hybrid warfare". *Political Psychology*, *40*, 1267–1281. https://doi.org/10.1111/pops.12609

Forum 24. (2023, October 30). *Gregor: Pro boj proti dezinformacím je třeba politická vůle. Nebudu vládě radit, jak být populárnější*. https://shorturl.at/byFU3

Gierło-Klimaszewska, K. (2019). Political fact-checking in the Czech Republic on the example of demagog.cz and manipulatori.cz portals. *Mediatization Studies*, 3(1), 115–135. http://dx.doi.org/10.17951/ms.2019.3.115-135

GLOBSEC. (2020). *Voices of Central and Eastern Europe. Perceptions of democracy & governance in 10 EU countries*. https://www.globsec.org/sites/default/files/2020-06/Voices-of-Central-and-Eastern-Europe-read-version.pdf

Gregor, M. (2024, February 6). *Prezidentova kritika vlády kvůli dezinformacím je přehnaná. Předchozí vláda nedělala nic, říká premiérův poradce Gregor*. https://shorturl.at/eDEF6

Gregor, M., & Mlejnková, P. (2021). Facing disinformation: Narratives and manipulative techniques deployed in the Czech Republic. *Politics in Central Europe*, *17*(3), 541–564. https://doi.org/10.2478/pce-2021-0023

Hacek, J., & Virostková, L. (2022). Lies are all around but who are the liars? Addressing online disinformation platforms in the Czech Republic and Slovakia. In J.C. Correia, P Jerónimo, & I. Amaral (Eds.), *Disinformation Studies* (pp. 171–191). Universidade de Beira Interior.

Hooghe, L., & Marks, G. (2003). Unravelling the central state, but how? Types of multi-level governance. *American Political Science Review*, *97*(2), 233–243.

IPSOS. (2023, May 29). *S fungováním demokrace je v Česku spokojena třetina lidí, politici podle nich nenaslouchají lidem*. https://www.ipsos.com/cs-cz/s-fungovanim-demokracie-je-v-cesku-spokojena-tretina-lidi-politici-podle-nich-nenaslouchaji-lidem

iRozhlas. (2023, January 10). *Peterková je pravomocně odsouzená dezinformátorka. Musí zaplatit odškodné 250 tisíc korun*. https://www.irozhlas.cz/zpravy-domov/jana-peterkova-soud-dezinformace_2301101001_ako

Jacuch, A. (2024). Czech-Russian relations. Russian disinformation campaign. *Polish Political Science Yearbook*, *53*(1),145–166. https://doi.org/10.15804/ppsy202250

Kopecký, K., Sztkowski, R., Kožíšek M., & Kasáčková, J. (2018). *Starci na netu. Výzkumná zpráva 2018*. Univerzita Palackého v Olomouci. Centrum prevence a rizikové virtuální komunikace.

Kopecký, K., Voráč, D., Mikulcová, K., Krejčí, V., & García Gomez, G. (2021). Disinformation and its negative impact in the changing world of mass media (specifically focused on the COVID-19 pandemic in the Czech Republic). *International Journal of Library and Information Studies*, *72*(4).

Law no. 40/2009 Coll. Criminal Code, version 1.7. 2023-31.3. 2024.

Ministry of Defence. (2021). *National Strategy for Countering Hybrid Operations*.

Ministry of Foreign Affairs. (2015). *Security Strategy of the Czech Republic*. https://vlada.gov.cz/assets/ppov/brs/dokumenty/bezpecnostni-strategie-2015.pdf

Novinky. (2023, December 13). *Soud potrestal dezinformátora Netíka za výroky proti míru*. https://www.novinky.cz/clanek/krimi-soud-potrestal-dezinformatora-netika-za-vyroky-proti-miru-40454138

Pavel, P. (2024, January 29). *Vláda nedělá v boji s dezinformacemi ani to minimum, myslí si president Petr Pavel*. https://shorturl.at/fjxyG

Rechtik, M., & Mareš, M. (2021). Russian disinformation threat: Comparative case study of Czech and Slovak approaches. *Journal of Comparative Politics*, *14*(1), 4–19.

Rekonstrukce státu. (2022, April 5). *Politici chystají zákon proti dezinformacím, připravili jsme jim k tomu šest praktických doporučení*. https://www.rekonstrukcestatu.cz/archiv-novinek/politici-chystaji-zakon-proti-dezinformacim-pripravili-jsme-jim-k-tomu-sest-praktickych-doporuceni

Robbins, J.W. (2020). *The Diversity of Russia's Military Power: Five Perspectives.* CSIS.

Suk, J. (2011). The turning-point between 'totalitarianism' and 'democracy': Hypothetical outcomes to events in Czechoslovakia in 1989. *Pamięć i Sprawiedliwość*, *18*(2), 13–52. https://doi.org/10.51134/sod.2009.034

Štětka, V., Mazák, J., & Vochocová, L. (2021). "Nobody tells us what to write about": The disinformation media ecosystem and its consumers in the Czech Republic. *Javnost – The Public*, *28*(1), 90–109. https://doi.org/10.1080/13183222.2020.1841381

Wenzel, M., Stasiuk-Krajewska, K., Macková, V., & Turková, K. (2024). The penetration of Russian disinformation related to the war in Ukraine: Evidence from Poland, the Czech Republic and Slovakia. *International Political Science Review*, *45*(2), 192–208. https://doi.org/10.1177/01925121231205259

Žanony, R. (2023). *Dopaminová past. Politický mozek, digitální veřejnost, nefunkční dialog*. Mda.

TOMÁŠ KOLOMAZNÍK

METROPOLITAN UNIVERSITY IN PRAGUE

Strategic Communication (StratCom) as a Tool to Counter Disinformation. Its Advantages and Limits

Abstract: The article discusses strategic communication as one of the tools for eliminating disinformation narratives in society. The goal is to present strategic communication, especially within the Czech context. First of all, the author analyzes individual approaches in the fight against disinformation, from restrictive measures to educational activities, the development of critical thinking to strategic communication and behavioural nudging. Using specific examples, it shows the advantages and limits of individual approaches. The article presents different understandings of strategic communication, including in the context of other communication activities, such as government propaganda or communication. It also focuses on the definition of strategic communication and its other connotations. The article presents different understandings of strategic communication, including in the context of other communication activities, such as government propaganda or communication. In his analysis, the author relies not only on the experience from the Czech Republic, but also on the experience of various foreign approaches, namely the United Kingdom or France. In this context, it defines the main steps on which the strategic communication model should be built. Furthermore, it reflects on the functioning of the entire communication "ecosystem" as an essential prerequisite for the fulfillment of strategic goals. Finally, it focuses on the advantages of strategic communication in relation to the above-mentioned tools and analyzes its limits.

Keywords: strategic communication; disinformation; hybrid threats; behavioural nudging; strategic communication "ecosystem"

Introduction

Like other countries, mainly in Central and Eastern Europe, the Czech Republic faces several disinformation campaigns, especially from Russia. These campaigns intensified, especially after Russia invaded Ukraine. Recent revelations about the pro-Russian website Voice of Europe provide concrete evidence of interference

in the European Parliament elections. The Czech intelligence services uncovered a network involved in disseminating Ukrainian propaganda across Europe. They reported that politicians in the Netherlands, Belgium, Germany, France, Hungary, and Poland were paid to spread Russian propaganda. In Poland, this issue is currently under intense investigation (ČT24, 2024).

For this reason, it is necessary to take appropriate measures to eliminate disinformation campaigns and build a resilient society. The Czech Republic has already taken several steps in this regard. One of the steps was building the state's strategic communication system. In this regard, the Czech Republic has adopted several conceptual and strategic documents that elaborate on the mentioned topic. In 2021, the Czech Republic adopted a *National Strategy for Countering Hybrid Interference*. It subsequently adopted the *Action Plan for the National Strategy for Countering Hybrid Interference*. One of the Action Plan key tasks is to elaborate a draft of the state's strategic communication system, including a mechanism for the systematic coordination of relevant actors (Ministerstvo obrany České republiky, 2024).

However, the Czech government did not completely succeed in fulfilling this task. In March 2022, the Czech government appointed a government commissioner for media and disinformation. The commissioner's task was to coordinate the fight against disinformation and communicate with relevant ministers and senior staff of state administration bodies that deal with media and disinformation. He was supposed to support strategic communication in the Government Office, cooperate in the preparation of state media outputs, and recommend media through which state communication will be implemented (Úřad vlády ČR, 2022).

Neverthless, less than a year later, the position of government representative was abolished and the agenda transferred to the national security adviser. The reason for this move was, among other reasons, the preparation of a controversial law on the regulation of websites, due to which the publishers sent an open letter to Prime Minister Fiala, in which they criticized the upcoming law (Echo24, 2023). After further discussions on how to set up strategic communication, the government, after more than a year, decided to restore the position of coordinator of strategic communication of the state in May 2024 (Úřad vlády ČR, 2024).

In this context, it must be admitted that the Czech Republic is still at the beginning of the whole process. At this moment, it is tough to predict how the tasks contained in the strategic documents will be fulfilled and what specific results they will bring. However, the discussion so far shows that perception of the concept of strategic communication in the Czech Republic is very diverse.

The primary objective of this paper is to introduce various tools for disinformation elimination, each with its own set of strengths and weaknesses. Simultaneously, we will delve into the definition of strategic communication. We will show different

understandings of strategic communication in the context of other government communication activities, such as government propaganda and government PR. Finally, we will focus on highlighting its advantages and limitations in the fight against disinformation narratives. As part of the paper, we will present the issue, especially within the Czech context.

"Polycrisis" and communication crisis

In 2022, a very interesting panel discussion took place at the World Economic Forum between Melissa Fleming (Under-Secretary-General for Global Communications, United Nations), Rachel Smolkin (Senior Vice-President, Global News, CNN Digital Worldwide), and Claire Wardle (Professor, Brown University School of Public Health), which was about countering disinformation, especially in the context of the COVID-19 pandemic. During the discussion, it was said that we have reached a communication crisis in connection with the pandemic. Social media platforms have become so dominant that the spread of disinformation has already reached an extreme level. On the other hand, the state was unable to react to this situation. Representatives of international organizations, as well as representatives of individual states, were forced to communicate unpleasant information to the public and, at the same time, ask them to do things they were not comfortable with. In this context, a discussion was opened about whether we can communicate and deliver to the public topics such as vaccination, which cannot be easily communicated and explained to the public (World Economic Forum, 2023).

Subsequently, the war in Ukraine and, together with it, the energy and financial crisis moved us into a phase that we began to call "polycrisis" (World Economic Forum, 2023). The polycrisis, marked by multiple simultaneous crises, has triggered a surge in disinformation narratives. European Commission President Ursula von der Leyen highlighted the seriousness of threats like disinformation and societal polarization, pointing out that they significantly undermine our ability to address other challenges. In her special address at the World Economic Forum Annual Meeting 2024, she asserted that this is not a time for division but for rebuilding trust (Business Standard, 2024). Countering disinformation narratives is undoubtedly one of the most significant security challenges. The critical question is how prepared we are for it. Do we have practical tools to counter various disinformation campaigns? Can we eliminate their impact on society and thus prevent its polarization?

Tools to eliminate disinformation narratives

The key question remains how to eliminate disinformation in the public space. There is no simple answer to this question, and there are several approaches, each with its positives and limits. If we wanted to divide individual approaches, we could discuss several areas. The first area is restrictive and regulation measures. The second area is long-term activities, among which we can include, for example, education and the development of critical thinking. The last area is active interventions in the public information space, where we can include strategic communication or behavioral nudging. Let us briefly introduce these approaches.

Suppose we were to talk about the first area. In that case, restrictive measures undoubtedly include "turning off websites" and making platforms unavailable based on the decisions of state authorities, especially in times of crisis. For example, the Czech Republic took this step in connection with the Russian invasion of Ukraine in 2022. This step had a specific symbolism that problematic platforms were pointed out as platforms with disinformation content, but on the other hand, it aimed at provoking a discussion about freedom of speech. It subsequently triggered a wave of lawsuits between the state and the platforms. The effect of blocking problematic websites was only short-term. The platforms switched to other channels and continued their activities (Advokátní deník, 2022). It is quite obvious that this "extreme" step can be taken, especially in times of crisis, and there must be legal support for it. At the same time, it is a form of reactive measure for a specific situation.

Undoubtedly, among other, rather regulatory measures, there is currently a lot of discussion about the Digital Services Act (DSA). This legislation has a relatively wide range of regulations, one of which is the restriction of the spread of hate speech and disinformation on social networks, but in full compliance with the Charter of Fundamental Rights and Freedoms. The 17 online platforms identified by the EU must implement transparent rules and flag fake news, propaganda, and hate speech (Digital Services Act, 2024).

However, the problem remains because the DSA does not define disinformation content. Articles 34 and 35 of the DSA only refer to the obligation of online platforms to take measures against systemic risks with adverse effects on fundamental rights and civil discourse (Doupal, 2024).

While the DSA represents a significant step towards regulating disinformation narratives, hate speech, and misleading advertising on social platforms, the regulation does not define what is and what is not disinformation. Thus, the deletion of posts will be at the discretion of the specific platform, but this may cause negative reactions in connection with the suppression of freedom of speech, etc. Regulatory measures are undoubtedly important, and the DSA, in particular, is the right step.

However, these measures do not guarantee that the disseminators of disinformation narratives will not find other ways and methods.

Let us introduce the second area of tools that we could call "long-term and complex activities". Among the frequently mentioned ones is the development of critical thinking. Developing critical thinking is not a one-time task. This process entails a systematic analysis of information, recognizing its validity, evaluating arguments, and avoiding misleading content. It involves logical reasoning, integrating evidence, and cross-referencing with other sources. Additionally, critical thinking requires introspection, where individuals examine their beliefs, acknowledge mistakes, and demonstrate a willingness to correct them (Babii, 2020).

From the perspective of psychologists and scientists who examine human behavior and decision-making, critical thinking plays a relatively minor role in everyday problem-solving compared to spontaneity. Critical thinking involves rational thought, primarily engaging the conscious brain system known as System 2, which accounts for only 5% of our brain's capacity. In contrast, emotions and intuition, which control the remaining 95%, have a much larger influence. It is widely recognized that disinformation narratives often succeed because they appeal to emotions. In everyday life, people often make decisions subconsciously, following predefined patterns of behavior rather than rational thought. Factual argumentation relies on heuristic approaches, which we use when problems appear familiar and no longer require additional information. Our decisions are influenced by cognitive biases, which are mental shortcuts that typically bypass logical rules. Disinformation exploits these cognitive biases, making us susceptible to manipulation (Kahneman, 2011).

The development of critical thinking can be achieved through educational initiatives. However, implementing educational activities that encompass information and digital skills requires a significant amount of time, and the results will only become apparent after a longer period. Rationality, therefore, is not the primary factor in everyday decision-making and problem-solving. While fostering critical thinking through education is important, it does not ensure a reduction in the "consumption" of disinformation. This is because disinformation appeals more to emotions than to rationality, and emotions are central to people's daily decisions. For this reason, critical thinking undoubtedly has its reasons. However, it does not guarantee that an educated person will not believe disinformation.

Another method is fact checking. Fact-checking is closely tied to critical thinking and serves as a primary method for uncovering disinformation. While fact-checking is typically the domain of journalists, politicians, and scientists, it is unrealistic to expect the average reader to verify the accuracy of every article they read. Nonetheless, fact-checking plays a crucial role in analyzing disinformation narratives. Several platforms are dedicated to debunking these false narratives, and they should

primarily be used by journalists, politicians, scientists, and other opinion leaders who play a significant role in shaping public discourse (Bateman & Jackson, 2024).

The Czech Republic is very active in this regard. On the one hand, the Ministry of Interior department called the Center Against Hybrid Threats (https://www.mvcr.cz/chh/) regularly debunks disinformation. In addition, several institutions, numerous think tanks or non-governmental organizations operating in the Czech Republic, such as Demagog.cz or Manipulátoři.cz, seek to provide the public with correct information.

In addition to fact-checking, monitoring individual disinformation narratives and campaigns is crucial. Effective tools for this purpose have been developed, and several companies and platforms are dedicated to this task. For example, in the Czech and Slovak regions, Semantic Vision, Gerulata, and the Czech Elves platform are notable contributors.

The Central European Digital Media Observatory (CEDMO) was established in the Czech Republic. It is an independent hub dedicated to monitoring the information space in Central Europe. They publish various papers about it and organize educational activities (CEDMO, 2024). Monitoring various disinformation campaigns is inherently important, especially for devising strategies to counter disinformation narratives. Understanding the information environment and its dynamics is essential for developing an effective strategy.

The advantage of these tools is their comprehensive approach to the issue of information space, its analysis and understanding of the processes that take place around us. Critical thinking, as well as fact-checking or monitoring disinformation narratives, play a key role in building a society resilient; it gives us an accurate mirror of the situation in which we find ourselves. In the long term, they have an irreplaceable role in building civil society. The disadvantage, especially with critical thinking, is the time frame when we get results after a more extended period. In the event of a crisis, the society must act within a shorter time horizon. If we are talking about fact-checking, it also requires a certain ability of expertise and the ability to navigate the media world. For this reason, it is especially suitable for journalists, media experts or influencers.

The third area of tools could be called "active interventions" in the information and media space. These methods include, for example, prebunking. The technique began to be used by Google and is called "vaccination against disinformation". The process is based on "preemptive refutation" of disinformation narratives. Internet users are introduced to truthful information or disinformation techniques before being exposed to manipulative content online. By warning them in advance about possible errors and flaws in false claims, prebunking increases the likelihood that they will not believe media manipulations (Jigsaw, 2024). However, this is a relatively risky technique that is based on a certain manipulation, which can become the object of criticism and its user can be accused of manipulation.

Last but not least, we can include in this group strategic communication, combined with behavioral nudging. Unlike the previously mentioned methods that focus on changing individual attitudes, strategic communication and behavioral nudging emphasize altering behaviors. This distinction is particularly important in crisis situations, as it is widely understood that people rarely change their attitudes quickly, with such changes typically occurring over an extended period (Kruger & Dunning, 1999). Strategic communication, together with behavioural nudging, thus, appears as a flexible tool, especially in times of crisis when we have to take quick measures. In the next section, we will discuss how these approaches work and what their advantages are.

How to define strategic communication

As we mentioned at the beginning, strategic communication is one of the most discussed topics in the Czech Republic. In 2021, the Czech Republic adopted the *National Strategy for Countering Hybrid Interference*, followed by the *Action Plan* for this strategy. Despite these steps, debates continue on how to effectively address this issue and establish a functional system. Strategic communication is not a new concept; it has long been associated with various organizational levels. Paul A. Argenti et al. defined it as a tool to advance a company's overall strategy, thereby enhancing its position (Argenti et al., 2005). Haseeb Tariq describes strategic communication as a comprehensive process that involves understanding who the audience is, why they are being addressed, how and when to communicate with them, the format of the content, and the channels through which it should be shared. As part of communication, we should be consistent in delivering the message. The messages should be purposeful and efficiently delivered and contain targeted messages. We should also know our target audience (Arkansas State University, 2022). In the book *Information War*, Karel Řehka explores strategic communication as a sophisticated process aimed at embedding a specific message in the minds of a target audience. He emphasizes that all conveyed messages must be consistent and mutually reinforcing. This approach can ultimately influence and alter people's behavior, which is the primary objective of strategic communication (Řehka, 2017).

In the security context (Divišová, 2022), strategic communication is understood as "integrated communication". This expression acts as an umbrella term for all forms of communication focused on achieving specific goals, blending various disciplines. Strategic communication within an organization's management is distinctly different from tactical and support communication. Several communication specialists position startegic communication within social constructivism, emphasizing the pivotal role of persuasion in crafting and altering perceptions of

reality. The roots of contemporary strategic communication trace back to the early 20th century, coinciding with the evolution of media and communication technologies. Scholars affiliated with the Chicago School of Sociology in the 1920s and 1930s asserted that media and communication exert significant influence on shaping both individual and collective experiences, solidifying identities, and fostering communities (Bolt et al., 2023).

If we were to summarize the individual definitions, strategic communication is the process of delivering a message to a target group to convince them of an organization's or a social entity's strategy in general. However, what is key to understanding strategic communication is that it tries to distinguish it from other forms of political persuasion, such as election campaigns or political marketing, and government propaganda, where the purpose of this associated field is understood to be deception.

Another question is, however, defining the difference between strategic communication and propaganda. Christopher Paul, for example, analyses the difference between propaganda and strategic communication. He points out that the difference between strategic communication and propaganda often develops in the negative connotation of the term "propaganda" (Paul, 2011). Vendula Divišová highlights the potential disparity between the two terms, suggesting that the utilization of falsehoods and disinformation may pose more significant challenges on a practical level. Strategic communication, by its essence, demands a seamless alignment between words and deeds, which may not be entirely true in the case of propaganda (Divišová, 2014).

The problem of the overall debate on the difference between strategic communication and propaganda mainly lies in the unclear understanding of both terms. It always depends on how we define both concepts. However, it remains true that the wider public can be satisfied with the difference that propaganda is rather associated with negative connotations. But it is also true that there is no clear distinction between strategic communication and propaganda in academic and professional discussions. Broadly speaking, it is a set of communication activities aimed at gaining and subsequently maintaining political power. The effort is to influence people's behavior and attitudes to their political advantage (Ftorek, 2017).

To complete our list, we should not forget about another term, namely "government communication" or sometimes "government public relations". "Government communication" is another term used to describe communication activities. In this context, however, it is a matter of diverse activities, including forming relations between the government and the public, government PR, and government marketing. In essence, these activities create a positive relationship between the government and the public (Blumler, 2015).

In summary, it is evident that we can encounter different forms of communication at the government level, but there are very close links between them. However, to reach a conclusion, we can state that strategic communication basically promotes

our goals, which can be both personal and societal. In essence, this means convincing individuals of the legitimacy of our goals and efforts so that they identify with and support them. For example, we can cite a campaign to support vaccination in the context of the COVID-19 pandemic. The percentage of vaccination was closely related to the extent to which the population in individual countries was convinced of the legitimacy and rightness of this step.

What role does behavioural nudging play in strategic communication?

Behavioral science is not an entirely new phenomenon; we have often encountered it in recent decades. One area where it is used is undoubtedly communication. What can be imagined under behavioral nudging, and how can it be used within the framework of strategic communication or within the framework of communication activities as such? The nudging theory was described by Richard H. Thaler and Cass R. Sunstein in their publication *Nudge: Improving Decisions about Health, Wealth, and Happiness* (2008). Nudging is the concept of behavioral science, the goal of which is to get people to change their behavior. Nudging is one aspect of how behavioral science can be applied in the public sector.

In everyday life, people are exposed to a number of dilemmas where they have to decide how to behave. From simple decisions about whether to pay a public transport ticket to decisions about whether to save for retirement or avoid paying taxes. Nudging is thus different from other forms of instruments, which can also have a restrictive nature. We can show how behavioral nudging works with a few specific examples. In 2010, David Cameron's UK government created the Nudge Unit. The name "Nudge" is based on the above-mentioned book by Thaler and Sunstein. The Nudge department has worked on various policy areas, such as encouraging people to pay their taxes on time or increasing organ donation. Thanks to the setting of a new communication strategy using behavioral nudging, the willingness to pay taxes among the middle class increased. At the same time, the number of people who were willing to donate organs increased as well. This centre played an irreplaceable role during the COVID-19 period (Institute for Government, 2020).

France has also created a similar center called BVA Nudge Unit. Eric Singler founded this center in 2013. He belongs to the world's recognized experts in behavioral nudging. His Center played a significant role in the fight against COVID-19, in particular. But it is no secret that President Emmanuel Macron also used behavioral nudging in his presidential campaigns (Collombat, 2021).

So, how does behavioral nudging relate to strategic communication? We can say that it is a persuasive tool that can be used within the overall concept of strategic communication. Since it is not a restrictive method but a method that creates

a positive message, it can be an effective part of a strategic concept. Above all, it can be effective when communicating sensitive topics that can cause a negative reaction in society. An example can be the mentioned payment of taxes, organ donation or most definitely COVID-19 in the UK.

What are the main steps for creating a strategic communication system?

In 2022, a group of Czech experts published a policy paper in which, among other topics, they defined specific measures that the government should apply in this direction. The first point that evaluated the contribution of strategic communication was the fight against disinformation. The concept called for the fight against disinformation not to be reduced to authoritative interventions but to be seen as a long-term effort to create social resilience. The recommendation mentioned the need for a long-term and unified concept of state communication, so that campaigns are synergic and that people perceive and also accept them as a standard tool for increasing the resilience of society (*Strategická komunikace státu*, 2022).

However, the topic of strategic communication is nothing new in the Czech Republic. The National Security Audit from 2016 already mentioned the call for the creation of a strategic communication system as a tool to eliminate hostile disinformation and propaganda campaigns (Ministerstvo vnitra České republiky, 2016). The Czech Republic has not yet succeeded in creating a comprehensive system of strategic communication. In this context, let us show how such a system should look and what parts and individual steps it should consist of. The whole system should consist of several parts. The first part should contain individual process steps. The second part includes the institutional level of this process. An equally important part is the legislative and conceptual provision of the whole process, which is partially fulfilled so far, especially in the form of the already mentioned *National Strategy* and *Action Plan*. Implementing the legislative system is more demanding; we will not deal with it, as it is a complex problem that could be the subject of a separate study.

So let us look at the process level. First, we should start the planning process. The planning process must undoubtedly begin with defining a long-term but achievable goal. If we were to give a practical example from the time of COVID-19, the defined goal would be a high vaccination rate of the population or compliance with restrictive measures. Another part of our strategy is a comprehensive understanding of the current state, including the internal and external environment. This environmental analysis is key because it involves assessing how well we know our target audience, the communication space, and the relevant topics that resonate within that space. Without this knowledge, we cannot effectively use individual tools and target specific population groups.

In the following steps, we must define communication tactics for target groups we want to influence. If we were to use the example of the COVID-19 pandemic again. As part of such a sensitive event, it is necessary to choose different tools for the young and other tools for the older population, and regional differences must also be taken into account. Each social group perceives the event differently, and at the same time, this event has different effects on each group.

The next step is to define effective channels and touch points. This communication matrix, which specifies messages, media and contact points, is essential for effectiveness, considering the different impacts of the same message in different contexts. We will use different touchpoints for the younger target group and others for the older ones, and we will also use various communication channels in the regions.

The next step is the initial implementation phase or pre-implementation phase. This phase involves testing and learning, optimizing communication formats for different environments and fine-tuning the media mix for various population groups.

When we optimise the communication and media mix, we move into the full implementation phase. This phase is marked by continuous measurement of key metrics that serve as a compass that guides us to verify to what extent we have achieved the set goal. This approach, which is based on data analysis, ensures that we stay on track and make reliable and valid decisions. If metrics prove insufficient for strategic goals, adjustments are made to ensure alignment with overall goals.

If we find that all our metrics are fully functional, we enter the adaptation phase, when the entire strategic communication system begins to gradually fulfill our goals that we defined at the beginning. An important step is how we will measure the effectiveness of communication and what we will consider as success. If we were to take the COVID-19 pandemic as an example again, indicators could include, for example, the awareness of the population about the need to wear masks or the percentage of the population vaccinated.

Measuring the effectiveness of strategic communication, and communication as such, is a topic that undoubtedly provokes discussion, and there is no clear opinion on it. But how can we achieve efficiency? From our point of view, there are 4 factors that will affect our overall efficiency.

1. Scope of interventions, or reaching a broad part of the audience or our target group. Sometimes, we do not have to focus exclusively on the entire population but only on a selected group.

2. Hit frequency, which emphasizes the need for frequent and successful content delivery, is a task we all share. The point is that the frequent message repetition better reaches the audience's awareness, and your active participation in this process is vital.

3. The third factor, quality and relevant content, is key in attracting attention. Its timeliness is essential, underscoring the importance of your role in creating impactful content.

4. "Flooding the media space" is, in essence, about gaining the dominance of our communicated narratives over the narratives of disinformers (Kolomazník et al., 2024).

The need to create a strategic communication "ecosystem"

The second condition for functioning is the institutional level of strategic communication and with it the involvement of relevant entities in this process. The institutional level can be understood both in a narrower concept, which represents only state bodies and institutions, and then also in a broader concept, which, in addition to state institutions, also includes organizations and experts outside the state administration. For example, we can use the United Kingdom as inspiration. The "Government Communication Service" is usually responsible for UK strategic communication. The aim of this service is mainly to support the British government and the state institutions in the administration of professional know-how in the field of communication and public policy. The office cooperates with ministries and government agencies (Government Communication Service, 2024). The office is essentially independent and its activities are not affected by the results of elections and the change of governments. We would find a similar organizational scheme and approach to strategic communication in other countries, such as France, where an interdepartmental office coordinates individual communication activities (Service d'information du gouvernement, 2024).

The Czech Republic is starting to institutionalize the entire system after appointing a government representative. As foreign experience shows, it is necessary that the institutions that are part of this system are not directly connected to the political leadership of the ministries and operate independently because such independence also means the credibility of the entire system. Based on foreign experience and the overall nature of communication activities' functioning in society, especially with the development of digitization, social networks, and AI, it is necessary to build a complex "ecosystem". In practice, this means that the strategic communication system should not be limited only to state or government institutions but should also include other organizations or individuals outside the state apparatus. Under the above-mentioned ecosystem, we can imagine, not only state institutions, but also NGOs, universities, educational centers, influencers, journalists and communication experts. The advantage of the ecosystem is its timelessness. Most of the elements of this ecosystem are outside state institutions, thereby declaring a certain independence. The ecosystem is built upon two pillars, each with its unique role. The first pillar, know-how, is the domain of experts in communication and marketing, as well as designers and journalists, who bring their specialized skills and

knowledge. The second pillar, institutions, includes a diverse range of entities, from state organizations and institutions to non-governmental organizations, think tanks, and IT companies, each contributing to the ecosystem in their own way.

However, we must perceive the system set up in this way as a natural element of our efforts. The ecosystem cannot be institutionalized in any way. Otherwise, it can become less effective and start to give the impression that it is purpose-built to support government propaganda.

Advantages and limits of strategic communication compared to other tools

In conclusion, we should summarize the advantages and limits of strategic communication. The advantages of strategic communication undoubtedly include choosing topics to be communicated. Thus, we can raise topics we need to communicate to achieve our goals. At the same time, we can gain dominance in the information space. In this regard, strategic communication is not a reactive tool where you react to the situation and try to solve it in some way. Reactive measures are always problematic, especially in the fight against disinformation. For example, blocking problematic websites has sparked a debate about the legal basis for the move and about freedom of speech. Strategic communication thus offers a proactive tool to avoid these discussions. Compared to fake-checking methods, we avoid the "unconscious" spread of disinformation in the social space. If we were to base our campaign on fact-checking, we would essentially have to confront disinformation narratives with the correct viewpoints, and by doing so, we would actually be letting them into space. At the same time, there is a risk of cognitive dissonance, i.e. that people who believe disinformation will be further confirmed in their beliefs, which has been proven many times by various researchers.

Finally, strategic communication gives us the opportunity to build trust in the system. As we have already mentioned, from a long-term perspective, thanks to this tool, we can also communicate the key values on which the society is built, respectively on which we would like to build it.

As for the disadvantages, they undoubtedly include the "misuse" of strategic communication for government propaganda. As we have already indicated, the boundaries between strategic communication, government propaganda or government communication are very fragile. It is quite logical that every government will try to use this tool to present its achievements, but there must be a line beyond which it should not go. Along with this, control mechanisms should also be set up to prevent this. It also involves the selection of topics that should be communicated within the entire concept is also related. In this context, the agreement of a significant part of the political spectrum is necessary. In general, everyone probably agrees

on topics such as the pandemic or energy savings. Other topics, such as tax reform or the continuation and forms of support for Ukraine, are already very problematic if we mean the Czech Republic. For the functioning of the entire system, it will undoubtedly be essential to agree on the topics so that there is no situation where, for example, the opposition parties will contradict the communicated topics.

Conclusions

The states of Central and Eastern Europe are exposed to extensive disinformation campaigns and influence operations, especially by Russia. In this regard, they are logically looking for ways to counter these campaigns and eliminate their impact.

We have introduced a wide spectrum of methods and tools. Each of these approaches has its advantages but also limitations. Restrictive measures are effective, but only for a short period of time. Restrictions can be perceived as efforts to limit freedom of speech, which is a very sensitive topic, especially in the Czech Republic. Other approaches related to education and the development of critical thinking require a longer time horizon. We do not want to question critical thinking and the education system, as both are an important prerequisite for building a resilient society. On the other hand, we need more flexible tools, especially in times of crisis.

For this reason, strategic communication appears to be an effective, efficient, and comprehensive tool. It can be used not only to eliminate disinformation narratives but also to help the government communicate with citizens. At the same time, value anchoring can strengthen the democratic process. In essence, it is also a two-way process, where the state also needs feedback from citizens. However, it is essential to create a concrete system of strategic communication based on its individual pillars, which we have imagined. In the Czech Republic, as in the countries of Central and Eastern Europe, we are at the beginning of the whole process. If we were to mention the situation in the Czech Republic, many of the measures mentioned in the strategic documents have not yet been effectively implemented. At the same time, at the very beginning, we mean the year 2021, we wasted time and gave space to question the overall concept with chaotic and ill-conceived steps. Experience from, for example, the COVID-19 pandemic failed to be implemented. Time will tell how successful the Czech Republic will be in strategic communication, especially after the appointment of a new government representative.

References

Advokátní deník. (2022, September 1). *„Znepřístupňování" webů*. https://advokatnidenik.cz/2022/09/01/znepristupnovani-webu/

Argenti, P.A., Howell, R.A., & Beck, K.A. (2005). The strategic communication imperative. *MIT Sloan Management Review*, *46*(3), 83–89.

Arkansas State University. (2022, February 7). *What Is Meant by Strategic Communications?* https://degree.astate.edu/online-programs/business/masters-strategic-communications/general-focus/what-is-meant-by-strategic-communications/

Babii, A.N. (2020). *The Use of Critical Thinking against Fake News*. NORDSCI.

Bateman, J., & Jackson, D. (2024). *Countering Disinformation Effectively: An Evidence-Based Policy Guide*. Carnegie Endowment for International Peace. https://library.csi.cuny.edu/c.php?g=619342&p=4310783

Blumler, J.G. (2015). Core theories of political communication: Foundational and freshly minted. *Communication Theory*, *25*(4), 426–238. http://commres.net/wiki/_media/comt12077.pdf

Bolt, N., Stolze, M., Haiden, L., & Althuis, J. (2023). *Understanding Strategic Communications*. NATO Strategic Communications Centre of Excellence.

Business Standard. (2024, June 6). *Misinformation, polarisation limit our abilities: European Commission chief*. https://www.business-standard.com/world-news/misinformation-polarisation-limit-our-abilities-european-commission-chief-124011600583_1.html

Central European Digital Media Observatory (CEDMO). (2024). https://cedmohub.eu/

Collombat, B. (2021, June 11). *Comment le nudge a conquis la Macronie*. Radio France. https://www.radiofrance.fr/franceinter/comment-le-nudge-a-conquis-la-macronie-4585964

ČT24. (2024, March 29). *Vyšetřování ruské propagandistické sítě je velmi znepokojivé, míní nizozemský premiér*. https://ct24.ceskatelevize.cz/clanek/svet/vysetrovani-ruske-propagandisticke-site-je-velmi-znepokojive-mini-nizozemsky-premier-347658

Doupal, F. (2024, February 21). *Jaké novinky, změny a povinnosti přináší Akt o digitálních službách (DSA)?* https://www.rmol.cz/novinky/jake-novinky-zmeny-povinnosti-prinasi-akt-o-digitalnich-sluzbach-dsa

Digital Services Act. (2024, May 16). https://www.consilium.europa.eu/cs/policies/digital-services-act/

Divišová, V. (2014). Strategická komunikace v protipovstaleckých operacích NATO. *Vojenské rozhledy*, *2*. https://www.obranaastrategie.cz/cs/archiv/rocnik-2014/2-2014/clanky/strategicka-komunikace-v-protipovstaleckych-operacich-nato.html

Divišová, V. (2022). Strategická komunikace: od reaktivního boje s dezinformacemi po komplexní využití v oblasti národní bezpečnosti a obrany státu. *Vojenské rozhledy*, *2*. https://www.vojenskerozhledy.cz/kategorie-clanku/bezpecnostni-a-obranna-politika/strategicka-komunikace-oblasti-bezpecnosti

Echo 24. (2023, February 15). *Klíma končí jako vládní zmocněnec pro dezinformace. Část jeho agendy přebere Pojar*. https://www.echo24.cz/a/HYd6F/zpravy-domov-klima-konec-zmocnenec-dezinformace-agenda-prebere-pojar

Ftorek, J.B. (2017). *Manipulace a propaganda na pozadí současné informační války. 1*. Grada Publishing.

Government Communication Service. (2024). https://gcs.civilservice.gov.uk/

Institute for Government. (2020). Nudge Unit. https://www.instituteforgovernment.org.uk/article/explainer/nudge-unit

Jigsaw. (2024). *Prebunking is a technique to preempt manipulation online*. https://prebunking.withgoogle.com/how-to-prebunk/

Kahneman, D. (2011). *Thinking, Fast and Slow*. Random House.

Kolomazník, T., Rod, Z., & Sarvaš, S. (2024). *Proč věříme dezinformacím? Strategická komunikace jako možná cesta z bludného kruhu*. Kniha Zlín.

Kruger, J., & Dunning, D. (1999). Unskilled and unaware of it: How difficulties in recognizing one's own incompetence lead to inflated self-assessments. *Journal of Personality and Social Psychology*, *77*(6), 1121–1134.

Ministerstvo obrany České republiky. (2024). *České strategické dokumenty*. https://mocr.army.cz/dokumenty-a-legislativa/ceske-dokumenty-46088/

Ministerstvo vnitra České republiky. (2016). *National Security Audit*. https://www.mvcr.cz/chh/clanek/audit-narodni-bezpecnosti.aspx

Paul, Ch. (2011). *Strategic Communication: Origins, Concepts, and Current Debates*. Praeger Security International.

Řehka, K. (2017). *Informační válka*. Academia.

Service d'information du gouvernement. (2024). https://www.modernisation.gouv.fr/nos-actions/les-sciences-comportementales/sciences-comportementales-nos-projets-en-cours

Strategická komunikace státu. Policy Paper. (2022, June). www.rekonstrukcestatu.cz/download/XATrRQ/analyza-a-doporuceni-strategicka-komunikace-statu.pdf

Thaler, R.H., & Sunstein, C.R. (2008). *Nudge: Improving Decisions about Health, Wealth, and Happiness*. Penguin Books.

Úřad vlády ČR. (2022, March 24). *Novým vládním zmocněncem pro oblast médií a dezinformací se stal Michal Klíma*. https://vlada.gov.cz/cz/media-centrum/aktualne/novym-vladnim-zmocnencem-pro-oblast-medii-a-dezinformaci-se-stal-michal-klima-195260/

World Economic Forum. (2023, January 13). *We're on the brink of a 'polycrisis' – how worried should we be?* https://www.weforum.org/agenda/2023/01/polycrisis-global-risks-report-cost-of-living/

PART III

Media and Security

PIOTR CELIŃSKI

MARIA CURIE-SKŁODOWSKA UNIVERSITY, LUBLIN

Communicational Security: Between Biomedia and Biopolitics

Abstract: In this essay, the author undertakes a preliminary analysis of selected problems of communication security. Taking biomedia technologies as a starting point, he focuses on political and social ways of designing, implementing and using communication technologies that come into close contact with sensory organs and the body. Reflections on the basic conceptual categories describing communication possibilities and related to the implementation of power strategies are illustrated here through a discussion of several examples of contemporary technological solutions and social practices.

Keywords: communication; media; body; security; interface; politics

Introduction

One of the areas of contemporary security in the cultural and civic dimension is communication security. It includes the ability to express oneself and communicate with others directly and through various media, access to information and participation in communication circuits (Babik, 2018; Batorowska, 2018). The importance of this area is growing with the increasing presence of manipulation and disinformation practices (Olejnik, 2024; Rosińska, 2021), the tendency to control the information sphere in the spirit of political correctness (Aksiuto et al., 2023), the increasing presence of artificial intelligence (Amir, 2017) and radical changes in the way media are used (transition from mass media to interactive and networked media) (Mrozowski, 2020). Here I am interested in the ways in which media are used, both the user interfaces of media machines and the actions of different media users made possible by these interfaces. I believe that in this area of contemporary social practices, biopolitical and biomedia tendencies radically meet and clash with the previous status of citizen and subject. This circumstance means that both the security of communication and the social understanding of communication, media and the human person that it constitutes require analysis and comment.

Biomedia

Let us begin by specifying the conceptual categories mentioned above and pointing out the connections between them. Interfaces (a media studies category) are technical formats and, at the same time, culturally encoded rules of use for contemporary media machines. They are primarily digital and networked, i.e. they enable contact with media, information and networks of their exchange in a standardised way. These are screens, keyboards, loudspeakers, but also methods of interaction (e.g. TikTok is dominated by thumb movements, other social platforms by liking and sending). On the one hand, they offer digitised versions of all previous media (cinema, press, photography, audio). On the other hand, they enable access to information (download) as well as interaction with media and, through media, with the entire digital information ecosystem (upload) (Lunenfeld, 2011). These technologies are important because they regulate our ability to communicate in terms of access to knowledge and media use, and this is the functional basis of the modern world, which has developed technologically thanks to the fulfilment of one of the ideological postulates of the so-called digital social revolution, which was to reject the old media of propaganda and consumption and replace them with media of interaction, action and communication decentralisation (Couldry & Hepp, 2016). Ultimately, what kind of infosphere we have, both the public one and the one that remains the private experience of users, and how these users co-create and thus change the information ecosystem, depends on the form of media interfaces, the agency they offer, and the regulatory institutions behind them (technological and media platforms, system regulators) (Galloway, 2012). Old media allowed us to observe and listen to the global village, while digital and network media, at least nominally, also allow us to broadcast, i.e. to speak to the world, to show it and to contact others through media. The media formats through which we operate in the information space are not only technological solutions (smartphone, television, social platform), but also the rules of the social and political game encoded in these machines. The digital hardware and software at our disposal are controlled by their manufacturers, sellers, service providers and, ultimately, by national and international regulators. This seemingly obvious relationship has constitutional significance for interactions in the digital world. What is told and mythologised in narratives about the digital revolution as interactions and media activity/agency is only partly the independent action of the media user and the communicating social entity towards the information universe and others communicating in it. The aforementioned system regulators that format the activities have an equally important position in this system. Equally important in this system are the aforementioned system regulators, who format users' actions and determine opportunities and levels of interaction according to their interests and current policies. In the language of media studies, we can

do as much with digital media as the openness of the tools and options available to us in their technical menus allow (Manovich, 2003). Above all, however, those who control interfaces and information systems aggregate and analyse the knowledge that emerges from the traces of users' actions, who carry out most of their actions on controlled platforms and thus not only act but also leave precise traces of their actions. Interactivity has its price: we pay for the possibility of multidirectional action with different actors of network exchange by generating traces of our activity, which form personality, cultural and social patterns and become the subject of market and political games (Markus, 1987). Such a system of interaction opens up a number of possibilities for its regulators. I am particularly interested in one of them, which manifests itself in the form of biomedia and the biomediation they make possible (Thacker, 2004; Ogonowska, 2021). This concerns the media formats of interface technologies, as well as the mechanisms of controlling social interactions, which consist in implementing into social circulation and controlling the functionality of interactive media devices that come into close contact with the bodies (primarily the sensory organs and cognitive mechanisms) of subjects. Biomedia plug into the connections of the nervous system (as is the case with modern neural interfaces), expand the possibilities or replace individual members and organs (artificial eyes, ears, prosthetic limbs), map or regulate the work of individual internal organs (bionic cameras, stimulators, bypasses). Biomedicine offers the possibility of directly addressing individual organs and rules of perception, thus testing the subject's perception, which consists firstly in the physical separation of individual cognitive channels and experiences, and secondly in the possibility of bypassing the awareness of perception as a condition of connection with the external environment. For example, a subject using an artificial bionic eye connected to the optic nerve and the brain may be able to internalise the visual signals thus obtained to such an extent that they become his native experience, which over time becomes a natural perceptual and cognitive scheme. Various prostheses, stimulators and bionic organs work in a similar way. They replace inefficient organic equivalents and nestle into the bodies and modes of action of their subjects. In the situation of their implantation, cognitive distance is reduced or even eliminated, as is their awareness of the presence of the medium and nature of its mediation. The flow of signals between the senses and the people who carry them is not predetermined or even controlled by the traditional physiological, cognitive and behavioral schemes. The regulators of interaction behind biomedia use them to bypass and invalidate the previous rules of communication exchange, conscious presence and autonomy of action. Traditional media, as well as earlier digital media, addressed entities holistically – they referred simultaneously to a person's senses, cognitive mechanisms and intellectual processes, even if the main cognitive channel they used was images, sounds or text. The creators of biomedia will offer "intuitive" and effective interactions with the external world, consisting

of the automated translation of "thoughts" into interface responses and the agency of these actions in specific situations, but in return they will gain insight into the ways of "thinking" and "acting". The knowledge resulting from such insight is the "oil", "gold", "lithium" of our time.

I will not go into a number of details, both in terms of definition and in terms of the current and future possibilities of this type of media technology. I am only interested in pointing out these new formats of biomediation and their communicative possibilities, because their presence has a key causal potential in the context of the titular communication and civic security. Biomedia is a category that concerns both biocommunication and biopower. Interactions that take place at the level of the body and consist of the use of organs and senses separated from subjectivity are a politically interesting situation. The systemic actors of games around bodies and their communicative capacities are well aware of the potential of biopower and biocontrol that they can materialise with the help of biomedia. Whereas previous analogue and digital media sought to "govern souls" by attempting to influence the state of knowledge and beliefs of their recipients (hence the accusation of ideological manipulation of public opinion, propaganda), biomedia first maps organisms and then begins to manage them completely physiologically. This is a shift that I would initially define, using the language of media studies, as a transition from symbolic communication to biocommunication. In symbolic communication, symbols, signs, narratives and the media themselves remained outside the body, perceived and processed by an autonomous subject. In the case of biomedia communication, stimuli are replaced by signals and exchanges that take place despite skin and organs, despite will and intellect – the media "communicate" electrically or chemically with individual organs, address the senses, bypassing the holistic cognitive strategies of the human being. The subject, and therefore the citizen and the person, is thus reduced to bodily resources that can be separated from his subjectivity and identity. This comes as no surprise to the discourse on society, communication and politics, which has been recognising and attempting to name such practices for several hundred years. Thomas Hobbes, in the figure of Leviathan (Hobbes, 1651), already articulated the idea of the state as a body composed of the bodies of its subjects, which only has a chance of survival within a centralised social structure and thanks to the political power at its head. In his influential and controversial theory of biopolitics, Michel Foucault (2011), summarising the rules of power in the modern world, identifies the control of bodies and their disciplining as the main mechanism of social life. Earlier, Julien Offray de la Mettrie (1747), reacting to the technological revolution and modern rationalism, conceptualised the human body as a machine that works best when it is plugged into the technological system of society. After the madness of the Second World War, these overly utopian visions were corrected by cyborg narratives. In these, the figure of the cyborg meant the

opening up of organisms to hybrid connections with technology and, as a result, physical emancipation from oppressive social systems (Haraway, 2003). However, from the critical perspective of media and media culture analysis, we can say that, after an only partially successful strategy of managing social moods and imagination with the help of traditional media (propaganda, mass culture), political power is beginning to invest in the old idea of biopower with the help of biomedia, based on the latest forms of communication.

Moreover, before our very eyes, this field of political practices is becoming a site of geopolitical rivalry, one of the new registers of the global arms race and technological superiority. The goal of this race today is as follows: whoever gains an advantage in understanding the complexity of the human organism (i.e. in its medial connection and mapping) and in designing and implementing tools for the remote management of organisms (the aforementioned biomedia interfaces) will gain real tools of biopower and biopolitical advantage over the rest. Whoever is the first to "land" on the skin and get inside the body and the subject, whoever is the first to map and use the resources inside, will be the first to reach the organic "Eldorado". After landing on the moon and in the depths of the ocean, organic matter in all its complexity remains a field for exploration and then for colonisation and domination. For such discoveries and conquests to be possible, appropriate media and communication protocols are needed, and this is where biopolitics meets biomedia and biocommunication. Let us illustrate these abstract considerations of far-reaching and complex social and geopolitical strategies with examples of current social practices and technological solutions at the interface of biomedia, bio-power and communication security.

Interface with the brain

The "holy grail" of techno-political solutions in the field of biomedia are neural interfaces (Celiński, 2010). In their case, the aim is to create tools that connect the human brain directly to information systems. Both state actors and large corporations with global reach are involved in their creation. The creation of a sufficiently efficient and effective device of this kind will be reflected in medical or biotechnological achievements and in many other fields, but let us focus on the possibilities of bio-communication and bio-power in this area. For example, Neuralink (Neuralink – Pioneering Brain Computer Interfaces), a company run by Elon Musk, is working on neurointerface solutions. This is a figure whose political and economic connections are no secret, nor are the company's objectives. They are as follows: 1) understand how the brain works; 2) build an interface to the brain; 3) start engineering the brain. This is probably the most essential and clearest indication of the

possibilities of combining media practices and biopolitical potential. First, to use all available media to precisely map and index the brain, to make a map of it, similar to the actions that allowed the mapping and codification of the human genome in the post-war decades, to make a map of the world in the formula of Google Earth, or even a precise index of social relations that social platforms, led by Facebook, are working on. The medial view of the brain means scanning it with technologies derived from the tools developed by Roentgen, but also advanced visualisations using microscopes or spectral scanners. At this stage, we are able to capture the jumps of single electrons between synapses and have almost the same level of knowledge about the functionality of individual brain elements, so we can say that a detailed map of the brain already exists, and only its final resolution remains an open question. Even if we consider today's accuracy to be relatively low, i.e. not providing sufficient knowledge about individual neurons and synapses, we can expect with a high degree of probability that a process will occur here that characterises the history of digital tools in general. Over the years, their resolution has increased and their energy consumption has decreased, as in the case of digital images, which have gone from a volume of a few hundred pixels to mega and terapixels. The project of mapping the human brain applies both the cultural framework of thinking about media and media optics, which have become referential representations of reality, and digital ways of working with the knowledge thus obtained, which is collected in databases thanks to interfaces and processed algorithmically. We are moving towards digital models (representations and simulations) of brains and tools for analytical work within them. When it comes to creating an interface with the brain, the company can boast of the first prototypes implanted in patients, which have proved to fulfil the hopes placed in them, both in terms of "reading" the brain and "writing" it. Sensors implanted in the form of a subcranial implant are able to detect the desired electrical activity of the brain and transmit the data generated to the outside, where they are digitally processed to provide an insight into the functioning of the organ. Micropulse electrical emitters, which, in addition to the sensors, make up the contents of the device, can effectively stimulate tissues and centres electrically, forcing them to perform specific activities. Finally, there is the question of neural engineering, which is the ultimate goal of this and other similar business and political projects. Here, cooperation between global economic and political actors is arranged according to converging interests and needs. During the presidency of Barack Obama, the United States announced through his mouth the funding and launch of one of the largest multi-year government research and implementation programmes dedicated to mapping the nervous system and building technical connections to it, under the name of the Brain Initiative (The BRAIN Initiative | The White House). The beneficiaries of this programme are, of course, mainly large American companies in the fields of biotechnology, medicine and information technology, and the

involvement of gigantic public funds shows that this issue is treated as a priority by the world power and leader in cybernetic and biotechnological progress. It is hard not to succumb to the temptation of projection here, which suggests that since such technological solutions are funded with government money and are intended for military purposes, they will eventually turn out to be a military resource and a resource related to the maintenance of political power at the disposal of those who fund them. The history of American entrepreneurship in the broad field of IT makes such a scenario likely to the point of certainty. And although this is not the place for geopolitical considerations, I will only mention that other important actors in the global game for power and control are working on their own solutions in this area, using similar intersectoral patterns (SCIO, 2023). As I mentioned earlier, the race to map the brain and the ability to "inform" it is one of the courses of global technological competition, one of the faces of the arms race.

Havana Syndrome

Of course, biomediation and the biopower it implements are not limited to the race to develop and apply neural interfaces that connect the human brain to the external environment. Many media technologies are already in use in social and political practice, interfering with the human body, extracting data from it and establishing formats of interaction within it.

Among the simplest, but already relatively widespread, are tools and systems used by law enforcement agencies around the world to scan faces and biosignatures such as fingerprints or iris patterns, to collect, store and process DNA information, to record the thermal signatures of organisms, or to pacify protesters by emitting incapacitating infrasound. Each of these, and many other similar media technologies, could receive a great deal of attention, but since this text is in the context of international security issues, I will focus on one case of the use of audio technologies. This is the case of the use of high-intensity radio-microwave emitters, which led to a series of symptoms of illness in American diplomats and security personnel – a case that the media have dubbed the "Havana Syndrome" (Corera, 2021). Here we have both an expansion of the possibilities for media technologies to affect individuals and an international conflict between superpowers, which is also evidence of the testing of unconventional technical solutions. Like a lens, in this particular case many dimensions of biomediation and bio-power are focused. Firstly, we have modified traditional media technologies, i.e. the phenomenon of waves of a certain frequency and intensity, which we normally use to transmit audiovisual signals. Keeping the original media concept, but under the conditions of increasing the strength and precision of the impulses sent in this way, it turns out that it

is possible to knock a person out of their physiological and intellectual well-being. Those who were irradiated in this way complained of numbing headaches, difficulties in maintaining balance and impaired cognitive functions. In this way, the state of the subject was affected, bypassing his or her ability to perceive and react – and also to doubt the nature of the event, since it could not be properly categorised legally. Although a person is the ultimate subject of law (and its creator), it must be admitted that in the legal field there is no unambiguous interpretation of his nature as a subject of law, as a subject of cultural and communicative events. The international consequences of this event are difficult to assess. Some do not admit to possessing or using such tools. Others play down the impact and are reluctant to admit publicly that they have been victims of their use and to comment on these events. In the background, there is a high stake in making the whole event (this and similar ones) public. If public opinion and influential actors were to begin a real exchange of arguments and the formulation of positions on this issue, it would become clear that legal and systemic solutions are not only unprepared to deal with this problem, but most likely deliberately maintain the "grey" status of such events and procedures. They are reluctant to recognise the physical interference mediated by such communication machines as a legal event. Police and law enforcement agencies around the world use similar solutions to pacify gatherings (Long Range Acoustic Device – LRAD technology), military drones kill people, and it is difficult to legally identify and punish those personally responsible for such deaths. It is strategically profitable for states and their subcontractors, i.e. the military sector, public security and, broadly speaking, IT and biotechnology, to maintain this state of affairs. In this perspective, bodies are treated separately from subjects, separately from consciousness, will and agency – but that is a topic for separate considerations.

Morphological freedom

At the same time, even the state of affairs just suggested does not explain the complex relations between bodies, subjects and media well enough. The strategy of biopolitics, for which corporeality is the arena of technological races and international games, is only one of the faces of social relations in this field. The other, which I would like to mention here for the sake of contrast, was developed in the spirit of the dualistic tradition of the Enlightenment, which made the Cartesian distinction between body and mind the driving force of emancipatory thinking for technologically advanced Western societies. Descartes, the aforementioned De La Metrie, who understood the body as a machine, and finally American technoptimist feminists such as Donna Haraway, are the authors of the idea and the inspirers of the activism that followed, from which the cult of the cyborg emerged – a figure promising

technological liberation and fulfilment for an identity imprisoned in the body, and thus in the oppressive, traditional system of social and cultural norms and prohibitions. As is well known, emancipatory discourses and activities are well established in Western culture and prove to be a highly attractive narrative platform. For many inhabitants of the Western world, the cyborg imagination is synonymous with the most promising format of development and fulfilment. Among the many techno-optimistic and techno-utopian narratives that exploit these assumptions, I choose for further analysis the movement that calls itself Morphological Freedom. Social activists, including researchers, educators, celebrities and politicians who identify with it more or less directly, focus on transhumanist solutions: a radical extension of the right to one's own body, consisting in the possibility of using medical and technological solutions to modify one's own body according to one's own desires, possibilities and imagination. A more or less advanced cyborg (because there is no question about the degree of mechanical or chemical intervention in the body) is the most promising formula for liberation from the reach of traditional power and political control, and a promise of fulfilment in escaping organic, physiological (including sexual) limitations. The morphological freedom movement is a commitment to the values, positions and social readability of the widest possible diversity of physiologies, biotechnological-logical hybridisations, morphologies and lifestyles (Sandberg, 2013; Lindenmeyer, 2017). Let us examine the practice of transhumanist ideas in the projects of famous media artists. The cyborgisation of the body, understood as the exploitation of its medial extensions and connections to external information systems, is also an area of enormous involvement for media art, which has provided the transhumanist imagination with ready-made metaphors and models of action over the last few decades. In this context, it is enough to recall the works of the Australian artist Stelarc, who made the slogan of the extended body one of the main motifs of his artistic activity (Fernández, 2023; Atzori & Woolford, 1995). In this vein, he experimented with exoskeletons that allowed the body to move by means of a robotic skeleton, audiovisual transmissions from inside the body using specially designed cameras, microphones and sensors, organ displacement and the reorganisation of the senses.

Conclusions

Media technologies, practices of political power and social imaginaries constructed around the idea of cybrotic emancipation are a nexus at the centre of which are practices of biocommunication. They involve increasingly advanced (smaller, more efficient and closer to the body and the senses) biomedia. Their current use is regulated, on the one hand, by the agency of traditional political actors, both in

the international dimension in the form of biotechnological rivalry between states and supranational organisations, and in the internal dimension related to social and communication control within states, and, on the other hand, by social actors who, according to their own convictions and ideas, seek to contest the dominance of the power apparatus, but also to emancipate themselves socially and culturally by using biotechnological possibilities in a radical way, opening bodies to information flows and technophysiological changes.

It is impossible at this stage to assess the actual agency of both sides, the effects of global competition in the field of biocommunication and the implementation of such solutions in politics. There is no doubt, however, that the question of the ability to communicate through media, the integrity and communicative agency associated with their attachment to bodies and the transmission of their representations, and the extension/alteration of their physiology and perception, are areas of social practice that cannot be ignored in analyses of the issue of communication security. Since we have organs and bodies that are detached from persons and addressed from the perspective of biomedia, access to media and the possibility of using them are not the only values of this type of security. From a civic and "human" point of view, the possibility of limiting the access of media and transmissions to bodies and senses seems equally, if not more, important. We are safe when we can autonomously, i.e. with cognitive and neural distance, apply to reality the possibilities of perception, cognitive patterns, intellectual efficiency and social imagination that we co-create.

References

Aksiuto, K., Pomarański, M., & Wallner, M. (2023). *Poprawność polityczna. Źródła, przejawy, kontrowersje*. Wyd. UMCS.

Amir, H. (2017). *The Sentient Machine: The Coming Age of Artificial Intelligence*. Profile Books.

Atzori, P., & Woolford, K. (1995, September 6). *Extended-Body: Interview with Stelarc*. journals.uvic.ca/index.php/ctheory/article/view/14658

Babik, W. (2018). Bezpieczeństwo informacji wyzwaniem dla bezpieczeństwa lokalnego. In A. Filipek & D. Krzewniak (Eds.), *Elementy teorii i praktyki transdyscyplinarnych badań problemów bezpieczeństwa*, t. 7: *Teoretyczne i formalne aspekty bezpieczeństwa w wymiarze lokalnym*. Wyd. Uniwersytetu Przyrodniczo-Humanistycznego.

Batorowska, H. (2018). Bezpieczeństwo informacyjne. In O. Wasiuta, R. Klepka, & R. Kopeć (Eds.), *Vademecum bezpieczeństwa*. Instytut Nauk o Bezpieczeństwie Uniwersytetu Pedagogicznego w Krakowie.

Celiński, P. (2010). *Interfejsy. Cyfrowe technologie w komunikowaniu*. Wyd. UW.

Corera, B.G. (2021, September 8). *'Havana syndrome ' and the mystery of the microwaves*. BBC. https://www.bbc.com/news/world-58396698

Couldry, N., & Hepp, A. (2016). *The Mediated Construction of Reality*. Wiley.

Fernández, C.R. (2023, February 23). *Stelarc – making art out of the human body*. Labiotech.eu. www.labiotech.eu/trends-news/stelarc-ear-art-human-body/

Foucault, M. (2011). *Narodziny biopolityki*. PWN.

Galloway, A. (2012). *The Interface Effect*. Polity Press.

Haraway, D. (2003). Manifest cyborgów. *Przegląd Filozoficzno-Literacki*, *1*(3), 49–87. www.academia.edu/40925328/Donna_Haraway_Manifest_Cyborg%C3%B3w

Hobbes, T. (1651). *Lewiatan*. Europa.

Lindenmeyer, C. (Ed.). (2017). *L'humain et ses prothèses*. CNRS Éditions. https://doi.org/10.4000/books.editionscnrs.29652

Lunenfeld, P. (2011). *The Secret War Between Downloading and Uploading. Tales of the Computer as Culture Machine*. MIT Press.

Manovich, L. (2003). New Media from Borges to HTML. In N. Wardrip-Fruin & N. Montfort (Eds.), *The New Media Reader*. MIT Press.

Markus, M.L. (1987). Toward a "critical mass" theory of interactive media: Universal access, interdependence and diffusion. *Communication Research*, *14*(5), 491–511. https://doi.org/10.1177/009365087014005003

Mettrie de la, J.O. (1747). *Człowiek maszyna*. Europa.

Mrozowski, M. (2020). *Przenikanie mediów. Ewolucja mediów a przemiany ładu społecznego* PWN.

Ogonowska, A. (2021). Media ucieleśnione. (Nowe) konteksty badawcze w relacjach media – ciało. *Annales Universitatis Paedagogicae Cracoviensis | Studia De Cultura*, *13*(1), 36–54. https://doi.org/10.24917/20837275.13.1.3

Olejnik, Ł. (2024). *Propaganda. Od dezinformacji i wpływu do operacji i wojny informacyjnej*. PWN.

Rosińska, K. (2021). *Fake news. Geneza, istota, przeciwdziałanie*. PWN.

Sandberg, A. (2013). Morphological freedom – why we not just want it, but need it. In M. More & N. Vita-More (Eds.), *The Transhumanist Reader* (pp. 56–64). John Wiley & Sons. https://doi.org/10.1002/9781118555927.ch5

Thacker, E. (2004). *Biomedia*. University of Minnesota Press.

The State Council Information Office of China (SCIO). (2023). *Report: China emerges as brain-computer interface technology innovation hub*. english.scio.gov.cn/chinavoices/2023-06/01/content_86028414.htm

DANIEL ŠÁROVEC

METROPOLITAN UNIVERSITY PRAGUE

TikTok as a Security Threat? A Challenge for Political Actors in the Czech Republic

Abstract: The phenomenon of digitalization naturally also affects the functioning and decision-making of political actors. In recent years, even the Chinese social network TikTok has experienced an unprecedented rise among all social networks. Although there are opinions that TikTok *de facto* devalues politics, political actors have a completely different attitude towards it. This chapter focuses on TikTok from a security perspective. It follows from the reactions of several state authorities that this application poses a particular risk that must be dealt with. Despite many debates and warnings about the specific security shortcomings of this application, there are a number of political parties and politicians themselves who use this application as an effective means of communicating with young voters or first-time voters. Therefore, the question arises whether it is appropriate to choose the path of partial bans and restrictions of this application or whether the choice should be left to the user himself.

Keywords: Central Europe; communication; Czech Republic; China; NÚKIB; security; political parties; TikTok

Introduction

Over the past several decades, the patterns of functioning of political actors in the digital era have become a highly important and relevant area of social research in fields like political science, international relations, and security studies. The gradual development of the online environment has been accompanied by novel and ever-broader possibilities for political actors' online behaviour (Macková, 2017; Barberà et al., 2021; Šárovec, 2022a). The rise and development of social media marked a new chapter and an additional dimension of focus for this research.

The following chapter deals with an important contemporary phenomenon, the TikTok social media platform. It is characterized by a practically infinite amount of available content. Any TikTok user can become a video creator and obtain likes or

other interactions, as the app is easy and very intuitive to use. From the app's launch, its developers have targeted teenage users and the young generation in general. The platform makes it easy for users to express themselves creatively.

However, its unique features and benefits are accompanied by certain risks. Leaving aside the potential negative effects on users' mental health, we are going to deal with the frequently mentioned threats of user data collection and the spread of disinformation or other inappropriate content (see Czarnecki, 2023). Those threats have driven the decisions by many governments or other institutions to impose penalties, restrictions, or outright bans on the platform. We are going to start with a basic outline of the beginnings and characteristics of TikTok.

Then we will discuss the positions taken by actors in the EU and beyond. Special attention will be paid to the positions of Czech authorities and political actors. This is because despite all the risks identified and restrictions taken, parties and their candidates are among the main actors who still see a great potential in TikTok, and they do not shy from recruiting new voters through it.

TikTok as an online communication phenomenon

TikTok is certainly one of the most frequently used social media platforms nowadays. Developed by the Chinese company ByteDance, it primarily serves to create and publish videos, or to simply watch other users' videos. Typically used as a smartphone app,[1] it can also be controlled through a web browser. TikTok's top content creators have followings in the order of hundreds of millions.[2] Ordinary users follow not only popular influencers but also their friends and acquaintances. The official mission of TikTok is defined as follows:

> TikTok is the leading destination for short-form mobile video. Our mission is to inspire creativity and bring joy. TikTok's global headquarters are in Los Angeles and Singapore, and its offices include New York, London, Dublin, Paris, Berlin, Dubai, Jakarta, Seoul, and Tokyo. (TikTok, 2024a)

TikTok is available in over 160 countries and 75 languages. In China, the app was launched as Douyin in 2016 and soon became "the major money spinner for ByteDance". While they are highly similar apps, TikTok and Douyin support different network protocols because Douyin is designed to comply with China's regulations

[1] Available on the App Store and Google Play.

[2] Khabane "Khaby" Lame of Italy is considered the most-followed TikTok creator. Known for his videos about the bizarreness of complicated "life hack" videos (Karimi, 2022), he is currently followed by more than 162 million users (Tiktok, 2024b).

in general and its censorship policies in particular. "In 2017, the privately-owned tech company bought a US-based video startup and released TikTok as the overseas version of Douyin. It also bought popular lip-syncing app musical.ly, and moved those users onto TikTok in 2018" (Yeung & Wang, 2023; Fu & Wakakbayashi, 2024).

According to Demandsage company, TikTok has "2.05 billion registered users worldwide in 2024", including "1.56 billion monthly active users". Its users "spend 58 minutes and 24 seconds on the app daily as of 2024"[3] (Demandsage, 2024). "As of April 2024, Indonesia was the country with the largest TikTok audience by far, with almost 127.5 million users engaging with this platform. The United States followed, with around 121.5 million TikTok users. Brazil came in third, with almost 101.8 million users on TikTok" (Statista, 2024).

Moving on to Figure 1 on the evolution of registered user counts from 2018, there has been a remarkable, several-fold increase in the number of users.

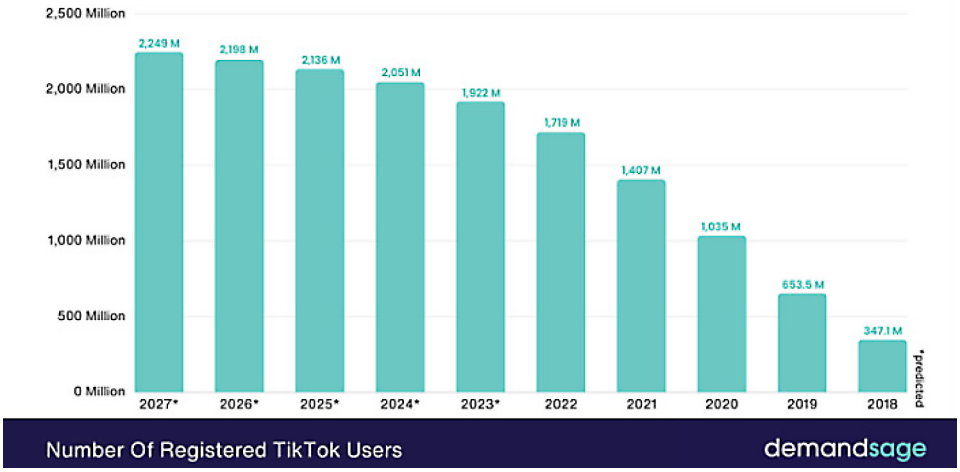

Figure 1. Number of registered TikTok users

Source: (Demandsage, 2024).

Despite the immense global success of TikTok, many have been highly critical of the background of its functioning. Since Chinese government maintains a relatively strict control over private companies, the question is how much it controls ByteDance, the app's algorithm, and the user data processed by the company. Even though TikTok and ByteDance have repeatedly denied such allegations, these

[3] To compare that to the previous year, "TikTok users spent totally 55 minutes and 28 seconds on the platform in 2023". That shows "an increase of 2 minutes and 36 seconds in TikTok usage per day" (Demandsage, 2024).

questions have not been clarified (Forbes, 2024). And the debate continues on whether TikTok is appropriate and safe to use.

The proponents of (carefully) using TikTok argue that it is full of young people, an interesting voter category that cannot be let slip away. And since numerous populists and extremists operate on the platform, the argument goes that one should not leave TikTok users at their mercy. Similar arguments have been presented with regard to fighting disinformation and deep fake videos (E15, 2024). Yet it is difficult to prove empirically whether or not the advantages outweigh the risks.

A central fact often mentioned in the debate is that ByteDance operations are governed by Chinese laws. Under the National Security Law of 2015, all Chinese citizens and organizations are subject to the vaguely defined obligation to provide support and assistance to government authorities in matters of national security. The National Intelligence Law of 2017 compels all citizens and organizations to support national intelligence activities. The Counter-Espionage Law of 2014 imposes an obligation to assist law enforcement and disclose information about the foreign clients of Chinese companies if they are suspected of espionage, whereas Chinese authorities can interpret the term "espionage" as a broad array of activities, including ones conducted outside China.[4] Finally, the Company Law of 2013 authorizes the Communist Party of China to intervene in the operations of private corporations. Even this short list of legal rules clearly substantiates legitimate concerns that China's interests "may be placed above the interests of technology users of companies subject to the [Chinese] legal environment" (Nukib.gov, 2023). And this gives rise to additional questions about the ways TikTok processes sensitive data.

On this matter, TikTok's operator has publicly stated that while the data of European users are being stored in the U.S. and Singapore, they can be remotely accessed by certain entities based in China, but also Brazil, Malaysia, the Philippines, and the above-mentioned U.S. and Singapore (Nukib.gov, 2023). Precisely these European and non-European security aspects have been highly scrutinized and debated. Moreover, many governments have taken clear positions on the subject.

Insight in EU and non-EU security aspects

The European Network and Information Security Agency (ENISA)[5] has defined a social network as "an online community that allows people, through a built-up profile, to meet, communicate, keep in touch, share pictures and videos with other

[4] Implementation of these laws is not subject to independent judicial review (Nukib.gov, 2023).

[5] ENISA is "dedicated to achieving a high common level of cybersecurity across Europe" (ENISA, 2024).

community members with whom a connection is shared" (ENISA, 2010). Even if the definition precedes the emergence of TikTok, it clearly covers the platform in question. More important than the theoretical background was the assessment of actual threats that may be associated with TikTok.

At the EU level, as many as three institutions have banned TikTok on staff devices based on known security threats: the European Parliament, the European Commission and the Council of the European Union. This was accompanied by a "strong recommendation" that members of the European Parliament remove the app from their personal devices as well. In addition, a number of EU member states have instituted, mostly in the years 2022–2024, various restrictions on TikTok use, typically on government-issued or staff devices. Those include Estonia, France, the Netherlands, Belgium, Denmark, and others (Euronews, 2024).

Similarly, the IT systems of the Slovak parliament started blocking the China-based app from staff devices in 2023. And in the same year, Poland's Digitization Council "expressed a positive opinion" on removing TikTok from the "work phones of public administration officials and employees". Among the non-EU countries applying measures against the platform are Norway and Turkey, among others. In March 2023, Turkish authorities fined TikTok TRY 1.75 m for insufficient protection of user data. Outside Europe, restrictions in response to the risks of TikTok have been implemented by India, Taiwan, and others (Fišer, 2023; Vilček & Fišer, 2023; Reuters, 2023; Euronews, 2024).

In April 2023, Australia banned the app from federal government devices, thus, joining "the so-called Five Eyes (FVEY) intelligence-sharing partners (the United States, Canada, Great Britain and New Zealand) which have taken similar steps". This decision went hand-in-hand with the concern of Western governments that "TikTok poses risks to cybersecurity and data privacy, and that the app could be used to promote pro-Beijing narratives and misinformation" (Apnews, 2023).

In February 2024, the European Commission decided to open formal proceedings against TikTok under the Digital Services Act[6] (European Commission, 2024a). And although US President Joe Biden signed a law potentially banning TikTok in the country, his campaign is still embracing the platform and working with TikTok influencers (Apnews, 2024). Despite all measures taken, the attitudes of European as well as US politicians may appear somewhat paradoxical. Indeed, even French President Emmanuel Macron or PM Giorgia Meloni of Italy have their TikTok accounts (E15, 2024), suggesting they are not only challenging the restrictions

[6] The Digital Services Act (DSA) aims to regulate "online intermediaries and platforms such as marketplaces, social networks, content-sharing platforms, app stores, and online travel and accommodation platforms". Its crucial goal is "to prevent illegal and harmful activities online and the spread of disinformation. It ensures user safety, protects fundamental rights, and creates a fair and open online platform environment" (European Commission, 2024b).

against the platform implemented thus far but also, more importantly, prioritizing the recruitment of new voter segments despite the risks.

Apparently, there has been not only a global debate about the risks of using TikTok but also a series of various concrete measures taken by public authorities, mostly with identical motivations and highly similar justifications. Naturally, this debate in EU and non-EU countries alike has been reflected in the Czech Republic as well, where a concrete warning has been issued by the National Cyber and Information Security Agency (NÚKIB), eliciting responses among Czech politicians.

The Czech Republic and its cyber security warning

NÚKIB is certainly of the Czech Republic's important government authorities. It serves as "the central administrative body for cyber security, including the protection of classified information in information and communication systems and cryptographic protection.[7] (...) It was established on August 1, 2017 on the basis of Act No. 205/2017 Coll., amending Act No. 181/2014 Coll., on Cybersecurity and on Amendments to Related Acts (the Cyber Security Act)" (Nukib.gov, 2024a). In his capacity as NÚKIB Director, Mr. Lukáš Kintr "regularly attends meetings of the State Security Council (BRS[8]) and is a member of the Cyber Security Committee, which is the BRS's permanent working body for coordinating and planning cybersecurity measures in the Czech Republic" (Nukib.gov, 2024a). In NÚKIB's organizational structure, the Director coexists with four Deputy Directors (Nukib.gov, 2024b).[9]

The National Cyber Security Centre (NCKB[10]) and the Strategic Affairs and Engagement Division (SSAS[11]) are "the executive sections" of NÚKIB. They are mainly responsible for "prevention of cybernetic threats to critical infrastructure elements, basic service information systems, important information systems, and selected public administration information systems". Furthermore, they focus on traditional "awareness and educational activities concerning cybersecurity", research and development in the field, international cooperation, but also, e.g. "evaluating cybersecurity risks and taking the appropriate corrective and preventive measures" (Nukib.gov, 2024c).

[7] NÚKIB also oversees the implementation of the public regulated service of the Galileo Global Navigation Satellite System (Nukib.gov, 2024a).

[8] In Czech: *Bezpečnostní rada státu*.

[9] Namely: Martin Smrčka (Information Security Division), Věra Vojáčková (Legal and Administrative Division), Tomáš Krejčí (National Cyber and Security Center Division), and Pavel Štěpáník (Strategic Affairs and Engagement Division) (Nukib.gov, 2024b).

[10] In Czech: *Národní centrum kybernetické bezpečnosti*.

[11] In Czech: *Sekce strategických agend a spolupráce*.

So-called warnings are a tool for highlighting existing cybersecurity threats that are serious enough to warrant immediate action. A warning is addressed to entities managing or operating "critical information and communication infrastructure systems, information and communication systems of essential services and important information systems." It "is not generally applicable to other organizations or natural persons". However, with regard to the nature of each concrete threat, "NÚKIB recommends even those organizations and persons to consider the warning" (Nukib.gov, 2024d).

On 8 March 2023, NÚKIB issued a warning against the China-based app TikTok (Nukib.gov, 2024d). This elicited media coverage by a number of outlets in the country (iRozhlas, 2023; Ct24.ceskatelevize, 2023). NÚKIB warned against "installing and using the TikTok app on devices accessing critical information and communication infrastructure systems, information and communication systems of essential services and important information systems". It issued the warning "based on the Agency's findings and information from partners" (Nukib.gov, 2024d).[12]

And what were the main contents of the warning? Among the main threats indicated by NÚKIB were "the amount of user data that is collected by the app as well as the way the data is handled". Last but not least, the Czech agency drew attention to "the legal and political environment of the People's Republic of China".[13] The level of threat was assessed as "high", indicating "probable to very probable" risk (Nukib.gov, 2024d).

NÚKIB director Lukáš Kintr commented on the new warning as follows:

> I proceeded to issue the warning based on a comprehensive analysis of information about TikTok that we obtained from public sources and our allies. The amount of data being collected and handled, combined with the legal environment in China and the growing number of users in the Czech Republic, leave us with no other choice than to describe TikTok as a security threat (...) The warning does not distinguish between users from the public and private sectors. The key issue is whether a threat to a particular system could harm the functioning of the Czech Republic and the security of each of us. (Nukib.gov, 2024d)

NÚKIB recommended the general public "to pay attention to what access the TikTok application requires, what data it collects and how it is handled".[14]

Even if Czech political parties were not bound by the NÚKIB warning, the text is going to focus on the social network communication strategies pursued by their

[12] It should be noted that NÚKIB had been consistently monitoring and assessing the risks associated with TikTok use. For example, in 2022, there was a body of assessments, findings and analysis supporting some suspicions related to the app as such (Nukib.gov, 2024d).

[13] Primarily with respect to ByteDance, the developer and administrator of TikTok.

[14] NÚKIB generally recommends installing and using only applications trusted by the user.

political (election) campaigns, including on a social network as disputed as TikTok. Such focus is relevant in the context of the so-called permanent campaigning, an overall change in political parties' social network patterns, but also the accumulation of consecutive elections in the country.

Czech political parties and TikTok

According to AMI Digital Index (2023) data, TikTok is a highly popular social network in the Czech Republic and has potential for further growth.[15] Like Snapchat, TikTok has seen an expansion in the numbers of users and in their activity. TikTok exhibited the highest rate of growth in 2023. Despite its risks, it is very popular among users and may continue to expand in the future (AMI Digital Index, 2023). Given TikTok's potential, political actors may find it highly attractive.

Seven political parties gained representation in the lower chamber of the Czech parliament after the Chamber of Deputies elections of 2021: ODS, TOP 09, KDU-ČSL, STAN, the Pirates, ANO 2011 and SPD (Šárovec, 2022b). There are important differences in their TikTok positions. This is also because their TikTok target audiences consist of voter groups exhibiting little to no use of other platforms. Hence politicians are faced with a clear choice between contacting their youngest constituencies (young or first-time voters) and ignoring the China-based social network to comply with the warnings of NÚKIB and other authorities (Rambousková, 2024).

Since 2021, the country has experienced Senate and local elections (2022), the presidential election (2023), and European Parliament elections (2024). Those will be followed by the Senate elections and regional elections of 2024, and the series will most likely culminate with the next Chamber of Deputies elections in 2025 (Volby, 2024). While the series consists of both first-order and second-order elections, it is more than evident that voters have been nearly constantly exposed to different forms of election campaigns. Among those are not only on-site campaign events, the dominant form of retail politics, but also numerous TV debates and, of course, various organized or individual presentations of politicians and political parties in the context of social networks such as TikTok.

Table 1 presents an overview of the TikTok attitudes and patterns of individual political parties. What they have in common are highly personalized forms of self-promotion. Thus, instead of political parties' official profiles, politicians tend to create personal accounts, where they communicate their political affiliation in one way or another.

[15] AMI Digital Index is an annual study of the Czech social media market. The 2023 survey was conducted on a sample of 1,010 internet users aged 15+ and residing in the Czech Republic (AMI Digital Index, 2023).

Table 1. The TikTok attitudes and patterns of political parties represented in the lower chamber of the Czech parliament

Attitude	Party and leader	TikTok pattern of the party
In favour or somewhat in favour	ANO 2011 – Andrej Babiš	very open & experimenting
	SPD – Tomio Okamura	similar to ANO, but not so strong
	STAN – Vít Rakušan	less humour, trying to balance the content
	Czech Pirate Party – Ivan Bartoš	individual activities of some members
Against or somewhat against	ODS – Petr Fiala	against in response to NÚKIB recommendation, but considering some ways
	TOP 09 – Markéta Pekarová Adamová	against in response to NÚKIB recommendation
	KDU-ČSL – Marián Jurečka	against in response to NÚKIB recommendation

Source: Author's own study based on (Rambousková, 2024; E15, 2024).

The above overview suggests the existence of two groups of parties: those (somewhat) in favour of using TikTok and those (somewhat) against it. Arguably, the list is not entirely arbitrary because, especially after the European Parliament elections, the different parties analysed the effectiveness and efficiency of their election campaigns and their basic approaches to communication. As a result, they may have somewhat changed their TikTok patterns as well.

Starting with politicians with high levels of TikTok activity, the profile of Andrej Babiš (ANO 2011 leader) has been a great success, with a total of 160 thousand followers. Tomio Okamura (head of SPD) has accumulated almost 66 thousand followers. The deputy leader of ANO 2011, Alena Schillerová, has gathered more than 36 thousand followers, perhaps thanks to her oft debated light content. Former presidential candidate and elected MEP Danuše Nerudová (STAN) is followed by more than 96 thousand TikTok users. New MEP Filip Turek, an independent elected for Přísaha and a big surprise of the 2024 EP elections, is followed by almost 39 thousand users. And to name one representative of the Czech Pirate Party, Prague's Deputy Mayor for Transport Zdeněk Hřib is followed by more than 10 thousand users (Rambousková, 2024 and own update via TikTok).

The TikTok patterns of different political actors in the Czech Republic reveal that some of them are aware of the risks highlighted by NÚKIB. However, most are still willing to use the platform despite the risks, thus, prioritizing the benefit of effectively and directly targeting the young generation and first-time voters. Thus, they are taking a relatively clear position to questions about the safety of using TikTok in general and whether to prefer security over election and political success in particular.[16]

[16] Moreover, these patterns are very much like those of other European leaders.

Conclusions

The observable trends in political communication clearly demonstrate that social networks provide an indispensable tool in the fight for people's votes. In addition to the specific roles of each platform and the individual politicians/candidates, influencers play an essential and increasingly important part.

In contrast to the era of traditional print media, television, and radio, there has been a clear and repeatedly demonstrated shift to online platforms and social networks, whose potential is diverse, especially across voter groups, and changes over time. Self-promotion on social networks is subject to the criteria of simplicity, understandability, quality, and originality. These facts are well known to the different parties and political leaders.

Political communication on TikTok appeals to emotions, sympathy, and a sense of humour and novelty. There are also negative or comparative forms of communication aimed at distancing oneself from competitors or opponents. Personalization of politics is another key trend. It often goes hand-in-hand with tabloidization and results in highly simplifying TikTok content. This clearly leads to the hollowing out of politics and political content, a currently under-researched risk.

Despite all potential and real threats, the TikTok platform is a phenomenon of the time. According to various types of available predictions, the platform will continue to grow. And with each cohort of teenagers approaching voting age, it will continue to help politicians expand their sub-constituency of young and first-time voters. This is evidently a very strong argument for some parties and politicians, one that plays a central role in their deciding whether or not to promote themselves on TikTok despite its security risks.

This chapter has sought to analyse and review the TikTok risks defined thus far and the related challenge facing political actors. What we do not know is whether particular restrictions imposed on a given social network really are an effective tool for fighting the above risks. This remains a question for future empirical research on the topic.

While risks surely have to be monitored, assessed and responded to, the existing body of knowledge suggests that regulating the entire environment is the more robust solution. Regulation may ultimately help create clearer and more stable conditions for the operation of TikTok as well as other social networks that might raise suspicions with respect to transparency and the handling of user data.

References

Ami Digital Index. (2023). *AMI Digital*. https://amidigital.cz/index2023/

Apnews. (2023). *Australia bans TikTok from federal government devices.* https://apnews.com/article/tiktok-australia-ban-government-devices-ce06a8d4215bbf8b85b692d91f96cf32

Apnews. (2024). *Biden just signed a bill that could ban TikTok. His campaign plans to stay on the app anyway.* https://apnews.com/article/biden-tiktok-campaign-account-young-voters-ban-d351ccb17c59890473af1685a0a756f3

Barberà, O., Sandri, G., Correa, P., & Rodríguez-Teruel, J. (Eds.) (2021). *Digital Parties: The Challenges of Online Organisation and Participation.* (Studies in Digital Politics and Governance). Springer.

Ct24.ceskatelevize. (2023). *TikTok je bezpečnostní hrozba, varuje NÚKIB.* https://ct24.ceskatelevize.cz/clanek/domaci/tiktok-je-bezpecnostni-hrozba-varuje-nukib-9537

Czarnecki, S. (2023). Dezinformacja w Republice Czeskiej. In S. Czarnecki, Ł. Lewkowicz & A. Tatarenko, *Dezinformacja w Republice Czeskiej i Republice Słowackiej w obliczu wojny rosyjsko-ukraińskiej* (pp. 13–42). Instytut Europy Środkowej.

Demandsage. (2024). *TikTok User Statistics 2024 (Global Data).* https://www.demandsage.com/tiktok-user-statistics/

E15. (2024). *Bezpečnostní hrozba plná voličů. Starostové vstoupili na čínský TikTok, tancovat prý nebudou.* https://www.e15.cz/byznys/technologie-a-media/bezpecnostni-hrozba-plna-volicu-starostove-vstoupili-na-cinsky-tiktok-tancovat-pry-nebudou-1413747

European Commission. (2024a). *Commission opens formal proceedings against TikTok under the Digital Services Act*. https://digital-strategy.ec.europa.eu/en/news/commission-opens-formal-proceedings-against-tiktok-under-digital-services-act

European Commission. (2024b). *The Digital Services Act*. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en

ENISA. (2010). *Online as soon as it happens.* European Union Agency for Cybersecurity. https://www.enisa.europa.eu/publications/archive/onlineasithappens

ENISA. (2024). *About ENISA*. The European Union Agency for Cybersecurity. https://www.enisa.europa.eu/about-enisa

Euronews. (2024). *Which countries have banned TikTok and why?* https://www.euronews.com/next/2024/03/14/which-countries-have-banned-tiktok-cybersecurity-data-privacy-espionage-fears

Fišer, M. (2023, March 2). *Turecko udělilo TikToku dvoumilionovou pokutu kvůli ochraně dat.* https://www.novinky.cz/clanek/internet-a-pc-turecko-udelilo-tiktoku-dvoumilionovou-pokutu-kvuli-ochrane-dat-40424477

Forbes. (2024). *Čínský ByteDance žaluje vládu USA. Chce blokovat zákon, který ho nutí prodat TikTok.* https://forbes.cz/cinsky-bytedance-zaluje-vladu-usa-chce-blokovat-zakon-ktery-ji-nuti-prodat-tiktok/

Fu, C., & Wakakbayashi, D. (2024, April 25). *There Is No TikTok in China, but There Is Douyin. Here's What It Is.* The New York Times. https://www.nytimes.com/2024/04/25/business/china-tiktok-douyin.html

iRozhlas. (2023). *TikTok je bezpečnostní hrozba, upozorňuje český kyberúřad. Varuje před používáním aplikace.* https://www.irozhlas.cz/veda-technologie/technologie/tiktok-je-bezpecnostni-hrozba-upozornuje-cesky-kyberurad-varuje-pred-pouzivanim_2303081130_ako

Karimi, F. (2022, September 15). *This wordless comedian is now the most-followed person on TikTok.* CNN. https://edition.cnn.com/2022/06/23/world/khaby-lame-most-followed-man-tiktok-cec/index.html

Macková, A. (2017). *Nová média v politické komunikaci. Politici, občané a online sociální sítě.* MUNI Press.

Nukib.gov. (2023). *Varování.* NÚKIB. https://nukib.gov.cz/download/uredni_deska/2023-03-08_Varovani-TikTok_final.pdf

Nukib.gov. (2024a). *Národní úřad pro kybernetickou a informační bezpečnost – O NÚKIB.* NÚKIB. https://nukib.gov.cz/cs/o-nukib/

Nukib.gov. (2024b). *Vedení úřadu.* NÚKIB. https://nukib.gov.cz/cs/o-nukib/vedeni-uradu/

Nukib.gov. (2024c). *Kybernetická bezpečnost.* NÚKIB. https://nukib.gov.cz/cs/kyberneticka-bezpecnost/

Nukib.gov. (2024d). *Aplikace TikTok představuje bezpečnostní hrozbu.* NÚKIB. https://nukib.gov.cz/cs/infoservis/hrozby/1941-aplikace-tiktok-predstavuje-bezpecnostni-hrozbu/

Rambousková, M. (2024). *Politici jdou na nebezpečný TikTok. Je tam víc než milion budoucích voličů.* Seznam Zprávy. https://www.seznamzpravy.cz/clanek/domaci-politika-politici-jdou-na-nebezpecny-tiktok-je-tam-vic-nez-milion-budoucich-volicu-247239

Reuters. (2023, March 27). *Polish council recommends banning TikTok on public administration phones – media.* https://www.reuters.com/technology/polish-council-recommends-banning-tiktok-public-administration-phones-media-2023-03-27/

Statista. (2024). *Countries with the largest TikTok audience as of April 2024 (in millions).* https://www.statista.com/statistics/1299807/number-of-monthly-unique-tiktok-users/

Šárovec, D. (2022a). Digitalizace a stranické akce: případová studie České republiky. In B. Linhartová, P. Dubóczi & D. Gajdoščík (Eds.), *Pandémia & demokracia. Budúcnosť demokracie v postcovidovej dobe* (pp. 43–57). Univerzita Pavla Jozefa Šafárika v Košiciach, Vydavateľstvo Šafárik Press.

Šárovec, D. (2022b). Volby do Poslanecké sněmovny Parlamentu ČR 2021: dvě hnutí vs. dvě koalice. In M. Žac, V. Dudinský & A. Polačková (Eds.), *Budúcnosť Európy* (pp. 85–95). Prešovská univerzita v Prešove.

TikTok. (2024a). *About TikTok*. https://www.tiktok.com/about?lang=en

Tiktok. (2024b). *Oficiální kanál uživatele Khabane lame (@khaby.lame).* TikTok. https://www.tiktok.com/@khaby.lame

Vilček, I., & Fišer, M. (2023, March 24). *Slovenský parlament zablokoval TikTok.* https://www.novinky.cz/clanek/internet-a-pc-software-slovensky-parlament-zablokoval-tiktok-40426820

Volby. (2024). *Volby.cz – Český statistický úřad.* ČSÚ. https://volby.cz/

Yeung, J., & Wang, S. (2023, March 24). *TikTok is owned by a Chinese company. So why doesn't it exist there?* CNN. https://edition.cnn.com/2023/03/24/tech/tiktok-douyin-bytedance-china-intl-hnk/index.html

JUSTYNA KIĘCZKOWSKA

MARIA CURIE-SKŁODOWSKA UNIVERSITY, LUBLIN

Medical Data Security in the Digital Era

Abstract: In the era of digitalization, the security of medical data has become an important issue in the context of protecting patient privacy and compliance with legal regulations. Transformations in healthcare information technology have brought numerous benefits, such as improved efficiency and accessibility of medical services, but have also increased the risks associated with protecting sensitive information. This article discusses the main aspects of health data security, paying particular attention to technical, organizational and regulatory protection measures to effectively secure medical data. Modern data security challenges require continuous adaptation to the changing threat environment and technology development to ensure the highest level of protection of health information and compliance with applicable regulations.

Keywords: medical data security; digitization; encryption; access control; GDPR; HIPAA; risk assessment; security audit

Introduction

In the digital era, medical data is slowly becoming one of the most sensitive and valuable resources. Electronic medical records (EDM) and IT systems in health care improve the quality of patient care, enabling, for example, quick access to information, better coordination of treatment and more precise diagnosis. As the amount of data stored and processed increases, the risk of unauthorized access, leakage and other forms of security breaches increases as well. Data has become one of the most valuable resources for enterprises, public institutions and individual users. Technological progress, the growing popularity of the Internet and the development of cloud computing have led to a dynamic increase in the amount of data generated, stored and processed on a global scale. In this context, data security has become crucial.

Data security refers to practices and technologies designed to protect information against unauthorized access, theft, loss, damage and other possible threats. The growing importance of data also generates threats related to their security.

Cyber attacks, such as ransomware, phishing, DDoS (Distributed Denial of Service) attacks and data leaks have become a daily challenge for organizations around the world. In particular, medical data, which are sensitive data and contain information about patients health condition, treatment history, tests results, and genetic data are extremely valuable. Protecting this data is not only an ethical issue, but also a legal one. Many countries decide to introduce strict regulations to protect personal data, such as the General Data Protection Regulation (GDPR) in the European Union, Health Insurance Portability and Accountability Act (HIPAA) in the United States, or state legal acts. In the context of medical data protection, healthcare IT systems pose particular challenges. Electronic health records, patient information management systems (PIMS), telemedicine, and other advanced health technologies increase the efficiency and quality of health care while carrying data security risks. These threats may lead to serious consequences, such as violation of patient privacy, disruptions in the functioning of medical facilities as well as a direct threat to patients lives in the event of manipulation of medical data. For this reason, protecting medical data requires a comprehensive approach that includes both security technologies and appropriate data management procedures and policies. Encryption, access control, security audits, intrusion detection and prevention systems (IDS/IPS), regular software updates and staff training are just some of the key elements of an effective data security strategy. The aim of this article is to present the main challenges and best practices related to medical data security in the digital era. Data security in the digital era is a dynamically developing area that requires constant attention and adaptation to new threats. The protection of medical data is very important due to their sensitivity and importance for the health and life of patients. A correct approach to data security in the medical sector is therefore necessary to ensure not only the protection of patients privacy, but also the effective, safe functioning of the entire healthcare system.

Medical data and their security

Medical data is data of natural persons regarding their entitlement to the provided and planned health care services, health status, as well as the other data including, for example, personal data that is processed in connection with these services, health prevention and implementation of health programs. These include information contained in electronic medical records, such as a person's medical history, diagnoses and treatment, medications, allergies, vaccinations along with radiological images and laboratory tests results (Pracodawcy dla zdrowia, 2023). This type of data also includes sensitive data, i.e. genetic and biometric data that allow for the unambiguous identification of a natural person, regarding health, sexuality or sexual orientation

(Pacjent.gov, 2024). These data are subject to special protection and may only be processed in exceptional situations. In the Personal Data Protection Act, health data is treated as the so-called sensitive data. The regulations clearly prohibit the processing of this type of data. Exceptions to the prohibition are strictly defined and included in particular: the processing of data for the purpose of protecting health, providing medical services, treating patients or managing the provision of medical services by entities professionally engaged in treatment or providing other medical services or managing the provision of such services. In the context of medical data, the most important issue right now is EDM. Act on the health care information system (Act of April 28, 2011 on the health care information system, Journal of Laws of 2011 No. 113 item 657) introduces the concept of EDM, understood as documents created in electronic form with a qualified electronic signature or a signature confirmed by the ePUAP trusted profile. The Act also specifies that medical documentation contains the so-called individual medical data, i.e. personal data and other data of natural persons regarding entitlements to granted, provided and planned health care services, health status, as well as other data processed in connection with planned and provided health care services containing health prevention and implementation of health programs. In fact, the information contained in medical records (traditional and electronic) and in the created medical registers is a huge amount of personal data, both from ordinary (such as name and surname or PESEL number) and data subject to special protection of health data, e.g. medical history (treatment, therapies, medications/doses taken), diagnostic tests, mental health information, medical records (patient chart, doctor's notes), information about medical visits (consultations, visits, hospitalizations), information about diseases in the family. The provisions introduced by the GDPR (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC) move away from the concept of sensitive data, pointing to a set of special categories of data, such as, among others: health data, genetic data or biometric data, while maintaining a general prohibition focused on the processing of this type of data. The GDPR also specifies exceptions allowing their processing in specific situations, in particular related to the provision of medical care (Krakowiak, 2018).

In the face of digital progress in the health care system, ensuring data security in a broad sense is becoming an essential and necessary issue, primarily for the proper functioning of the system and all its elements. Health data security can therefore refer to the practices, procedures, technologies, and policies designed to protect the confidentiality, integrity, and availability of the health data. This includes protecting all health care-related information, including patient information, diagnoses, treatments, medical procedures, laboratory tests results and other sensitive health data.

Patient privacy is one of the main reasons why medical data security is so important. Medical data contains highly sensitive information that, in the event of unauthorized access, can lead to stigmatization, discrimination and even legal and professional problems for patients. Breaches of privacy may turn out into a loss of trust in medical institutions, which may discourage patients from sharing complete and accurate information about their health, which will lead to a negative impact on the quality of medical care. Medical data security is the foundation of modern healthcare, ensuring protection of patient privacy, integrity and availability of key medical information, and compliance with legal regulations. In a dynamically changing digital and security environment, medical institutions must constantly adapt their data protection strategies to effectively counter new threats and ensure the highest level of medical data security.

Threats to the security of medical data

The health care system and its elements have now become the main target of cyber criminals, both in Poland and around the world. In Poland, 43 hacker attacks on medical facilities were reported in 2023, in 2021, there were only 13 (an increase of over 300%). In turn, worldwide, it is estimated that hacker attacks in healthcare reach 1,800 per week (an increase of 74% compared to 2022). A small number of reports should not indicate a low level of threat, but it does indicate low attack detection. Attacks on medical data are the type of threat that falls on fertile ground. In hospitals and other entities providing health services, patients personal data are processed, such as name, surname, PESEL number or residential address, including sensitive data regarding the patients health condition. Cybercriminals encounter no resistance and have no major difficulties in breaking the security (which is often lacking) regarding personal data at the appropriate level.

The growing scale of the threat of hacker attacks in hospitals and medical facilities prompted the reaction of the European Network and Information Security Agency (ENISA). After analyzing hacker attacks in EU countries from January 2021 to March 2023, it prepared the report *Health Threat Landscape* (ENISA, 2023). The report clearly states that one of the main cyber threats in healthcare is ransomware, which accounts for 54% of all security incidents. As many as 43% of ransomware attack events resulted in data breaches (Poradyodo, 2023). Ransomware is a type of malware that encrypts a victim's data and then demands a ransom to unlock it. The medical sector is particularly susceptible to this type of attacks due to the need for uninterrupted access to patient's data. An example is the ransomware attack on the British NHS system in 2017, which disrupted the operation of many medical facilities, negatively impacting patient care. The NHS was hit hard by the

WannaCry ransomware attack, which disrupted around 81 NHS departments and 600 primary care organizations. The costs of this cyberattack are estimated at USD 115 million (GBP 86 million), and resulted in the cancellation of over 19,000 visits (Blog.osoz, 2024).

Another threat for the health care system and medical data are phishing attacks. Phishing is a fraud method that involves sending fake emails to obtain sensitive information such as passwords or credit card information. In the medical context, phishing can lead to unauthorized access to information systems, which may end up in the theft of medical data. Among the facilities attacked by hackers, more than half (54%) fell victim to phishing – according to the study "IT Security in the Health Care Sector" by Fortinet (Marszycki, 2022). In the case of phishing messages, the weakest link is the branch employees, who unknowingly allow access to systems or databases.

At the level of Polish hospitals, software vulnerabilities are also a serious threat, as they can be exploited, for example, with code to carry out an attack or gain unauthorized access. Until the flaw is fixed, the hacker could affect the program, database, computer or network. Unauthorized access may also be an internal threat, coming directly from the health care facility. Internal threats concern employees of medical facilities who may gain unauthorized access to medical data. This can be the result of either an intentional action or an unconscious error. An example is the case of an employee who accidentally shared confidential information on a public network drive. Another form of threat related to gaining access to data can be simply the theft of portable devices, such as laptops, tablets or smartphones with medical data. Theft of such devices can lead to data loss if they are not properly secured, for example, through encryption.

In 2023, the number of DDoS attacks on hospitals in Poland increased. The pro-Russian Killnet group is increasingly attacking hospitals, warn cybersecurity experts. Their specialty is DDoS (a type of attack, e.g. on a server or website, which generates artificial traffic so as to use all the free resources of the victim and lead to the unavailability of services. As a result, users cannot enter, e.g. a given website or platform), which results in lack of access to the system, e.g. with patient data. Killnet targeted the websites of healthcare organizations, beginning its campaign in February 2023 and targeting hospitals in more than 25 US states. According to Microsoft analysts, in November 2022, 10–20 attacks could be observed per day, and in February – 40–60 per day. Nearly 1/3 of them affected pharmacy, hospitals (26%), health insurance (16%) and health services and care (16%). In Poland, there is also a problem of DDoS cyberattacks on hospitals. On Monday, February 6, 2023, there were problems with the internal systems of the Central Clinical Hospital in Łódź. The facility's website and email box have stopped working. An official letter confirmed that an attack had taken place in November 2022. The Polish Mother's Health

Center Institute fell victim to a cyber attack. The facility was forced to switch to traditional mode of operation based on paper documentation. The incident caused difficulties in the functioning of the hospital, which, of course, was most painful for the patients (CyberDefence24, 2023). Microsoft experts emphasize that this type of activities are increasingly used to divert attention in order to hide more sophisticated operations (e.g. data theft) carried out at the same time (Palczewski, 2023).

Loss or threat to data security may also occur as a result of inappropriate behavior of the staff of a hospital or other health care facility. An incorrect approach of staff to data protection can even lead to personal data protection violations, resulting primarily in the disclosure of data to unauthorized persons. According to the 2019 report by the Supreme Audit Office, there are situations where one patient accidentally took the medical records of another patient from one of the clinics, and a man with mental disorders stole three patient files from the registration room, two of which were not found. Cases are also mentioned where copies of medical documentation were made available to unauthorized persons by the persons to whom the documentation concerned; in other cases, the documentation was issued without prior verification whether the person receiving it was actually authorized to do so. In data protection, an important issue is also the organization of the appropriate process of granting authorizations to process personal data (Topyła, 2019). In its report, the Supreme Audit Office pointed out that there were situations in which authorizations were granted to too broad a group of people, i.e. service employees – for example, orderlies. On the other hand, it was possible to notice the practice of not granting authorizations to people who should have such authorizations – for example, doctors or nurses. The errors also included granting access rights to the IT system processing personal data by IT without the prior consent of the hospital director or failing to revoke rights to IT systems to persons leaving work. The report showed that some employees had the rights of administrator of IT systems processing personal data, even though the scope of their duties did not include such obligations. Such solutions increased the risk of malware being installed on the computers they used. Situations were indicated in which the antivirus system was not used at all in hospitals or had an outdated virus database.

A significant problem is the failure to use any authorization data for access in computer operating systems or the use of the same data – the Supreme Audit Office showed that employees often used the same logins and passwords. Such conduct results in the inability to determine which employee performed specific operations in the system (including, for example, the breach of personal data protection), as well as the inability to revoke access rights of former employees. The Supreme Audit Office also pointed out irregularities regarding the security measures used or problems in the application of security measures specified in internal regulations: inappropriate password strength (e.g. too few characters or passwords such as Alicja123),

failure to change the password after 30 days in accordance with internally adopted requirements and lack of system lock in the event of entering the wrong password several times, inadequate security of the server room, storing a backup copy in the same place as the source data.

Medical data, due to their sensitivity and value, are particularly vulnerable to various types of attacks, for instance, ransomware, phishing, and unauthorized access. These threats can lead to serious consequences for patients, like a loss of privacy, health risks, as well as for medical institutions, which may incur costs related to data breaches, loss of public trust and legal penalties. In the face of growing threats, medical institutions must constantly adapt their protection strategies. Data encryption, security policies, staff training, and regular audits and updates are just some of the many tools that can help increase the security of medical data. In the digital age, a dynamic and adaptive approach to data protection is essential to ensure patient privacy and the integrity and availability of critical medical information.

Protective measures

Medical data has become a resource that requires special protection. Electronic health records (EHRs), patient data management systems, and telemedicine platforms significantly improve the efficiency and quality of healthcare, while exposing this sensitive information to a variety of cyber threats. Attacks on medical data can lead to serious consequences, including identity theft, financial fraud, and direct threats to patient health. The protection measures implemented at the level of health care systems containing technical measures, and in this group, encryption is the most important. Encryption is a fundamental data protection mechanism that ensures that information is only accessible to authorized users. Medical data should be encrypted both during storage (data at rest) and during transmission (data in transit). Encryption algorithms such as AES (Advanced Encryption Standard) provide a high level of security that is difficult to crack without the appropriate encryption key. Data encryption is one of the most effective preventive measures against unauthorized access. In the case of cyber attacks such as hacking, malware and phishing, encrypted data is much more difficult to exploit. Even in the event of physical theft of storage media as laptops or hard drives, encrypted information remains protected (Schneier, 2015). Another solution are intrusion detection systems (IDS) and intrusion prevention systems (IPS). These are essential tools in the defense arsenal of every medical institution. IDSs/IPSs play an important role in protecting medical data by monitoring network traffic and detecting unauthorized access attempts to information systems. IDSs analyze network traffic in real time to detect suspicious activity, while IPS can block potentially malicious operations.

This makes it possible to detect and neutralize threats early, before they can cause serious damage. The choice of the appropriate IDS/IPS depends on the specific needs and infrastructure of the medical institution. Factors to consider include the size of the network, the types of data stored, and the technical and financial resources available. The ideal solution may be a combination of different types of IDS and IPS, providing multi-layered protection (Scarfone & Mell, 2007).

Authorization and authentication play a fundamental role in the process of protecting medical data. Authentication is the process of verifying the identity of a user or system before granting access to resources. In the context of health data, effective authentication is key to ensuring that only authorized individuals have access to sensitive information. Passwords are a traditional authentication method that involves the user entering a password. Commonly used passwords are unfortunately susceptible to brute force and phishing attacks, requiring additional protection measures such as password complexity policies and regular password changes. Two-factor authentication (2FA) is a process that requires a user to confirm their identity using two independent methods, for example, a password and a code sent to their mobile phone. 2FA significantly increases the level of security by minimizing the risk of access by unauthorized persons, even in the event of password theft. Authorization is the process of granting or denying access to resources based on the identity of the authenticated user. In medical data management systems, authorization is used to ensure that users only have access to data that is necessary to perform their professional duties. In large medical institutions, managing authentication and authorization for thousands of users can be complex. This requires scalable solutions that can be easily adapted to the growing needs of the organization. Implementing automated identity and access management (IAM) systems can help scale access management and improve operational efficiency. Effective implementation of these mechanisms requires the use of advanced technologies and adaptation of security policies to dynamically changing needs and regulations (Stallings & Brown, 2017). One of the key elements of a security strategy is regular software updates and the use of security patches. Regular updates and security patches are essential to protect systems from newly discovered vulnerabilities. Hackers often exploit known software vulnerabilities to launch attacks. Therefore, deploying security patches quickly and effectively is crucial to minimizing the risks associated with exploit attacks. An example is ransomware attacks, which often exploit vulnerabilities in outdated software to encrypt data and demand a ransom for decryption. Software updates often contain bug fixes that may affect the stability and performance of medical systems. Regularly implementing these updates helps ensure that systems operate without interruption, that is crucial to the continuity of operations in healthcare facilities. IT systems in medical facilities are often complex, consisting of various components and software provided by different suppliers. Managing updates and patches in this

kind of environment can be difficult, requiring careful planning and coordination to avoid system disruptions (Ghafur et al., 2019).

In order to ensure an appropriate level of protection, medical institutions must implement effective security policies and procedures that are considered organizational security measures. The data protection policy sets out general principles for the management of medical data in the organization. It should cover aspects such as data classification, access rights, data storage and deletion rules, and procedures in the event of a data breach. The data access policy defines who has access to medical data and under what conditions. An important aspect of this policy is role-based access control (RBAC), which assigns access permissions based on the functions performed by employees in the organization. This policy should specify user authentication and authorization procedures as well. Health care entities should also have mechanisms in place as part of security incident management procedures that specify the steps to be taken in the event of a security incident being detected. They should include processes of identification, analysis, response and reporting of incidents plus procedures for restoring normal operation of systems after an incident (Anderson & Moore, 2006). Appropriate training of medical staff is considered one of the basic elements of a data protection strategy. Human errors are often the weakest link in security systems. The training is aimed at increasing employee awareness of potential threats to medical data. Healthcare staff who are aware of risks such as phishing, ransomware and other forms of cyberattacks are more likely to follow security procedures and be more effective at recognizing suspicious activity. Training helps reduce the risk of security incidents by educating staff on data protection best practices. Employees who are trained in the safe use of IT systems are less likely to make mistakes that may lead to data leakage. One of the main challenges in implementing training is ensuring staff engagement. Medical workers often have busy schedules and may perceive training as an additional burden. It is important that training is tailored to their needs and available in a form that minimizes disruption to their daily duties.

A security audit – another technical security measure – allows for the systematic identification of threats and security gaps in IT systems, including systems storing medical data. The audit process involves analyzing existing security measures, assessing their effectiveness and identifying potential weaknesses, that can be exploited by cybercriminals. Detecting vulnerabilities early allows them to be patched quickly. Audits make it possible to assess the effectiveness of the data protection measures used and introduce appropriate improvements. The audit process identifies not only weak points, but also areas that are functioning well, which allows you to strengthen your data protection strategy. Audits often lead to the implementation of new, more effective solutions, which translates into better security of medical data.

The last group of measures are regulatory measures. The General Data Protection Regulation (GDPR) in the European Union and the Health Insurance Portability

and Accountability Act (HIPAA) in the United States are two fundamental pieces of legislation that regulate how medical data is processed and ensure its protection. The GDPR, introduced in May 2018, is an EU regulation that aims to protect the personal data of all European Union citizens. This regulation defines the rules for the processing of personal data and imposes obligations on organizations processing this data. In the context of medical data, the GDPR establishes specific provisions for sensitive data, which includes health data. HIPAA, introduced in 1996, is a US law designed to protect the privacy and security of health information. This Act establishes standards for the protection of health information and regulates how this data may be stored, processed and transferred. HIPAA establishes health information privacy rules that include requirements for patient's consent to the processing of their data and requirements for the confidentiality of health information. HIPAA defines health information as "protected health information" (PHI), which is subject to strict regulations regarding its protection. Both pieces of legislation require appropriate security measures, but the GDPR places greater emphasis on privacy protection and data anonymity, while HIPAA focuses on the security of health information, including physical and technical security (HIPPA, 2024). The GDPR and HIPAA provide for high financial sanctions for violations of the regulations, but enforcement mechanisms vary depending on the region and the specific nature of the regulations (U.S. Department of Health & Human Services, 1996). Risk assessment has become a tool in managing medical data protection. Using this practice allows you to systematically identify, analyze and manage the risks associated with the processing and storage of sensitive health information. Effective risk assessment not only protects against potential security incidents, but also ensures compliance with applicable legal regulations. Risk assessment allows for the implementation of effective protection measures tailored to the identified threats. For example, if a risk analysis reveals a high likelihood of ransomware attacks, an organization may decide to implement advanced protection mechanisms like IDSs/IPSs and regular backups. It is also a cyclical process that requires regular monitoring and auditing. As new threats emerge and technologies change, it is necessary to periodically review and update risk assessments and protective measures. Regular audits help identify areas for improvement and ensure that protection measures are effective. By using various risk assessment methods, such as SWOT analysis, FMEA, ISO 27001 standards and NIST guidelines, organizations can effectively identify threats, assess data sensitivity or implement appropriate protection measures (Medidesk, 2021). Protecting health data requires approaches and initiatives that combine technical, organizational and regulatory measures. Effective data security requires not only the implementation of appropriate protection technologies, but also the creation of solid security policies and the provision of continuous training and auditing. Legal regulations such as the GDPR and

HIPAA provide a key framework for data protection, but practical implementation requires commitment at all levels of the organization. Contemporary challenges in the protection of medical data require flexibility and adaptation to the changing threat environment and developing technologies.

Conclusions

The security of medical data in the digital era is a complex and multi-faceted challenge that requires taking into account both modern technologies and complex legal regulations and organizational procedures. The development of digitalization in health care has brought many benefits, e.g. increasing the efficiency of health care, easier access to information and improving the quality of services. At the same time, however, there is a risk related to the security of medical data. Medical data is becoming a valuable target for cybercriminals and is also exposed to various other threats, such as human errors, data mismanagement and technical failures. The increase in cyber attacks and issues related to privacy and regulatory compliance pose problems for the functioning of the system. Modern IT systems are often complex and integrated, which makes security management difficult and again requires the implementation of advanced technical solutions and effective risk management strategies. Technical measures to protect health data are important to ensure its confidentiality, integrity and availability. Data encryption, both during storage and transmission, is a basic protection mechanism that ensures that data is unreadable to unauthorized persons. Access control, including multi-factor authentication, and intrusion detection and prevention systems (IDS/IPS) are essential elements for monitoring and securing IT systems against unauthorized access and attacks. Regular software updates and security patches are important to eliminate known security vulnerabilities and protect against new threats. The introduction of appropriate organizational policies and procedures provides the basis for effective protection of medical data. The development of data management policies, incident response procedures and data protection principles is the foundation of security. Regular staff training aimed at increasing awareness of threats and knowledge of best practices is a guarantee of minimizing the risk of human errors. Security audits and monitoring of IT systems also allow for identifying weaknesses and assessing the effectiveness of security measures, enabling strategies to be adapted to changing conditions and threats. Regulations like the GDPR in the European Union and HIPAA in the United States are the flagship legal frameworks for protecting medical data. These laws, while varying by region, are intended to ensure a high level of protection of medical data and ensure patient privacy. Looking to the future, the development of technologies, especially artificial intelligence and automation, can

significantly improve the effectiveness of medical data protection. AI-based tools can automatically identify threats and predict potential risks allowing for faster and more precise response to incidents. Integration with security management systems, such as threat intelligence management (SIEM) systems, can enable better real-time threat monitoring and analysis. With the growing importance of data protection, the development of standards and norms for medical data security can contribute to standardizing practices and ensuring their high quality. Therefore, contemporary challenges in the field of medical data security require flexibility and adaptation to the changing threat environment and developing technologies.

References

Act of April 28, 2011 on the health care information system, Journal of Laws of 2011 No. 113 item 657.

Anderson, R., & Moore, T. (2006). The economics of information security. *Science*, *314*(5799), 610–613.

Blog.osoz. (2024). *Brytyjski odpowiednik NFZ ostrzega przez cyberatakami*. https://blog.osoz.pl/brytyjska-narodowa-sluzba-zdrowie-ostrzega-prze-cyberatakami

CyberDefence24. (2023). *Prorosyjscy hakerzy coraz częściej atakują szpitale. Rośnie skala DDoS*. https://cyberdefence24.pl/cyberbezpieczenstwo/prorosyjscy-hakerzy-coraz-czesciej-atakuja-szpitale-rosnie-skala-ddos

ENISA. (2023). *Health Threat Landscape Report*. https://www.enisa.europa.eu/publications/health-threat-landscape

Ghafur, S., Kristensen, S., Honeyford, K., Martin, G., Darzi, A., & Aylin, P. (2019). A retrospective impact analysis of the WannaCry cyberattack on the NHS. *NPJ Digital Medicine*, *2*(1), 98.

HIPPA. (2024). https://law-store.wolterskluwer.com/s/product/hipaa-a-guide-to-health-care-privacy-and-security-law-vitallaw/01tG000000Lu0NWIAZ

Krakowiak, J. (2018). *Dane medyczne – należy usuwać czy przechowywać?*. https://www.rp.pl/dane-osobowe/art2045831-dane-medyczne-nalezy-usuwac-czy-przechowywac

Marszycki, M. (2022). *Jak wygląda stan bezpieczeństwa IT w polskich szpitalach?*. https://itwiz.pl/jak-wyglada-stan-bezpieczenstwa-it-w-polskich-szpitalach/

Medidesk. (2021). *Jak zadbać o elektroniczną dokumentację medyczną*. https://medidesk.pl/jak-zadbac-o-elektroniczna-dokumentacje-medyczna-w-placowce/

Pacjent.gov. (2024). *Ochrona danych pacjenta*. https://pacjent.gov.pl/artykul/ochrona-danych-pacjenta

Palczewski, S. (2023). *#CyberMagazyn: Co to jest DDoS? Te ataki nękają Polskę*, https://cyberdefence24.pl/cyberbezpieczenstwo/cybermagazyn-co-to-jest-ddos-te-ataki-nekaja-polske

Poradyodo. (2023). *Cyberbezpieczeństwo w szpitalach i innych placówkach medycznych – coraz więcej ataków hakerskich*. https://www.poradyodo.pl/ado/cyberbezpieczenstwo-w-szpitalach-i-innych-placowkach-medyczne-coraz-wiecej-atakow-hakersskich-12463.html#

Pracodawcy dla zdrowia. (2023). *Zasady bezpieczeństwa danych medycznych i ich wykorzystania tematem konferencji*. https://pracodawcydlazdrowia.pl/zasady-bezpieczenstwa-danych-medycznych-i-ich-wykorzystania-tematem-konferencji/

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

Scarfone, K., & Mell, P. (2007). *Guide to Intrusion Detection and Prevention Systems (IDPS)*. NIST.

Schneier, B. (2015). *Applied Cryptography: Protocols, Algorithms, and Source Code in C*. Wiley.

Stallings, W., & Brown, L. (2017). *Computer Security: Principles and Practice*. Pearson.

Topyła, M. (2019). *Ochrona danych osobowych w szpitalach. Typowe błędy*. https://kancelariatopyla.pl/ochrona-danych-osobowych-w-szpitalach-typowe-bledy/

U.S. Department of Health & Human Services. (1996). *Health Insurance Portability and Accountability Act of 1996 (HIPAA)*. Public Law 104-191.

PART IV

Migration Security

MICHAL KLÍMA

METROPOLITAN UNIVERSITY PRAGUE

The Migration Crisis of 2015–2024 and Its Impact on European Security

Abstract: This chapter addresses a new security threat facing Europe and Western democracies. The primary threat is a result of German Chancellor Angela Merkel's welcoming migration policy of 2015. This policy has caused the greatest destabilisation of Europe in the 21st century. It has become a Trojan horse for the infiltration of influence of millions of people from different world civilisations which adhere to an intolerant culture and religion. What further proof of the destructive nature of this migration policy is needed than the fact that the secret services of Russia and Belarus have transported tens of thousands of migrants to Poland's borders since 2021 as a weapon in a hybrid war against democratic Europe? At the same time, Putin and Lukashenko employed the same destructive strategy against Finland and the Baltic states – Lithuania, Latvia and Estonia – between 2022 and 2024. The organisers of such illegal migration aim to provoke a crisis and destabilise European democracies. This is not just a threat to the national security of individual countries but a threat to the entire European civilisation. Moreover, the current conflict between Hamas and Israel shows a potential to escalate tensions in European cities.

Keywords: migration; democracy; security; Islamism; Central Europe; European civilisation

Introduction

What would have recently been labelled xenophobia, racism and misinformation is now, in 2024, considered by more mainstream politicians and media across the European Union member states to be a serious security issue. Therefore, this text will present some current conflicts and phenomena related to mass migration that directly threaten security, whether at the level of individual member states or within the entire European Union. In this context, the governments and parliaments of Finland, Denmark, Iceland, Norway, Sweden, the Netherlands, France and Germany have already approved significant changes to migration policy in

2023–2024. A similar reaction is taking place among the political, media and academic elite in the Czech Republic and Central Europe.

In this context the terrorist attack by Hamas on Israel on 7 October 2023 caused a seismic shift in perspectives in the military, security, diplomatic and psychological contexts, not only in the Middle East but also in adjacent Europe. Religious anger spilled into the streets of European cities in the form of massive demonstrations and terrorist attacks. Europe is experiencing a turning point in its view of reality. The dangers stemming from mass migration from different world civilisations, particularly from the Middle East, Africa and parts of Asia, can no longer be ignored. It is paradoxical that Europe is discovering what has long been discovered. This is due to the mainstream ideology of progressivism, associated with boundless humanism and blindness that did not allow a deep understanding of the disruption. Those who dared to criticise the unrestrained migration policy were labelled populists or anti-system enemies – extremists, racists or xenophobes.

Europe has lost 20 years that it will never get back. Yet, in 2005, a book by the classic political scientist and expert on extremism, Giovanni Sartori, was published in Czech under the title *Pluralism, Multiculturalism, and Immigrants. An Essay on a Multiethnic Society*. Sartori addresses the question of to what extent an open society can accept migrants from ethnically, culturally and religiously different parts of the world without disintegrating. He refers to "the degree of openness that does not lead to the self-destruction of society, to its explosion or implosion" (Sartori, 2005, p. 13). Sartori's central focus is Islamic fundamentalism, whose values are at odds with the rules of democracy.

The conclusions of Sartori's analysis have been confirmed by world events over the last three decades: the terrorist attack on Manhattan in September 2001, the failure of the Arab Spring in 2010–2012, the rise of the Islamic State (ISIS) between 2014 and 2019, the end of the secular state in Turkey during President Recep Tayyip Erdoğan's tenure after 2014, the migration crisis in Europe from 2015 to 2024, and the explosion of anger in the Muslim world in the wake of the war between Hamas and Israel in 2023–2024. Let us now compare the following thoughts of Sartori with the present.

Sartori – Pluralism, Multiculturalism and Immigrants

(1) Sartori: "The political community has regarded internal division as a threat to its survival for millennia and has demanded unity without division from its subjects (…) Multiculturalism represents a historical break (…) emphasizing contradictions, (…) creating strengthened identities by blending and overlapping, for example, language, religion, ethnicity, and ideology (…) Multiculturalism involves

the disintegration of the pluralist community into subgroups of closed and homogeneous communities" (Sartori, 2005, p. 77).

Present: Merkel's welcoming policy in 2015 caused the greatest destabilisation of Europe in the 21st century. Western Europe's absorption capacity was exceeded. The result was terrorist attacks, mass riots, a rise in crime including attacks on women, drug gangs and no-go zones in suburbs. This affects France, Germany, the United Kingdom, Belgium, Sweden and other countries. The theory and practice of multiculturalism failed under the conditions of extreme migration from different cultural and religious spaces.

(2) Sartori: Immigrants differ in four basic distinctions: language, customs, religion and ethnicity. "The first two represent surmountable differences, while the latter two pose a problem of fundamental difference". Regarding religion, the contrast between Islam and Christianity is particularly striking (p. 65). "Jews, Indians, and Asians belong to flexible and segmented cultures capable of maintaining a balance between remaining closed and being open. Islam in its crude form, as exported to Europe, lacks this flexibility" (Sartori, 2005, p. 91).

Present: In an open letter in 2021 addressed to French President Macron, twenty retired generals, a hundred officers and over a thousand soldiers warned of Islamism, civil war and the breakdown of democracy (Jemelka, 2021). In June 2023, the main participants in extensive rioting in France were immigrants uninterested in education or learning the local language, but only interested in social benefits. The religious and political demands of local imams are escalating.

(3) Sartori: "The immigration problem is not only caused by cultural distance (…) but also by the number, i.e., the quantity of immigrants. A foreign population of around 10 percent may still be an acceptable quantity (…) and if it reaches 30 percent, it is almost certain to encounter strong resistance. Would such resistance be an expression of racism? Let us admit that it would (without agreeing with it): but this racism was caused by those who provoked it" (Sartori, 2005, p. 73).

Present: According to political scientist Petr Sokol (2023), there are over 20 million Muslims in the European Union, and their number is growing due to new migration and higher birth rates. There are over 4 million Muslims in the United Kingdom and nearly 5 million in Germany. In France, there are 5.7 million, which is almost 10 percent of the population. Muslims in Belgium, the Netherlands, Austria and Sweden are approaching 10%. Current migration contributes to a higher proportion of Arabs among Muslims. They are concentrated in large cities. For example, migrants make up nearly 40% of the population in Berlin's Neukölln and Brussels' Molenbeek.

(4) Sartori: "Scholars always conscientiously distinguish between open, reasonable Islam and closed, rejecting Islam. At the mass level, however, there has been a revival and rekindling of Islam in its purest form, that is, fundamentalist Islam. (…) Authentic Islam creates militant groups that seek to achieve three goals through

actions (violent, if necessary): cleanse the Muslim world, convert partially Muslim countries, revive the holy war (jihad), and take the West by storm. (…) The West does not take these things seriously, nor does it even understand them anymore. But this is a mistake" (Sartori, 2005, pp. 85–86).

Present: Western Europe has experienced countless terrorist attacks. In France alone, 20,120 people are listed as at risk of radicalisation towards terrorism. Of these, 5,300 individuals are actively monitored by state security forces. Most of them are foreigners, whether they are in the country legally and illegally (Hampejs, 2023). Due to the war between Hamas and Israel in Gaza, the number of Islamic radicals is expected to increase. What is the threshold beyond which security forces can no longer monitor all at-risk individuals, leading to the collapse of civil peace?

(5) Sartori: "In the age of mass media and media bombardment, there can be sudden and intense awakenings from lethargy. The power of this flame must be understood" (Sartori, 2005, p. 85).

Present: In November 2023, the leaders of the Muslim world – Erdogan, Sisi, Raisi and others – expressed their anger over the war in Gaza at an extraordinary summit in Riyadh. This anger may influence the Arab and Muslim public for a whole generation. This anger permeates Western and Northern Europe, splitting and disintegrating it (ECHO24 ČTK, 2023a). In October 2023, the newspaper *Bild* issued a nationwide manifesto titled "Germany, We Have a Problem!" It states: "Our worldview, our values are in danger, the events in Israel have shown how many people literally hate us and our values, how many of those who enjoy our hospitality raise their children to hate us and how many are willing to join terrorists to destroy us" (Bild, 2023).

The Threat of the Balkanisation of Europe

Europe and democracy face new threats. Until now, the prevailing opinion was that the greatest internal threat was the so-called illiberal democracy embodied by Viktor Orbán. However, there is now a growing concern over so-called progressive democracy. This shift is occurring because paradoxically it presents itself as a barrier against adversaries, yet on the other hand, it allows them to enter the heart of Europe. This concerns Chancellor Merkel's 2015 welcoming migration policy, a policy which has caused the greatest destabilisation of Europe in the 21st century. It became a Trojan horse for the infiltration of influence by millions of people from different civilisations which adhere to intolerant cultures and religions.

In the autumn of 2021, the secret services of Russia and Belarus transported tens of thousands of migrants to the borders of Poland as a weapon in a hybrid warfare against the West. Using that same destructive strategy, from 2022 to 2024 Putin

and Lukashenko also targeted Finland and the Baltic states – Lithuania, Latvia and Estonia. What further evidence do we need of the destructive nature of welcoming migration policies? Organisers of illegal migration aim to provoke crises and destabilise European democracies. It is not only a threat to the national security of individual countries, it is primarily a threat to the entire European civilisation. Moreover, the current war between Hamas and Israel has the potential to escalate tensions in the streets of European cities, further confirming the destructive effects of mass migration from the Middle East, Africa and parts of Asia.

What would have recently been dismissed as xenophobia and misinformation is increasingly being recognised in 2024 by mainstream politicians and media across EU member states as a serious security issue. The following sections will briefly summarise some of the current conflicts and phenomena related to mass migration that directly threaten security, whether at the level of individual member states or within the entire European Union, and marginally also in neighbouring European countries or the United States of America.

Frontex – European Union Agency for the Protection of External Borders

The European Union Agency for the Protection of External Borders, Frontex, stated that the migration crisis peaked in 2015 when over 1.5 million illegal migrants entered the Union. In 2023, there was a significant increase in the number of illegal border crossings within the Union, the highest since 2016. The majority of migrants came from Syria, Guinea and Afghanistan, with approximately 80% being men, 10% – women and 10% – children. In the first two months of 2024, most migrants came from Mali, Senegal, Mauritania, Bangladesh, Syria and Tunisia (ČTK, 2024; ECHO24, 2024c).

Ramadan in Europe

Frankfurt on the Main became the first city in Germany in 2024 to officially celebrate the largest Islamic holiday of Ramadan, which lasts from 10 March to 9 April. In a city with 100,000 to 150,000 Muslims, representing nearly 15% of the population, this was decided by the local council led by the Social Democrats and the Greens. Frankfurt was adorned with Christmas-like decorations: gold stars, shining crescents, colorful oriental lanterns and huge signs reading "Happy Ramadan". According to a survey by the INSA agency, a total of 71% of Germans consider migration from heavily Muslim countries a high security risk (Plesník, 2024b; ECHO24, 2024b). Similarly, in Italy, for the first time, a primary school administration decided to declare a holiday on the day marking the end of the fasting month of Ramadan. This happened at a school in the Milan metropolitan area, attended by approximately 1,300 children, 40% of whom come from Muslim families (ECHO24, ČTK, 2024b).

Austria

In Catholic Austria, shocking information emerged that the largest religious group in public elementary schools in Vienna is Muslims. In June 2024, Vienna Deputy Mayor Christoph Wiederkehr documented this in statistics. A total of 35% of children in these schools identify as Muslim, 26% have no religion and only 21% identify as Catholic. Another 13% are Orthodox, 2% are Protestant and the rest are labelled as "other" (Zadražilová, 2024d).

Finland

Russia is conducting a hybrid war against Finland and Europe. According to the Finnish Border Guard, Russia and Belarus are organising migration from the Middle East, Africa and Asia, particularly from Afghanistan, Kenya, Morocco, Pakistan, Somalia, Syria and Yemen (Gričová, 2024). In this context, European Commission President Ursula von der Leyen, after meeting with Finnish Prime Minister Petteri Orpo in the city of Lappeenranta, about 30 km from the Russian border, made the following statement in April 2024: "We all know how Putin and his allies instrumentalize migrants to test our defense and try to destabilize us. It is not only about Finland's security but also about the security of the European Union. We are in this together. We should be more Finnish when it comes to security" (Šmídová, 2024).

Ursula von der Leyen also discussed with the Finnish Prime Minister potential measures taken by the European Union and Finland to address hostile migration at Finland's eastern borders (Novák, 2024). Finland decided to close its 1,340-km border with Russia in December 2022 to prevent the smuggling of refugees which would thus provoke a migration crisis. Finland has subsequently extended this measure several times and did so indefinitely in April 2024. The Finnish government closed eight out of nine checkpoints with Russia. The only crossing that remains open is designated solely for railway (particularly freight) traffic (Šmídová, 2024).

The new conservative government of Finnish Prime Minister Orpo has also significantly tightened the asylum law to regulate migration. Henceforth, asylum proceedings will be conducted directly at Finnish borders with the aim of "expediting the return of individuals considered a threat to national security". According to Interior Minister Mari Rantanen, "it is about ensuring national security, which is always a priority, consistent with EU law. (…) We must change the relevant international agreements, also at the EU level". To qualify for Finnish citizenship, an asylum seeker must now reside in the country for at least eight years, instead of the previous five (Zadražilová, 2024b).

France

In December 2023, the centrist government of President Emmanuel Macron passed a new immigration law in Parliament that tightens rules for illegal arrivals. Specifically, it facilitates the expulsion of illegal migrants and limits social benefits. In a country with 67 million inhabitants, approximately 5.1 million foreigners live legally. Additionally, it is estimated that there are approximately 600,000 to 700,000 illegal residents. Two-thirds of French people believe, according to a public opinion poll, that immigration from non-European Union countries poses a threat to the country (ČTK, 2023).

Germany

In 2023, Germany faced the largest wave of illegal migrants since 2015, with over 127,088 illegal migrants arriving – a 38% increase compared to 2022 (ECHO24, ČTK, 2024a). This surge has shocked Germany with a concomitant rise in crime rates. The number of young criminals among foreign nationals has skyrocketed, as confirmed by Interior Minister Nancy Faeser: "We must discuss this openly". Germany recorded the highest level of crime in seven years in 2023. The most significant increase in crime among foreigners was among youths aged 14 to 18, with a year-over-year increase of 31.4%. There was also a notable rise in crime among non-German children under 14, with a 30.9% increase. Drug-related offenses, including cocaine and crack, rose by 30%. Robbery offenses increased by 17.4%, knife attacks by 9.7% and violent crimes by 8.6%. Police officers were attacked more than 106,000 times in the past year, averaging nearly 300 attacks daily, representing a 10% increase (Zadražilová, 2024a).

The Cologne-based Center for Strategy and Higher Management published the *2024 Security Report* indicating that over 80% of German citizens have little or no confidence in the federal government's migration policy. Germans perceive Islamists and migrant clans as the main threats. Three recent events illustrate the situation in Germany. First, in April and May 2024, two events in Hamburg involved thousands of radical Islamists demanding the establishment of a caliphate. It is paradoxical that a group from the organisation Muslim Interaktiv, adhering to Sharia law, was demanding a religious dictatorship that restricts other religions' freedoms and women's rights while insisting on freedom of assembly and expression (Švamberk, 2024). Second, Germany experienced a dramatic increase in knife attacks, with 8,951 incidents in 2023, averaging over 24 knife attacks daily (ECHO24, 2024d). Third, in many German cities, including Bremen, Freiburg, Heidelberg, Mannheim and Munich, women are provided with late-night taxi subsidies to enhance their safety (Zadražilová, 2024c).

The Netherlands

The new Dutch government has announced the strictest migration policy in the country's history. It aims to enforce stricter border controls and asylum seeker regulations. Illegal migrants will face immediate deportation. Additionally, the government plans to restrict labour migration and limit the acceptance of foreign students at Dutch universities (Plesník, 2024c).

Spain – Catalonia, the Canary Islands

Catalonia has the highest immigration rate in all of Spain, making the migrant issue a focal point alongside Catalan independence. Catalan mainstream political parties are increasingly adopting a tougher stance on immigration, particularly against Muslim immigrants, who are seen as a threat to Catalan identity, lifestyle, culture and freedoms. The turning point was in August 2017, when Moroccan nationals carried out a terrorist attack in Barcelona, killing 16 people and injuring at least 100 by driving a van into a crowd on a busy tourist street. Spanish political scientist Marc-Guinjoan Cesenak noted: "They seemed fully integrated, attending local schools and speaking fluent Catalan. There were no signs of radicalization. Their actions shocked the local society, leaving many wondering what went wrong" (Křováková, 2024b).

The Canary Islands have also been impacted by record migration levels. In January 2024 alone, 7,270 illegal migrants from West Africa arrived, a thirteenfold increase from the same month the previous year. In total, 39,910 migrants reached the islands in 2023. To address this growing trend, Spanish Prime Minister Pedro Sánchez visited Mauritania with European Commission President von der Leyen in February 2024, following earlier discussions with Senegal. The influx of new migrants arriving in the Canary Islands via the Atlantic route, from West African countries such as Senegal, Gambia and Mauritania, has drawn criticism across Spain. Regional politicians have especially criticised the central government's decision to relocate some refugees to facilities across Spain to ease the burden on the islands (Křováková, 2024a).

Sweden

Sweden has dramatically shifted its migration policy. Previously hailed as a humanitarian superpower, Sweden embraced an open-door migration policy from 2015 to 2016, registering 160,000 asylum applications in 2015 – the highest in Europe relative to its population. By the end of 2016, the then minister for integration announced that the country had exhausted its capacity for accommodation,

retraining and integration. Within eight years, Sweden in 2023, was described as a nation troubled by gang wars, rising crime, no-go zones, low labour market participation among migrants and the radicalisation of younger immigrants (Plesník, 2024a).

September 2023 saw a record number of murders due to gang wars, with gangs hiring teenage hitmen from disadvantaged groups, mainly children of immigrants. Swedish Prime Minister Ulf Kristersson stated on television: "Sweden has never faced anything like this, and no other European country has seen such a situation". A Swedish military representative confirmed that soldiers are ready to assist the police (Švamberk, 2023). Like other Western European countries, the Swedish government has undertaken a radical revision of its migration policy. It now seeks to streamline the process of returning illegal immigrants to their countries of origin, conditioning financial aid to third countries on their cooperation in repatriation efforts. The government aims to combat the adverse effects of migration on society (ECHO24, ČTK, 2023b).

The United Kingdom of Great Britain and Northern Ireland

British Prime Minister Rishi Sunak has made stopping illegal migration across the English Channel a top priority. In 2023, 29,437 migrants illegally crossed the Channel. The UK now spends over GBP 3 billion annually on asylum application processing, with accommodation costs for migrants in hotels and other facilities reaching approximately GBP 8 million daily. In response, the British government prepared a new immigration law in the spring of 2024, facilitating the deportation of over 30,000 asylum seekers to Rwanda within the first five years. This initiative follows an April 2022 agreement with Rwanda, under which the African nation will receive refugees arriving illegally in the UK in exchange for tens of millions of pounds. The UK hopes the new immigration law will deter migrants from paying human traffickers for Channel crossings (Michálek, 2024; iDNES, 2024; ECHO24, ČTK, 2024c).

Egypt

The Council of the European Union announced in March 2024 that it had provided Egypt with EUR 1 billion in financial aid as part of a long-term package worth EUR 7.4 billion. This aid is intended to support the Egyptian economy and is contingent upon reducing the number of migrants from the region. The EU's financial assistance is linked not only to the increase in Egyptian migrants passing through Libya or the Greek islands of Crete and Gavdos, but also to the tense regional situation regarding the Gaza conflict and Houthi attacks in the Red Sea (ČTK, Novinky, 2024).

The United States of America

The US is also undergoing a significant shift in migration policy. In June 2024, President Joe Biden approved a decree allowing the return of illegal migrants from the Mexican border without access to the US asylum procedure. This marks a substantial tightening of the southern border regime, returning to the original practice implemented in 2018 by President Donald Trump. The new policy includes a rule allowing the immediate return of illegal migrants once the daily quota of 2,500 migrants is exceeded. President Biden adopted this change despite previously criticising similar measures by his predecessor as violations of long-standing asylum rights. The change in Biden's migration policy is influenced by the upcoming presidential elections on 5 November 2024, with public opinion polls indicating that voters view foreign migration as a serious issue (Štěpánek, 2024).

Migration and Progressivism

Why does contemporary Europe face the danger inherent in the logic of the clash of civilisations? Why did the ruling elites fail across Europe during the 2015–2024 migration crisis? Why did they ignore Samuel Huntington's (2001) warnings about the clash of civilisations and allow it to unfold in the very heart of Europe? Why did they disregard Sartori's warning that "once a community from the Third World reaches a critical numerical state, it will begin to demand rights to its own cultural and religious identity and will eventually attack its presumed oppressors (the natives)"? Why did they not heed Henry Kissinger's assertion that, in the case of Germany, "it was a grave mistake to allow so many people of completely different cultures, religions, and beliefs into the country"?

The unbounded migration policy is a product of the new social engineers of the 21st century, radical left-wing progressives who have appropriated language and particularly the concept of liberal democracy, along with related terminology such as humanity, egalitarianism, morality and the far-right. To maintain their exclusive position as the sole interpreters of democracy, they verbally attack dissenting opinions and critical civil society. The mentality of combating perceived domestic enemies forms the basis of the progressive narrative.

Ultimately, the anti-immigration protest in Europe proved to be justified, as the arrival of millions of people from culturally and religiously risky areas caused irreversible demographic changes in Western and Northern Europe. This revealed that it is the proponents of progressivism who hold untenable views in the form of a set of radical dogmas. By doing so, they caused significant damage and losses, destabilising Europe and the entire democratic West.

This was not about random mistakes and errors, but a systemic problem – ideological blindness. They believed, in the words of writer Milan Kundera from his novel *The Joke*, that they had "ridden the back of history" (Kundera, 1968). They thought they would "conduct and create" history. They assigned themselves a leading role in society. They live their story of noble activists. This is part of their psychological makeup, their ideological conviction.

Much stems from the progressive ideology that has dominated the minds of European elite and the public sphere. It aims to revolutionarily transform the unique relationships that have formed on the continent over centuries. Instead of a national home, it offers a European superstate. Instead of protecting borders, it welcomes millions of immigrants from other civilisations, espousing hard-to-reconcile religious and cultural values. Instead of family bonds between a man and a woman, it emphasises the number and variability of genders, so-called transgenderism. In other words, instead of distinct European nations, it offers the utopia of a universal European or world citizen, devoid of nationality, religion, race and clear gender. Instead of natural mutuality and solidarity, it promotes moralistic populism. Instead of earthly joys, it preaches renunciation and bright tomorrows. Instead of a full life, it prefers existence behind the walls of a planetary monastery where a global order prevails.

If we accept the belief that, in the interest of the global good, we must erase differences between people, then all borders, including interstate ones, lose their meaning. This, however, denies the diverse and conflictual nature of the world, burying our heads in the sand with immeasurable consequences. Such boundless egalitarianism and humanitarianism drive Europe into a civilisational vacuum, making it an easy prey for more aggressive cultures and religions.

This time, it is not about socialist nationalisation of land and factories from evil farmers and industrialists, but the expropriation of nation-states, religions, races, and partially also genders. This is happening in the name of establishing a European Babylon and an enlightened supranational bureaucracy aimed at regulating every citizen, every hectare of land, and every dairy cow. Those who disagree are labelled internal enemies – reactionaries and disinformers.

This represents another radical leftist ideology advocating revolutionary engineering and asceticism. At the beginning are bright tomorrows, at the end are conflicts, chaos, disruption and disintegration. The self-harm mainly affects the indigenous European population. For how many times in its history has Europe, in the name of a higher good, disrupted natural human ties and civic organisation?

Migration and National Conservatism

When will progressivism advocates realise that they are uprooting centuries-old human ties and thus undermining the immunity and defence capabilities of the West? When will they understand that, based on the law of action and reaction, they have provoked outrage, and thus to a large extent, generated the counter-wave of defensive national conservatism? The conservative counterwave continues, as evidenced by the results of the European Parliament elections in June 2024.

Progressivism advocates have been promoting unlimited migration for so long that they have disrupted the demographic balance of Europe to the detriment of the indigenous population and to the detriment of democracy as a societal arrangement. It follows that the national conservative movement is genetically linked to progressivism, growing from it, being its offspring. It draws its ethos from the revolt against self-destructive migration policies, the erosion of national and state sovereignty, extreme green transformation, but also from opposition to suppressing opinion pluralism and abusing methods of silencing and disparaging dissenters.

Today, it is fashionable to label protest conservative movements far-right or ultra-right and to portray them as a danger to democracy. This either signifies a misunderstanding or an intent to discredit political and opinion opposition, which contradicts liberal democracy. Within the broad category of anti-progressivism, we distinguish between new right and new left parties. The former, the conservative right, is primarily represented by Giorgia Meloni in Italy and Marine Le Pen in France. The latter includes the conservative left, represented by Robert Fico in Slovakia and Sahra Wagenknecht in Germany. Within this spectrum, there are extreme and moderate positions. It is clear that the conflict between progressivism and national conservatism transcends the left-right dichotomy. In the context of Czech politics, it surpasses and cuts across the contentious party line "Babiš vs. Anti-Babiš".

If progressivism tends toward polarisation and self-destruction, national conservatism may end similarly. This is related to an atmosphere filled with emotions and passions. This is evident in the US presidential campaign, where, within the Republican Party, it was not the moderate conservative Ron DeSantis who succeeded against progressivism, but the radical Donald Trump.

What is lacking today is moderate centrist politics based on dialogue, respect and compromise. A moderate version of national conservatism is thus a challenge for all opposition and governing parties in the Czech Republic. These themes of a moderate version of conservatism are practically lying on the street: national interests and patriotism, stopping illegal migration from culturally and religiously different world civilisations, rational green policies, emphasis on traditional family, respect for minorities, protection of minors from activist pressures to change gender,

reduction of state and union regulations, close cooperation within an intergovernmental European Union and security anchoring in the European pillar of NATO.

These themes represent an imperative. They are a prerequisite for the ability of the Czech Republic, Europe and the collective West to face their own destabilisation and resist the pressure of imperial Russia, expansive China and radical Islamism within the clash of civilisations.

Conclusions

Europe is experiencing a significant security problem with those immigrants who abuse hospitality, have no interest in integrating and threaten to colonise the host country. Western and Northern Europe are most affected, where mass migration from other civilisational circles, particularly from the Middle East, Africa and parts of Asia, has been heading since at least 2015.

In Giovanni Sartori's book (2005), the theme of human boundaries – the boundaries of states, cultures, tolerance, power and diversity – runs like a thread. The theme of boundaries is also central now in 2024. European civilisation needs to guard its boundaries, especially due to the intolerant branch of Islam and the migration organised by Russia and Belarus into Poland, Finland and the Baltic States. In spring 2024, the European Union migration pact was decided. The Czech government took a neutral position, announcing that it would abstain from voting. Minister Martin Kupka stated: "Bureaucracy has increased, effective protection of external borders and effective return policy are becoming complicated" (Martinek, 2024).

These are interconnected vessels: progressivism paves the way for Islamism. European civilisation does not exist in a vacuum; it competes with other global entities. If it weakens its own identity while others strengthen theirs, it loses competitiveness. If it vacates its sphere of influence, it is occupied by other populations with different cultures, religions or ethnicities. These are natural, and thus human, laws that should not be underestimated.

The greatest danger to Western democracies is not Russian disinformation but self-harm orchestrated by their own elites. Under the banner of humanism, they are dismantling European civilisation associated with democracy – that is, the rule of law, civil liberties and gender equality. Europe is Balkanising, turning into Bosnia and Herzegovina. Instead of the declared European harmony, it is approaching a tipping point where national, religious and racial tensions escalate. It is approaching a tipping point where European Trumps will rise. Instead of one "America First" there will be more than thirty different nations "First".

Europe is awakening to a new reality. Finland, Denmark, Iceland, the Netherlands, Norway, Sweden, France and Germany have already announced radical changes in

their migration policies. And what self-reflection is the media, political and academic elite undergoing in the Czech Republic and Central Europe?

Acknowledgment

This chapter is the result of Metropolitan University Prague research project no. 100-1 "Political Science, Media and Anglophone Studies" (2023) based on a grant from the Institutional Fund for the Long-term Strategic Development of Research Organizations.

References

Bild. (2023, November 1). *Padesát bodů pro život v Německu.* https://www.bild.de/politik/inland/politik-inland/deutschland-wir-haben-ein-problem-hier-lesen-sie-das-bild-manifest-85895408.bild.html; https://neviditelnypes.lidovky.cz/zahranici/bild-padesat-bodu-pro-zivot-v-nemecku.A231031_143033_p_zahranici_nef

ČTK. (2023, December 20). *Francie zpřísnila pravidla pro imigranty, omezí sociální dávky*. https://www.novinky.cz/clanek/zahranicni-evropa-francie-zprisnila-pravidla-pro-imigranty-omezi-socialni-davky-40454825

ČTK. (2024, January 16). *Frontex hlásí 380 000 nelegálních vstupů do Evropské unie. Přibylo jich nejvíce od roku 2016*. https://www.irozhlas.cz/zpravy-svet/nelegalni-vstupy-evropska-unie-frontex-migrace_2401161544_ano

ČTK, Novinky. (2024, April 12). *EU pošle Egyptu miliardu eur, aby snížil počet migrantů*. https://www.novinky.cz/clanek/zahranicni-evropa-eu-posle-egyptu-miliardu-eur-aby-snizil-pocet-migrantu-40467699

ECHO24. (2024b, March 5). *Jako o Vánocích. Německý Frankfurt rozzáří výzdoba v rámci islámského ramadánu*. https://echo24.cz/a/H2x2g/zpravy-svet-frankfurt-nad-mohanem-rozzarila-svetla-pri-oslavach-ramadanu

ECHO24. (2024c, March 26). *Kriminalita v Německu výrazně vzrostla, spolkové orgány viní nekontrolovanou migraci*. https://echo24.cz/a/HFSET/zpravy-zahranici-kriminalita-vyrazne-vzrostla-nemecko-migrace-spolkove-zeme

ECHO24. (2024d, June 1). *V Německu prudce roste počet útoků nožem, za minulý rok bylo 8 951 případů*. https://echo24.cz/a/HxhQV/zpravy-svet-nemecko-rust-pocet-utoky-nuz

ECHO24, ČTK. (2023a, November 11). *Dorazil i Asad. Erdogan, Sísí, Raísí a další. „Rozzuření" muslimové se sjeli do Rijádu kvůli Gaze*. https://echo24.cz/a/HJa8F/zpravy-svet-dorazil-asad-erdogan-ssisi-raisi-rozzureni-muslimove-sjeli-rijadu-kvuli-gaze

ECHO24, ČTK. (2023b, December 26). *Historická revize. Švédsko chce kvůli vyhoštěným migrantům omezit zahraniční pomoc*. https://echo24.cz/a/HF8xe/zpravy-svet-svedsko-

omezi-zahranicni-pomoc-zemim-ktere-odmitnou-prijimat-vyhostene-migranty?utm_source=www.seznam.cz&utm_medium=sekce-z-internetu#dop_ab_variant=1198401

ECHO24, ČTK. (2024a, January 5). *Německo čelí největší vlně ilegálních migrantů od roku 2015*. https://echo24.cz/a/HQzZ3/zpravy-svet-nemecko-celi-nejvetsi-migracni-vlne-od-roku-2015

ECHO24, ČTK. (2024b, March 18). *Poprvé. Základní škola v Itálii vyhlásila volno kvůli konci ramadánu*. https://email.seznam.cz/?i&q=label-id%3A262&mid=126712

ECHO24, ČTK. (2024c, April 22). *První lety s migranty vyrazí do Rwandy do 12 týdnů, řekl Sunak*. https://echo24.cz/a/HGMjp/zpravy-svet-sunak-prvni-letadla-s-migranty-vyrazi-do-rwandy-do-12-tydnu

Gričová, A. (2024, January 18). *Migranti jako zbraň. Podle finské rozvědky se Rusko snaží uprchlíky verbovat ke špionáži*. https://ct24.ceskatelevize.cz/clanek/svet/migranti-jako-zbran-podle-finske-rozvedky-se-rusko-snazi-uprchliky-verbovat-ke-spionazi-345070

Hampejs, M. (2023, October 21). Macron chce nelítostný stát. *Lidové noviny*, 5.

Huntington, S. (2001). *Střet civilizací. Boj kultur a proměna světového řádu*. Rybka Publishers.

iDNES. (2024, January 20). *Britové cvičí deportace migrantů do Rwandy, v hangáru zkoušejí různé scénáře*. https://www.idnes.cz/zpravy/zahranicni/britanie-spojene-kralovstvi-rishi-sunak-premier-deportace-vyhosteni-nelegalni-migranti-migrace-laman.A240119_124050_zahranicni_dtt

Jemelka, P. (2021, April 27). *Dvacet vysloužilých generalů hrozí Macronovi pučem, pokud nezatočí s islamisty*. https://www.novinky.cz/clanek/zahranicni-evropa-dvacet-vyslouzilych-generalu-hrozi-macronovi-pucem-pokud-nezatoci-s-islamisty-40358481

Křováková, K. (2024a, February 19). *Nová vlna připlouvajících migrantů testuje španělskou vstřícnost*. https://www.seznamzpravy.cz/clanek/zahranicni-silici-vlna-priplouvajicich-migrantu-testuje-vyjimecnou-spanelskou-laskavost-245407

Křováková, K. (2024b, April 13). *Hrozba pro naši identitu. V Katalánsku roste nevraživost vůči migrantům*. https://email.seznam.cz/?i&q=label-id%3A262&mid=127350

Kundera, M. (1968). *Žert*. Československý spisovatel.

Martinek, J. (2024, February 7). *Česko migrační pakt v EU nepodpoří*. https://www.novinky.cz/clanek/domaci-cesko-nepodpori-evropsky-pakt-o-migraci-40459950

Michálek, M. (2024, April 15). *Uniklé dokumenty: Britský plán deportací do Rwandy má stát miliardy liber*. https://www.seznamzpravy.cz/clanek/zahranicni-unikle-dokumenty-britsky-plan-deportaci-do-rwandy-ma-stat-miliardy-liber-249925

Novák, L. (2024, April 19). *Von der Leyenová: Rusko chce migrací destabilizovat Finsko*. https://eurozpravy.cz/zahranicni/von-der-leyenova-rusko-chce-migraci-destabilizovat-finsko.06tixkgy

Plesník, V. (2024a, January 18). *Musíme začít bourat mešity. Švédská pravice se proti islamistům ozývá čím dál hlasitěji*. https://www.novinky.cz/clanek/zahranicni-evropa-musime-zacit-bourat-mesity-svedska-pravice-se-proti-islamistum-ozyva-cim-dal-hlasiteji-40457576#dop_ab_variant=1164111

Plesník, V. (2024b, March 6). *Frankfurt nasvítí ramadán. Signál ve prospěch života muslimů, vysvětlilo vedení města*. https://www.novinky.cz/clanek/zahranicni-evropa-frankfurt-nasviti-ramadan-signal-ve-prospech-zivota-muslimu-vysvetlilo-vedeni-vyzdobu-mesta|-40463026

Plesník, V. (2024c, May 17). *Nová nizozemská vláda ohlásila nejpřísnější migrační politiku v dějinách země*. https://www.novinky.cz/clanek/zahranicni-evropa-nova-nizozemska-vlada-ohlasila-nejprisnejsi-migracni-politiku-v-dejinach-zeme-40472287

Sartori, G. (2005). *Pluralismus, multikulturalismus a přistěhovalci. Esej o multietnické společnosti*. Dokořán.

Sokol, P. (2023, November 2). Kdo v Evropě podporuje Hamás. *Reflex*, 17.

Šmídová, H. (2024, April 19). *Úředník Evropské unie von der Leyen navštíví finsko-ruskou hranici, aby zhodnotil bezpečnostní situaci*. https://novinky.news/urednik-evropske-unie-von-der-leyen-navstivi-finsko-ruskou-hranici-aby-zhodnotil-bezpecnostni-situaci/

Štěpánek, V. (2024, June 5). Biden přitvrzuje na jižní hranici. *Lidové noviny*, 6.

Švamberk, A. (2023, September 29). *Švédsko hlásí rekordní počet vražd. Do boje s gangy chce zapojit armádu*. https://www.novinky.cz/clanek/zahranicni-evropa-svedsko-hlasi-rekordni-pocet-vrazd-do-boje-s-gangy-chce-zapojit-armadu-40445073

Švamberk, A. (2024, May 12). *V Hamburku znovu žádalo přes dva tisíce islamistů vznik chalífátu*. https://www.novinky.cz/clanek/zahranicni-evropa-v-hamburku-znovu-zadalo-pres-dva-tisice-islamistu-vznik-chalifatu-40471378

Zadražilová, J. (2024a, April 10). *Drogy, loupeže, útoky nožem. V Německu explodoval počet násilných činů u mladých cizinců*. https://email.seznam.cz/?i&q=label-id%3A262&mid=127270

Zadražilová, J. (2024b, April 19). *Finsko razantně zpřísňuje azylom zákon, naštvalo tím německou vládu*. https://www.novinky.cz/clanek/zahranicni-finsko-razantne-zprisnuje-azylovy-zakon-nastvalo-tim-nemeckou-vladu-40468559

Zadražilová, J. (2024c, May 13). *Německá města se bojí o bezpečnost žen. V noci jim přispějí na taxi*. https://www.novinky.cz/clanek/zahranicni-nemecka-mesta-zavadi-pro-zeny-prispevek-na-nocni-taxi-boji-se-o-jejich-bezpeci-40471454

Zadražilová, J. (2024d, June 11). *Katolické Rakousko v šoku. Muslimů je na vídeňských základních školách víc než křesťanů*. https://www.novinky.cz/clanek/zahranicni-evropa-katolicke-rakousko-v-soku-muslimu-je-na-videnskych-zakladnich-skolach-vic-nez-krestanu-40475859

KATARZYNA MARZĘDA-MŁYNARSKA

MARIA CURIE-SKŁODOWSKA UNIVERSITY, LUBLIN

The Limits of Technocratic Decision-Making: The 2015 European Union Relocation Policy and the Blind Spot Theory

Abstract: The 2015 European Union migration crisis exposed critical weaknesses in the EU's governance framework, particularly in its technocratic approach to crisis management. This article examines the EU's relocation policy through the lens of the "blind spot" theory, which highlights the organizational and cognitive limitations in decision-making processes. Despite the EU's comprehensive migration governance system, the relocation policy failed due to its narrow technocratic focus, overlooking the socio-political and cultural dimensions of the crisis. The study reveals that the EU's reliance on rational decision-making and expertise, typical of its bureaucratic nature, led to significant blind spots. These blind spots, characterized by incomplete information processing and lack of peripheral vision, resulted in unintended consequences such as increased divisions among member states, secondary migration flows, and the rise of populist movements. The article underscores the need for a more holistic approach in EU policy making that integrates technical solutions with broader human and political considerations.

Keywords: 2015 migration crisis; technocratic decision-making; European Union; blind spot theory

Introduction

In analyses of the 2015 EU migration crisis, much attention is given to political tensions and the clash of visions regarding EU migration policy represented by different member states. The failure of the EU's responses to the migration crisis, and the relocation policy in particular, is commonly associated with the attitudes of populist governments in Central and Eastern Europe towards migrants and their reluctance to share the responsibility. While this interpretation may be partially true, it omits the core problem embedded in the EU's reaction to the crisis. The weakness of the EU's response, as this article will attempt to demonstrate, lies in the technocratic

approach adopted to address the problem. This type of governance, based on expertise and rational decision-making typical of political and bureaucratic elites, proved ineffective when applied to the migration crisis. Using the blind spot concept as a theoretical framework, this article aims to show that the failure of the EU's response to the 2015 migration crisis was due to the underestimation of the human factor in the proposed solution, particularly in the context of the relocation policy.

The article consists of four parts. The first one briefly characterizes the migration governance system in the EU. Part two discusses the blind spot concept and its usefulness as an analytical tool. The main objective of this part was to develop an analytical model to analyze the EU's response to the 2015 migration crisis (part three) and in particular the relocation policy (part four). The analysis is based on secondary sources: books and articles, as well as documents and legal acts related to EU migration policy. The source material was collected using the desk research method. Qualitative methods, in particular content analysis, were used to analyze the collected material.

The EU Migration Governance System

The European Union has the most comprehensive model of regional migration governance in the world (Ceccorulli et al., 2021). It addresses mobility, social rights, security, and provides supranational enforcement mechanisms. It consists of two governance mechanisms: inward, i.e. the internal migration of EU citizens, and outward, i.e. the migration of people from third states. These cannot be treated separately, but rather as two sides of the same coin. The free movement of people within the EU (EU nationals) is part of the broader concept of the single market (Grabbe, 2006). It was included alongside capital, goods, and services as one of the four fundamental freedoms of the European single market. The right to free movement is treated as a fundamental EU principle and is enshrined in the Treaty on the Functioning of the European Union (Consolidated Version, 2024). The second EU migration governance mechanism is directed toward third-state nationals who want to enter EU territory. It includes policies on legal and illegal migration as well as an asylum policy. While many illegal immigrants who enter EU territory claim asylum or refugee status, the asylum policy is a key element of the EU's external migration governance framework in this context (Zaun, 2017).

The aim of the EU asylum policy is to harmonize asylum procedures across member states by establishing common asylum arrangements. Work on this initiative began in 1999. Over the next six years (1999–2005), several legislative measures harmonizing common minimum standards for asylum were adopted. These include the Temporary Protection Directive (Council Directive, 2001), which allowed for a common EU response to a mass influx of displaced people unable to return to

their country of origin, and the creation of the European Refugee Fund,[1] aimed at strengthening financial solidarity between member states. The establishment of the new common European asylum system was completed in 2013 with the adoption of the amended Dublin Regulation (Dublin III, 2013; Lovec, 2017) and the Regulation on Eurodac (Regulation No 603/2013 of the European Parliament and of the Council of 26 June 2013). The revised Dublin Regulation aimed to establish the responsibility of member states for processing asylum applications (specifically, the first member state the asylum seeker reaches). On 10 April 2024, the European Parliament voted in favour of new migration legislation – The Pact on Migration and Asylum (Regulation (EU) 2024/1351 of the European Parliament and of the Council of 14 May 2024 on asylum and migration management, amending Regulations (EU) 2021/1147 and (EU) 2021/1060 and repealing Regulation (EU) No 604/2013). It was formally adopted by the EU Council on 14 May 2024. This new legislation establishes a common asylum system that will come into force in 2026.

The complexity of the EU's Common European Asylum System reflects a technocratic approach, wherein asylum seekers are treated through rational decision-making and standardized rules. The intention behind such a comprehensive system is to prepare the EU for any migration-related situation that may arise in the future. Based on previous experience, such a system works when the rational conditions considered during its setup are met – specifically, when the number of asylum seekers is stable and does not exceed the average. However, the migration crisis in 2015 revealed its weaknesses. The EU's response to the mass influx of people was perhaps rational from a bureaucratic point of view but proved completely ineffective given the scale of the crisis. Both the perception of the problem and the solutions proposed contributed to the ultimate failure of the EU's response to the migration crisis.

A number of studies have been published to explain why the EU was unable to solve the problem despite having such a well-developed governance system (Cusumano & Riddervold, 2023; Börzel, 2016). A commonly highlighted factor was the lack of solidarity between EU Member States, followed by the high politicization of the crisis in public discourse, particularly by populist movements, which found it to be a convenient issue to exploit. This study proposes an explanation that shifts attention from the political to the organizational context. There is no doubt that the European Union, as a bureaucratic organization, is subject to the same principles as national administrations. The way in which problems are perceived and solved is strongly influenced by a specific organizational culture. This study will use the concept of "blind spots" as a theoretical framework to explain how the organizational context of the European Union determined the proposed solutions and why, in the long run, they proved ineffective.

[1] European Refugee Fund established in 2000, was replaced by Asylum Migration and Integration Fund in 2014.

The "blind spot" concept as an analytical tool

The term "blind spot" is derived from medicine and refers to a spot on the optic nerve that lacks receptor cells and cannot receive information, causing the blind spot (Merriam Webster Medical Dictionary, n.d.). The concept of the "blind spot" has been adopted in various disciplines and fields of study.[2] Its appeal lies in identifying the unconscious aspects of an individual's functioning, which inadvertently influence their actions. In psychology, the concept of the blind spot is used to analyse individuals' behaviour. Particularly notable is the phenomenon of the bias blind spot, which refers to the cognitive bias where an individual recognizes the influence of biases on others' judgment while failing to see the impact of biases on their own judgment. According to the blind spot mechanism, people tend to believe they are less biased than others, regardless of their actual decision-making abilities (Pronin et al., 2002).

The term, coined by social psychologists, has been used as a theoretical framework for leadership analysis (Schramer, 2008). Its explanatory potential has also been recognized by social scientists, who use it to study institutional failures that produce undesirable result – unintended consequences in social sciences in general and executive government in particular (Bach & Wegrich, 2019b). In this context, the blind spot is a distinct subset of phenomena defined by the unknown inability to detect and process potentially critical information, relating to the selective perception of problems and solutions (Lodge, 2019).

The use of the blind spot concept to analyse decision-making processes in public organizations is a relatively new research approach. Its analytical potential was fully demonstrated in the publication entitled *The Blind Spots of Public Bureaucracy and the Politics of Non-Coordination*, edited by Tobias Bach and Kai Wegrich, published in 2019. The book is based on the assumption that the blind spot is an inseparable feature of any organization. The blind spots, defined "as not seeing the not seeing" (Lodge, 2019, p. 29), relate to the biases that affect the handling of information flows and, as a result, limit vision. The authors of the volume identify four biases in organizational decision-making behaviour that emerge from the intentionally rational behaviour of bureaucratic organizations operating in political contexts: "selective perception", "Achilles' heels", "bureaucratic politics", and "blind spots" (Bach & Wegrich, 2019a, p. 6). These biases have been developed based on two criteria: the type of organizational behaviour (intended vs. unintended) and the

[2] The term "blind spots" in IT sector highlights the limitations and overlooked issues in AI development and ethical guidelines; in psychology refers to cognitive biases; in politics refers to areas of ignorance, oversight, or bias that affect political decision-making; in economics, refers to areas or issues that are often overlooked, under-researched, or inadequately addressed such as cultural and social factors; in history, refers to areas or aspects of the past that have been overlooked, marginalized, or inadequately studied such as Non-Western Histories.

type of analytical perspective (focus on structure vs. focus on identity). As a result, four categories of biases can be distinguished: 1) intended, focused on structure – "selective perception"; 2) intended, focused on identity – "bureaucratic politics"; 3) unintended, focused on structure – "Achilles' heels"; 4) unintended, focused on identity – "blind spots" (Bach & Wegrich, 2019a, p. 11).

While the element of unintentionality is evident in the context of blind spots, their specificity is also due to the fact that they are rooted in the institutional nature rather than the formal structure of an organization (Bach & Wegrich, 2019a, p. 19). The institutional nature of an organization results from informal values and norms, which strongly influence its behavior. Consequently, a distinct organizational identity is created, recognized by employees and stakeholders (Bach & Wegrich, 2019a, p. 8). The institutional nature of an organization creates the environment in which the normal processes of organizational life take place, and blind spots are the unintended consequences of these processes, reflected in the organization's institutional features.

The conceptualization of blind spots draws attention to the organization's unawareness of its incomplete information processing – its inability to detect and categorize potentially important information, without being aware of this inability (Bach & Wegrich, 2019a, p. 19). This inability results from institutional features such as: the frames used in processing information, the type of expertise within an organization, insulation from feedback from the wider environment (due to the concentration of professionals whose background can shape the organization's view, or a lack of effective feedback loops), and the worldviews cultivated as part of organizational identity (Bach & Wegrich, 2019a, p. 21).

The concept of blind spots developed in the aforementioned publication offers analytical categories (Bach & Wegrich, 2019b) that will be used to analyze the EU's reaction to the 2015 migration crisis and its relocation policy. These categories include:

– organizational identity features (frames used in processing information, expertise, communication with the external environment, worldviews),

– the way the problem is perceived and solved ("tunnel" vision – lack of peripheral vision, operating procedures),

– key features of blind spots (lack of actions despite available information, absence of information due to the lack of measuring tools to detect changes in the environment and inside the organization, inability to identify causes),

– types of blind spots (structurally generated – emphasis on procedures; culturally generated – emphasis on cultural compatibility; generated by myths and reputation management – emphasis on double talk and types of reputation – performative, moral, technical, procedural).

The "blind spots" in the EU reaction to the 2015 migration crisis

The 2015 migration crisis posed one of the most significant challenges in the history of the European Union. The arrival of over a million asylum seekers highlighted profound inadequacies in the EU migration and asylum policies.

The EU, particularly through the European Commission, operates as a technocratic organization. As a repository of knowledge and expertise, the Commission is mandated to act in the general European interest, independent of political pressures (Nugent, 2010). This technocratic identity shapes its problem-solving approaches, emphasizing rational and technical solutions while avoiding politicization. The Commission's worldview, influenced by rationalism and positivism, fosters a belief in controlling historical processes through expertise and universal values. Consequently, the Commission tends to adopt a one-size-fits-all approach, assuming that rational, expert-based decisions are the best responses to complex problems (European Commission, 2024).

The technocratic nature of the EU is well-documented, especially its reliance on technocratic governance (Majone, 1996) and expertise-based approach to policy-making (Radaelli, 1999). These perspectives explain why the European Commission tends to frame migration issues in technical terms, focusing on resource management and legal frameworks rather than the human and political dimensions of the crisis.

Undoubtedly, the features of the EU's organisational identity strongly influenced its perception of the 2015 migration crisis and the strategies adopted to address it. The EU's approach to the crisis reflected the lack of peripheral vision and focusing narrowly on technical dimensions. During the crisis, the European Commission adopted an evidence-based, neutral, and scientific approach to manage migration, especially emphasizing the redistribution of asylum applications to alleviate pressure on border states. However, this type of governance perspective ignored broader social, political and cultural factors, which ultimately limited the effectiveness of the response, which was criticised both before and after the crisis (Boswell, 2009; Geddes & Scholten, 2016). As a result, the EU failed to take into account the broader context, which should have included Member States' political reservations and societal attitudes on the one hand and, most importantly, asylum seekers' preferences on the other.

A significant problem limiting the EU's ability to move beyond a narrow – technocratic – perspective has been the process of gathering and processing information that serves as a basis for decision-making. In this context, one can speak of the EU's struggle to take into account different perspectives and information in the policy-making process, highlighting the challenges of vertical policy-making (Guiraudon, 2000). As well as the EU's difficulties in dealing with the complex and

diverse aspects of migration (Bendel, 2005), pointing out that incomplete information processing can lead to inadequate and ineffective policies. It can therefore be stated that the institutional constraints due to the technocratic nature of the EU resulted in incomplete information processing by the European Commission during the crisis and a failure to take into account critical data and feedback from various stakeholders. For example, the Commission did not adequately address objections from Member States opposing the relocation process, criticism from the President of the European Council or concerns about potential security threats from terrorists hiding among asylum seekers. Most importantly, however, the European Commission completely ignored asylum seekers' preferences regarding countries of destination, existing migration networks in Western Europe, attitudes of host communities, language and cultural barriers and resource constraints reported by Member States.

As a result, the EU's response to the 2015 migration crisis led to several unintended consequences, revealing significant blind spots in its approach to the problem. These consequences included increased divisions and hostility between EU Member States, the European Commission's limited ability to build consensus on migration issues, divergent positions between EU institutions, the lack of significant improvement in the situation in border countries, the secondary flow of asylum seekers to Western European countries and the strengthening of anti-immigrant movements and populist parties.

Structurally, the technocratic nature of the European Commission has led to a narrow perception of the problem, ignoring the political and human dimension. This has resulted in polarisation among member states and strengthened anti-immigration positions. Culturally, the incompatibility in migration conditions between Western and Eastern Europe was overlooked. The Commission ignored culturally determined factors such as language, social attitudes and migration networks, which led to secondary movements of relocated migrants. From the reputational point of view, the Commission's efforts to demonstrate its efficiency and effectiveness led it to disregard criticism and undermined its ability to build consensus among Member States.

Undoubtedly, the 2015 migration crisis revealed significant gaps in the EU's migration policy, stemming primarily from its technocratic approach. While this approach may be effective on technical issues, it has failed when dealing with complex, politicised human factors issues such as the migration crisis. The EU's reliance on rational decision-making and expertise, without adequately considering the political, cultural and social dimensions, ultimately led to unintended consequences that, rather than providing a solution, brought an impasse and deep divisions between Member States.

The "blinds spots" in the EU relocation policy

The European Union's response to the 2015 migration crisis stands as a striking example of the limitations inherent in technocratic governance. Amidst the influx of over a million refugees and migrants, the EU devised a relocation policy aimed at equitably distributing asylum seekers across member states. This policy, envisioned as a fairness mechanism, sought to centralize decision-making at the EU level to alleviate the pressure on frontline states like Greece and Italy. However, despite its rational design and technocratic foundation, the policy floundered, revealing significant blind spots that hindered its implementation and effectiveness.

Undoubtedly, relocation policy was one of the most contentious and ultimately unsuccessful measures taken by EU institutions to address the 2015 migration crisis. Despite its intent, the policy failed to meet its targets. The plan, adopted in 2015 by a majority of EU interior ministers presumed that if the number of asylum-seekers in a member state reaches over 150% of a predetermined reference number, all further new applicants in that country are relocated across the EU until the number of applications is back below the reference number. If a member state refuses to take part in the relocation scheme, it must make a "solidarity contribution" of EUR 250,000 for each applicant for whom it would otherwise have been responsible to the member state that receives the person. None of these policies have been fully realized. At the end of 2018, it turned out that only 44,000 of asylum seekers from the EU border countries had been relocated, from the assumed 160,000. None of the opposing states have paid the assumed penalties (European Commission, 2016, 2024; European Court of Auditors, 2023).

The relocation policy was designed to redistribute asylum seekers based on quotas, on the assumption that a centralized, rational approach could effectively manage the influx. This meant that the Commission viewed the migration crisis more as a logistical and administrative challenge. The EU's approach to the relocation policy was emblematic of a technocratic tunnel vision. The Commission perceived the crisis through a narrow lens, focusing primarily on the managerial aspects of asylum application processing. The policy aimed to redistribute asylum seekers from overburdened states to other member states until the numbers normalized. If a state refused to participate, it was required to make a financial contribution, envisioned as a penalty for non-compliance. This technocratic focus on resource allocation and administrative efficiency overlooked critical political and cultural dimensions. Member states, particularly in Central and Eastern Europe, voiced strong opposition to the mandatory quotas, citing concerns over national sovereignty and cultural identity (Trauner, 2016). The Commission's reliance on technical solutions failed to engage with these political realities, leading to significant resistance and non-compliance.

A fundamental flaw in the EU's approach to the 2015 migration crisis, reflected in relocation policy, was its incomplete processing of crucial information. The Commission did not fully consider several vital factors that could have influenced the policy's success. These included the strong objections from certain member states, critiques from EU leadership, the preferences of asylum seekers, and the existence of robust migration networks in Western Europe. Moreover, the Commission overlooked the socio-political climates and capacities of host communities. The policy did not adequately address the cultural and linguistic barriers that would affect integration, nor did it consider the limited resources and varying circumstances of different member states. This oversight contributed to the policy's ineffectiveness and the uneven implementation across the EU. The relocation policy's blind spots led to several unintended consequences that undermined its goals. Firstly, the policy deepened divisions within the EU, with mandatory quotas perceived as an infringement on national sovereignty, fostering resentment and resistance (Schmidt, 2019). This division hindered the policy's implementation and weakened EU cohesion.

Secondly, the policy's failure to account for asylum seekers' preferences resulted in secondary movements, where relocated individuals moved from their assigned countries to preferred destinations such as Germany and Sweden. This secondary migration undermined the goal of equitable burden-sharing and placed additional strain on the already overburdened systems in these preferred countries.

Additionally, the policy inadvertently fueled the rise of anti-immigrant and populist movements across Europe. The perceived imposition of migrant quotas became a rallying point for nationalist parties, which capitalized on public fears and anxieties to gain political traction,what happened in Poland, helping the conservative Law and Justice to win the 2015 elections. This political shift further complicated the EU's ability to formulate and implement cohesive migration policies.

Structurally, the European Commission's technocratic nature led to a narrowed problem perception that overlooked critical political and human factors. The Commission's focus on technical solutions and rational decision-making processes failed to engage with the complex socio-political landscape of migration. Culturally, the policy ignored significant differences in migration conditions between Western and Eastern Europe. Factors such as language barriers, social attitudes towards migrants, and existing migration networks were not adequately considered. This oversight resulted in the unintended secondary movements of relocated migrants from Eastern to Western European countries, undermining the policy's effectiveness. Reputationally, the Commission's drive to demonstrate its efficiency and governance capabilities led to a dismissal of critical feedback and opposition. This pursuit of a positive image and perceived effectiveness resulted in a lack of consensus-building and further entrenched divisions within the EU.

Conclusions

In 2015, the EU faced one of the biggest crises in its history. The problem, however, was not in the nature of the crisis itself, but in the "mental trap" revealed by the way the EU addressed the migration crisis. The technocratic approach, a characteristic feature of every bureaucratic organization, can be effective when applied to technical, highly specific problems with low potential for politicization due to the involvement of expert knowledge, which is typically confined to a narrow elite. However, when it comes to the governance of mass flows of people, this approach often proves ineffective because it underestimates the human factor in rational decision-making. The relocation policy, hampered by blind spots in problem perception, information processing, and cultural sensitivity, failed to achieve its intended goals and exacerbated existing tensions within the EU.

References

Bach, T., & Wegrich, K. (2019a). Blind spots, biased attention, and the politics of non-coordination. In T. Bach & K. Wegrich (Eds.), *The Blind Spots of Public Bureaucracy and the Politics of Non-Coordination* (pp. 6–27). Springer.

Bach, T., & Wegrich, K. (Eds.) (2019b). *The Blind Spots of Public Bureaucracy and the Politics of Non-Coordination*. Springer.

Bendel, P. (2005). Immigration Policy in the European Union: Still bringing up the walls for fortress Europe? *Migration Letters*, *2*(1), 20–31. https://doi.org/10.59670/ml.v2i1.18

Börzel, T.A. (2016). From EU governance of crisis to crisis of EU governance: Regulatory Failure, redistributive conflict and Eurosceptic publics. *Journal of Common Market Studies*, *54*, 8–31, https://doi.org/10.1111/jcms.12431

Boswell, C. (2009). *The Political Uses of Expert Knowledge: Immigration Policy and Social Research*. Cambridge University Press.

Ceccorulli, M., Fassi, E., & Lucarelli, S. (2021). *The EU Migration System of Governance: Justice on the Move*. Palgrave Macmillan.

Consolidated Version of the Treaty on the Functioning of the European Union. *Official Journal of the European Union*, C 326/47. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12016ME/TXT

Council Directive 2001/55/EC of 20 July 2001 on minimum standards for giving temporary protection in the event of a mass influx of displaced persons and on measures promoting a balance of efforts between Member States in receiving such persons and bearing the consequences thereof. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32001L0055&qid=1648223587338

Cusumano, E., & Riddervold, M. (2023). Failing through: European migration governance across the central Mediterranean. *Journal of Ethnic and Migration Studies*, *49*(12), 3024–3042. https://doi.org/10.1080/1369183X.2023.2193713

Dublin III, Consolidated text: Regulation (EU) No 604/2013 of the European Parliament and of the Council of 26 June 2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person (recast). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02013R0604-20130629

European Commission. (2016). *Relocation & Resettlement: EU Members States urgently need to deliver*, https://ec.europa.eu/commission/presscorner/detail/en/IP_16_829

European Commission. (2024). *Evidence-Informed Policy Making*. https://knowledge4policy.ec.europa.eu/evidence-informed-policy-making_en

Geddes, A., & Scholten, P. (2016). *The Politics of Migration and Immigration in Europe*. Sage.

Grabbe, H. (2006). Free movement of persons in the single market. In *The EU's Transformative Power. Palgrave Studies in European Union Politics* (pp. 87–108). Palgrave Macmillan. https://doi.org/10.1057/9780230510302_6

Guiraudon, V. (2000). The politics of migration and immigration in Europe. *Journal of Common Market Studies*, *38*(2), 251–271.

Lovec, M. (2017). Politics of the Schengen/Dublin system: The case of the European migrant and refugee crisis. In C. Günay & N. Witjes (Eds.), *Border Politics* (pp. 127–146). Springer. https://doi.org/10.1007/978-3-319-46855-6_8.

Lodge, M. (2019). Accounting for blind spots. In T. Bach & K. Wegrich (Eds.), *The Blind Spots of Public Bureaucracy and the Politics of Non-Coordination* (pp. 31–46).

Majone, G. (1996). *Regulating Europe*. Routledge.

Merriam Webster Medical Dictionary. (n.d.). https://www.merriam-webster.com/dictionary/blind%20spots

European Court of Auditors. (2023). Migration and the EU policy. *European Court of Auditors Journal*, *2*. https://www.eca.europa.eu/ECAPublications/JOURNAL-2023-02/JOURNAL-2023-02_EN.pdf

Nugent, N. (2010). *The Government and Politics of the European Union*. Palgrave Macmillan.

Pronin, E., Lin, D.Y., & Ross, L. (2002). The bias blind spot: Perceptions of bias in self versus others. *Personality and Social Psychology Bulletin*, *28*(3), 369–381. https://doi.org/10.1177/0146167202286008.

Radaelli, C.M. (1999). The public policy of the European Union: Whither politics of expertise? *Journal of European Public Policy*, *6*(5), 757–774. https://doi.org/10.1080/135017699343360.

Regulation (EU) 2024/1351 of the European Parliament and of the Council of 14 May 2024 on asylum and migration management, amending Regulations (EU) 2021/1147 and (EU) 2021/1060 and repealing Regulation (EU) No 604/2013. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1351.

Regulation (EU) No 603/2013 of the European Parliament and of the Council of 26 June 2013 on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (recast). https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32013R0603.

Schmidt, V.A. (2019). The future of differentiated integration: a 'soft-core,' multi-clustered Europe of overlapping policy communities. *Comparative European Politics*, *17*, 294–315. https://doi.org/10.1057/s41295-019-00164-7

Schramer, O.C. (2008). *Uncovering the Blind Spot of Leadership*. https://www.scribd.com/document/11286391/Uncovering-the-Blind-Spot-of-Leadership

Trauner, F. (2016). Asylum policy: the EU's 'crises' and the looming policy regime failure. *Journal of European Integration*, *38*(3), 311–325. https://doi.org/10.1080/07036337.2016.1140756

Zaun, N. (2017). *EU Asylum Policies. The Power of Strong Regulating States*. Palgrave Macmillan.

PART V

War in Ukraine

ADRIAN SZUMOWSKI

MARIA CURIE-SKŁODOWSKA UNIVERSITY, LUBLIN

Critical Infrastructure Importance during the War in Ukraine 2022–2024

Abstract: The war in Ukraine is a testimony to the growing importance of destroying and protecting Critical Infrastructure hubs and nodes in particular regions of space. This is extremely visible due to the development and sophistication of those systems, which bear increasingly more functions in modern society. It is reflected mainly in the activities of government and national agencies. Early on, both parties discovered that dependency on Critical Infrastructure hubs and nodes would be crucial in forcing the second party into submission. During the war, there could be observed that both parties are trying to develop tactics whose main task is either cripple or retain that system. Their application could be observed with varied degrees of success, effectiveness, and cost. The summary of those efforts, analysis of the means, and information on their usage will become crucial elements of this chapter – furthermore, a lesson for other Nations that could be placed in similar circumstances. The knowledge of those operations is becoming a more important discipline of the art of war. A significant issue will also be whether critical infrastructure networks, especially on a global level, are dense enough to transmit ripples of its destruction powerful enough through transnational social space to trigger mutual defense mechanisms and be a cause of global war.

Keywords: Critical Infrastructure; security; war in Ukraine

Introduction

On February 24, 2022, in the early morning hours, Russian armed forces launched a full-scale invasion of Ukraine. The assault began not only by amour columns of mechanized infantry crossing the national border and the Line of Contact in Donbas but also with two other operations: airstrike and cyberattack. The first was an attack using specially designated tools, such as cruise missiles and strategic aviation, and reached targets located in the interior of Ukraine – mainly command centers, airports, and known military bases of Ukrainian forces (Watling, 2025, pp. 66–83),

but also civilian infrastructure, like railways, bridges, and roads. The second attack, however, started in the evening of the previous day, with designated operations in cyberspace, such as Distributed Denial of Service and distribution of malware within Ukrainian cyberspace (telecommunication networks, data processing centers, and Ukrainian section of the Internet), including sectors dedicated for military purposes (Cooper, 2024). The Ukrainian government has never officially admitted to the losses suffered as a result of these attacks. However, fragmentary reports and assessments by analysts and amateurs indicate they were terrifyingly effective. For example, it is estimated that the command and control networks of the Ukrainian Armed Forces did not regain full functionality until around February 28 (Cooper, 2024), which means that for a week or more, the Ukrainian General Staff could not implement its prepared war plans. It is not a secret that during this period of war, the Ukrainian armed forces suffered the most significant losses in both material and human assets (Cooper, 2024).

As the war progressed, and it became impossible for one of the war parties to win on the battlefield, such attacks – airstrikes and cyberattacks – became more frequent. The Ukrainian Armed Forces used mainly special operations teams, especially in the first phase of the war, and unmanned vehicles, mostly aerial but also sea, while the Russian Armed Forces relied primarily on long-range missile systems, including, somewhat surprising, air defense systems, such as the S-300, which for unclear reasons, can be set to ballistic mode (Fiszer & Fiszer, 2023); unmanned aerial vehicles, predominantly supplied by the Islamic Republic of Iran and manufactured in Russia on Iranian license, air powers means such as strategic aviation as well as regular units already operating in occupied Ukraine (Wilk et al., 2023).

It is also becoming increasingly clear that Critical Infrastructure, located predominantly in Ukraine but also on Russian soil, has become the primary and fundamental war objective. Depending on the party, the drive to secure or paralyze it is becoming a substitute for stagnated battlefield operations. This became particularly evident when, during the winter of 2022/2023, Russian leadership decided to shift toward deliberate attacks on undefended mid-level nodes of the Ukrainian power grid and heating grid in order to break the will of Ukrainian society to support the war effort. It could be referred to as a "war of currents" (Matuszak, 2023), and Ukraine won the first round, but some of the damage has not been repaired.

The main goal of this chapter will be to analyze the role and importance of Critical Infrastructure in the framework of contemporary armed conflict. Answers to three primary research questions will be sought. The first and most important question will be: What is Critical Infrastructure today? Which systems are its integral part, and which should be left outside its scope? The second question will be about the consequences of attacking and destroying contemporary Critical Infrastructure. This is a fundamental question for two intertwined reasons. First, localizing the

effects of destroying Critical Infrastructure nodes and hubs in a globalized world is complicated. Second, those consequences could trigger a cascading effect that could have devastating consequences across the global network of Critical Infrastructure extending from the country where the initial disruption occurs. In this context, the connections between Ukraine and the North Atlantic Treaty countries come to the fore. The third question will refer to the proper protection of Critical Infrastructure facilities.

The research will focus on analysis aimed at verifying three hypotheses. The first and most important is that as modern warfare has developed, especially as part of the trend of focusing on civilians, attacking and destroying Critical Infrastructure objects has become an essential element of the strategy of conducting military operations. The second hypothesis is that despite the cascading spill-over effect of the destruction of Critical Infrastructure, it has not reached the level at which it could be considered a cause of war for third countries. The third hypothesis indicates that proper protection of Critical Infrastructure systems requires systematic, massive, and multi-year expenditures and investments. Otherwise, it will be necessary to engage other entities of the international system in their defense and reconstruction to maintain the system's minimum efficiency.

The chapter will be divided into three main parts. The first will be dedicated to the issue of defining Critical Infrastructure, as well as the scope of modern infrastructure systems included in this category. The second section will focus on analyzing the catalog of actions against Critical Infrastructure used by both parties, along with an attempt to estimate their effectiveness and impact on a global scale. Four categories of attacks on Critical Infrastructure will be analyzed: cyberattacks, sabotage, airpower, and kinetic attacks using Armed Forces components (mainly engineering corps). The third part will be devoted to strategies for ensuring the security of critical infrastructure installations in the contemporary world, emphasizing the effectiveness of their application in Ukraine. These are international law regulations, camouflage, active defense (using classic means, such as air defense and maintaining cybersecurity), and redundancy. The summary will forecast these means' further development and impact on global civilization's future shape and functioning.

The scope of Critical Infrastructure

"Critical Infrastructure" is a term that is gradually gaining importance in the academic discourse on international relations. However, its scope is unclear and still widely debated. The general definition of Critical Infrastructure is best expressed by Alex Tarter, who indicates that it "describes infrastructure considered essential

by governments for the functioning of a society and economy and deserving of special protection for national security" (Tarter, 2015, pp. 74–75). This means that three primary conditions must be met to determine whether a given installation falls within the scope of Critical Infrastructure. The first is the importance of these systems for the effective functioning of society and the economy. However, what this importance should consist of needs to be specified. The second condition is securitization (Misiągiewicz, 2015, pp. 393–411), i.e. a speech act recognizing individual elements of Infrastructure as critical. This dimension is performed through documents adopted at various levels of government administration, usually in the form of a national security strategy. The third element is the dedication of special measures intended to secure these systems as part of activities aimed at ensuring national security. In conclusion, Critical Infrastructure is those systems that are essential for the functioning of the economy and society and are guarded by specially dedicated military and paramilitary systems as part of national security.

The fundamental caveat for this definition is that the concept's scope is constantly fluid. Because the question of which of the systems can or cannot be considered critical depends on the historical framework and social contexts. For example, in Ukraine, during the winter seasons, the unique targets for the Russian air campaign were power transformers (Grzeszak, 2023) and heating installations (*Rosja atakuje…*, 2024). Usually, these objects are not considered critical, but the purpose and consequences of their destruction necessitated their securitization and coverage by anti-aircraft protection. In other countries, however, the status of these objects is not critical.

Depending on the national and international solutions, the concept's scope varies depending on the actor responsible for composing it. Definitions of Critical Infrastructure extend to almost all socioeconomic activities. One of the best examples of this type may be the United States' definition of Critical Infrastructure, which was included in the Presidential Directive PPD-21 of February 12, 2013 (The White House…, 2013). In this approach, Critical Infrastructure is identified as "the source of services that support American society". The United States Critical Infrastructure also includes: "distributed networks, diverse organizational structures and operating models (including multinational ownership), interdependent functions and systems, both in physical space and cyberspace, and management constructs, taking into account mechanisms of multi-level authority, responsibility, and regulation". In the light of this definition, virtually every system and institution participating in human and social activity can be assigned to the category of Critical Infrastructure. However, unlike other systems, Critical Infrastructure must be characterized by "security and the potential to enable its efficient reconstruction in the face of all threats".

Moreover, the United States definition also raises the issue of operators of Critical Infrastructure systems and their responsibilities to various levels of government

institutions. The entire United States Critical Infrastructure system has been divided into sixteen sectors, which include the following elements: chemical industry, commercial Infrastructure, communications, critical industrial plants, dams, the military-industrial complex, emergency services, energy, financial sector, food industry along with agriculture, government installations, medical services, technology centers, nuclear power, transportation system, and water and sewage systems. The purpose of preparing the above document is to include the protection and regeneration of Critical Infrastructure in the institutional structure of the American government created under the aegis of the United States Department of Homeland Security (DHS).[1]

In this context, it should be noted that the extensive securitization procedure is the result of the terrorist attacks of September 11, 2001. It is also the subject of numerous controversies regarding the possibility of interference by national agencies conducted in the name of national security at the expense of realizing civil liberties and the general effectiveness of the entire system (Kettl, 2014). Another example of those challenges may be growing interest in the issue of critical Infrastructure and its importance for the security of the European Union, individual member states, and individual citizens. The basis for the undertaken activities is the European Program for Critical Infrastructure Protection, the introduction of which is the communication of the European Commission of December 12, 2006 (Commission of the European Communities…, 2006). This is, to a large extent, the basis for the program to undertake further, more detailed activities within the planned scope. In this context, Critical Infrastructure is infrastructures of the most significant importance for the community, the disruption or destruction of which would adversely impact at least two Member States or one Member State where the Critical Infrastructure is located in another Member State. This includes, among other things, cross-border effects resulting from the interdependence between interconnected, different infrastructure sectors (Commission of the European Communities…, 2006, p. 4). As a result, the above definition is somehow the opposite of the one provided by the United States. Instead of focusing on an exhaustive list of individual systems, there is a need to point out certain common elements to determine which parameters must be met for a system to be labeled as Critical Infrastructure. One of the crucial elements is the presence of a specific system in at least two Member States, which means that its disruption will create costs that are felt at the level of individual citizens. In this dimension, costs may reduce the overall efficiency of the entity's activities and the costs of reconstructing damaged systems and restoring destroyed capabilities. An additional element that complicates definitional issues is the inclusion of the national level of Critical Infrastructure, which is left to the decision-making power of national governments, which means practical diversification of this definition.

[1] More details about this agency can be found at https://www.dhs.gov/

Despite the use of a different logic in formulating both definitions, the effect of the European approach is comparable to that of the United States in creating an equally broad and unspecified catalog of systems included in the global Critical Infrastructure. Thus, a limited quantity of assets dedicated to its protection needs to be spread between numerous and dispersed systems defined as needed protection. It covers an extensive and sophisticated complex of interconnected structures of physical and transnational connections, perceived through different lenses at both European and national levels. Consequently, the simplest way to present it is to list the individual elements enumeratively in more detailed framework documents developed under this program (Lewis et al., 2013, pp. 51–60).

The last international definition, or rather the approach to defining Critical Infrastructure, is represented by international institutions. The North Atlantic Treaty Organization produced the *Multiple Futures Project Report. Navigating towards 2030. Final Report* (2009). In this approach, one can observe an attempt to define the elements of Critical Infrastructure, not by trying to identify and describe individual elements, as was the case in the United States definition, nor by trying to analyze their importance for civilizations and societies, but by determining the consequences of their destruction for member states and other entities located within the limits of Treaty Area and taking advantage of their capabilities. Thus, three features of the above action can be pointed out (*Multiple Futures Project Report. Navigating towards 2030. Final Report*, 2009, pp. 25–27).

Firstly, Critical Infrastructure hubs and nodes are primarily located within large urban agglomerations. This could be translated into an enormous capability to regenerate or replace damaged elements of Critical Infrastructure within a relatively short period. Therefore, their severe damage or destruction requires a natural or artificial disaster comparable to the use of weapons of mass destruction, with particular emphasis on nuclear weapons. Other weapon systems do not guarantee a sufficient level of system destruction to cause the dysfunctionality of a whole system. Additionally, it should not be forgotten that the use of a taboo weapon in a densely populated area results in a massive penalty for the aggressor, which will have an impact on its international legitimacy and, consequently, the possibility of taking advantage of this success in the perspective of implementing further elements of the international strategy.

Secondly, the immediate effects of destroying a Critical Infrastructure hub or node have devastating consequences in the short term. These are primarily economic and financial costs resulting from interrupting the system of transnational financial transactions, which supplements the proper functions of the circulation network of goods, services, people, and information. As a result, the trade routes and supply chains of these resources will be broken and forced to take alternative shapes, avoiding affected areas by the creation of *ad hoc* connections located in other

parts of the geopolitical space, which in European conditions most often means the jurisdiction of a separate Nation-State, and, consequently, the loss of revenues resulting from servicing this traffic. Additionally, the costs associated with the death of a significant part of the population, the induction of severe radiological diseases, the physical loss of industrial plants and other installations, and the costs associated with decontamination of the affected areas should not be underestimated, which means a considerable burden on the potential of the attacked Nation State. Its ability to operate in the international arena will not only be limited but downright impossible. In other words, the issue of restoring Critical Infrastructure hubs and nodes requires significant funds that block the possibility of taking up international activity.

Thirdly, there are also long-term effects, the most serious of which is the change in the regional balance of power. This is a consequence of the dispersion of resources for the purposes presented in the previous point, which will result in a long-term reduction in the potential of an attacked entity and its decline in the equation of balance of power until all physical effects of the use of weapons of mass destruction are removed and the paths of circulation of goods, services, people and information are modified again.

Wrapping it up, the NATO definition perceives Critical Infrastructure through the prism of losses that may result from an effective attack on its elements. In this dimension, this definition does not focus on listing individual systems included in the category of critical Infrastructure nor on attempting to analyze the parameters of individual systems. It was left for an intuitive understanding of the individual recipients of those reports. The only indicator allowing for a closer characterization of these systems is their connection with large urban agglomerations (*Multiple Futures Project Report. Navigating towards 2030. Final Report*, 2009, pp. 25–26). In this context, there was made a detailed analysis of the effects of attacks on these systems, particular strategies for preventing their damage, and their quick regeneration. They were based on existing collaborative efforts of numerous actors, supported by the framework of international institutions, such as NATO (*Multiple Futures Project Report. Navigating towards 2030. Finding and Recommendations*, 2009).

To summarize this definitional thread, it should be stated that three serious challenges should be included in a comprehensive definition of Critical Infrastructure. First, it is necessary to narrow down the number of systems included in it in order to avoid information overload, which would mean that practically every smallest industrial plant, such as a tailor's workshop, would be included in the Critical Infrastructure framework. Second, it is necessary to indicate relatively objective and generally recognized criteria against which these divisions will be applied. Third, it is also necessary to develop internal relations between the individual elements in this definition.

In this dimension, for a complete analysis of the importance of the Critical Infrastructure, it will be assumed that this category comprises systems for transmitting

material and intangible resources integrated at a global level. In this context, the whole system consists of three components. The first is large and smaller urban centers where systems compress material and intangible resources to transfer them between similar demographic centers. The second are systems enabling the effective functioning of large urban centers, from public services to municipal companies. The third component is global transport routes for the transmission of raw materials (pipelines) (Wyciszkiewicz, 2008), information (the Internet), and material resources and people (sea and air routes, highway systems, and the Infrastructure that speeds up their functioning, such as tunnels, canals, and similar investments). Despite their diversity, they have one fundamental common feature: their destruction or shutdown causes enormous losses for the affected country, and restoring their previous efficiency entails the dispersion of a significant part of the potential.

Additionally, in the context of producing and transporting valuable resources, it is possible to search for and find alternative suppliers with little or no problems for consumers, even though this is both time and money-consuming. Alternative suppliers do exist and are interested in acquiring additional contractors and clients. As a result, the practical effect of damaging Critical Infrastructure is to deprive a given sector of the population of a specific service for a relatively short time. In consequence, Critical Infrastructure can be divided into five basic structures intertwined on a global scale. It is a transport structure, including transshipment facilities, transport platforms, sea routes, a network of roads, railways, and air corridors. Infrastructure facilitates geographical space crossings, from bridges and canals to satellite navigation systems. Secondly, it is a telecommunications structure that allows information to be transmitted globally at speeds close to the speed of light. Thirdly, the structure of gas and oil pipelines enables the transmission of liquid and semi-liquid raw materials over long distances. Fourthly, the structure of public services ensures a minimum level of security for large urban centers. Fifthly, it is also a structure that ensures the supply of commodities to large agglomerations, from drinking water to electricity.

To organize subsequent considerations, Critical Infrastructure systems will be understood as those systems that are key to implementing three functions. The first and most important is ensuring access to the territory of a given Nation-State and access from the territory of a given Nation-State to the outside, international environment. In this context, Critical Infrastructure includes seaports, railway lines with stations and accompanying technical infrastructure, highways and roads with tunnels and bridges, and airports. The second function is to ensure the effective functioning of the economy and society by ensuring access to essential commodities, such as water, energy, and services, necessary to meet the basic needs of people living in modern society. This Infrastructure enables local societies to function efficiently in the contemporary global community. The third function is information processing and transmitting. In this respect, this scope includes not only computer

systems and access infrastructure to the global communication network but also mass media, the purpose of which is to construct and maintain society's identity and propagate the picked narrative. The symbolic attacks on TV towers in Kharkiv (Melkozerova, 2024) and Kyiv (Wilton, 2022) are special symbols for this dimension of Critical Infrastructure.

Attacks on Critical Infrastructure

Shifting considerations toward the issue of disrupting Critical Infrastructure systems, it should be mentioned that this is a growing problem for strategists and practitioners of strategic studies. Questions of how Critical Infrastructure can be effectively destroyed or protected started extending beyond science fiction. Especially since the recent conflict in Ukraine proved that modern warfare, despite numerous attempts to give it humanitarian constraints, increasingly revolves around this issue. Critical Infrastructure is a physical network of connections between smaller (nodes) and more significant (hubs) centers. The purpose of this structure is to effectively transfer people, goods, energy, and information in the real world without the need to use simple mechanical devices by replacing them with installations located in nodes and hubs of the Critical Infrastructure network. For example, modern civil aviation radar systems are not located only at airports but operate on the principle of exchanging information with transponders on board aircraft (Placha, 2014). These functions can be multiplied. However, this also entails dependence: without installations ensuring the implementation of individual functions, the rest of the system remains ineffective. For this reason, mechanisms called redundancy are built into the whole. This phenomenon means that the system is created with capacity that usually exceeds demand so that if the system fails, is destroyed, or becomes under increased load, a cascading collapse does not happen.

Generally, three basic strategies are used to paralyze Critical Infrastructure systems. The first is the gradual elimination of individual parts of the system so that the whole system becomes ineffective. It includes a series of attacks on the Ukrainian IT network to prevent the Ukrainian side from taking any actions in the media sphere. The second strategy is to attack the so-called "bottlenecks" of the network, i.e. nodes and hubs that, intentionally or not, are responsible for managing most of the traffic within the said network. In this context, attacks on the shipment infrastructure located in Ukraine's Black Sea ports are apparent to prevent the export of Ukrainian crops to the global trade network. The third strategy is to attack the Critical Infrastructure systems on which the remaining sections depend. The more dependencies there are, the more valuable the system is and the more vulnerable it is to attacks. This strategy was implemented during the Ukrainian "war of currents",

where the attack was directed at mid-level nodes of the power grid: transformers. Their massive destruction in the air attack campaign caused such significant damage to the system that it negatively affects all Critical Infrastructure systems today.

Due to the means applied, four tactics of attacking Critical Infrastructure systems were used during military campaigns in Ukraine. These are cyberattacks, sabotage, airpower, and kinetic attacks using classic armed forces (mainly engineering units). Interestingly, all these tools are used by both parties of the conflict. However, in quantitative terms, their application is asymmetric. For example, the Ukrainian side specializes in sabotage and attacks using drones, while the Russian side mainly uses airpower and traditional armed forces, including military engineers. Both sides use cyberattacks with varying degrees of success. Each of these tactics has its advantages and disadvantages, as well as different levels of effectiveness or the ability to recover the attacked system, and is susceptible to different countermeasures.

Cyberattacks

This is one of the most critical issues of contemporary national security. It is generally understood as an action to neutralize computer, IT, and telecommunications networks. Contrary to popular belief, however, applying the Microsoft definition, cyberattack "attempts to gain unauthorized access to computer systems to steal, modify or destroy data" (*Co to jest…*, 2024). Therefore, the primary target of a cyberattack is not critical infrastructure sectors but primarily their content: information. From this perspective, it is the most ephemeral tactic: it is difficult to determine whether IT network disruptions are malevolent or result from less sinister causes. This happens mainly for two reasons. Firstly, the operating environment is exceptionally modal and relatively easy to recreate, change, or transform. Thus, attacked elements are restored to full functionality relatively quickly. For example, on November 1, 2022, Russian military intelligence appeared to have access to the Ukrainian military management information system "Delta". According to Ukrainian government officials, access was limited to just a few minutes, after which security measures were activated, and the stolen passwords were blocked (*Rosyjskie media…*, 2022). Computer systems are subject to constant change and modification: any gain can be lost and any loss recreated, depending on the efficiency of the IT sector in the attacked nation-state.

The second feature of cyberattacks is that the attacked entities are very reluctant to provide information about such events, preferring to indicate other, less compromising, reasons for their vulnerability and disruption in performance. Therefore, the most common response to information from the opposing party is to deny or reduce the scale of the threat, which was the case in the example mentioned above. As a result, even the most severe attacks of this type can be relatively easily hidden in the thicket of other, more spectacular information.

Those tactics are the most accessible because access to these particular sections of Critical Infrastructure is an integral part of their strategy. Paradoxically, despite the high degree of technological dependence, their weakest link is still someone who, for example, uses the same password to access databases with varying degrees of security. For this reason, access to these systems can be obtained at a relatively low cost. However, the losses that the attacked side suffers are usually short-lived.[2] The cyber environment is intangible and can, therefore, be recreated almost unchanged. However, during these attacks, one of the most valuable and irreplaceable resources is wasted, namely time. For this reason, it is usually used with other kinetic power application tools, which was the case in the first week of the war.

This tactic has the most significant potential to delocalize the consequences of an attack and move it to a global level, especially when using increasingly autonomous malware programs. The global failure of systems based on the Windows platform may demonstrate the scale and possibilities of such events. The malfunction concerned an update of CrowdStrike's Falcon program and the Azure platform, which affected over 8,500,000 devices based on these systems (less than 1% of the total) but caused global disruptions to Critical Infrastructure in the transport sectors, including aviation and a range of services, with particular emphasis on banking (*Microsoft twierdzi…*, 2024). Assuming this failure was accidental and not intentional, the question should be asked about the possibility of initiating collective defense systems, for example, Article 5 of the North Atlantic Treaty Organization. Emphasizing, the open question is if the cyberattack could be considered a triggering factor for mutual defense clauses, which could be found in said Article; therefore, if a cyberattack will cause turmoil on a global level, which, in turn, will be localized to be considered a threat to undertake even military countermeasures.

Nowadays, two years into the war, such probability is not considered a reliable factor in collective security and mutual defense mechanisms. Of the documents discussed, only the Multiple Futures Project discusses scenarios of significant damage to NATO Member States Critical Infrastructure, but only caused by weapons of mass destruction. That means that governments did not recognize disruptions of Critical Infrastructure caused by cyberattacks as comparable to those caused by weapons of mass destruction. At least not yet. It seems, however, that in the absence of potential response scenarios to the above challenges, the Alliance will be faced with the prospect of making a political decision reflecting the political context. In the context of the tendency to de-escalate the conflict with Russia, a decision

[2] One thing needs to be mentioned: there has been no recorded case so far where a cyberattack led to the physical destruction of a Critical Infrastructure installation, except for one still being discussed. This is the case of the destruction of centrifuges at the Natanz research and production center, which, depending on the delivery method of the virus, may be described as a cyberattack or sabotage.

will be made not to raise these issues. The exception is the genuinely significant destruction of Western Critical Infrastructure, which is unlikely to happen using known cyberattack tools.

Sabotage

This action against Critical Infrastructure networks is common during the analyzed armed conflict. It is predominantly the domain of operations of Ukrainian Special Operations Command agents. There is very little data on the nature of these operations. There was unconfirmed information that special forces units began to penetrate the border even before the conflict entered the active phase. There is also the issue of ATESH organization activities, which are operating in the occupied territories, including Crimea, probably formed in September 2022 (Official statement…, 2022). Sabotage is "a devastating rear warfare action, an element of the combat arsenal intended to distract the enemy's attention. Acting covertly to weaken the defense or economy of an enemy in time of war or an enemy state in time of peace. Disorganization of enemy forces, destroying or damaging enemy military resources" (*Regulamin działań…*, 1999, p. 262). The Russian Federation carried out activities of this type almost exclusively in the first phase of the armed conflict, infiltrating the defenses of Kyiv and Kharkiv. This activity was significantly limited after the retreat towards Belarus and the displacement of Russian forces from the eastern Kharkiv region.

Ukrainian units, on the other hand, operate almost throughout Russia, functioning not only as saboteurs but also as weapons of psychological warfare. In Russia, since the beginning of the war, there has been a series of mysterious fires covering Moscow (Bounaoui, 2024), St. Petersburg (*Wielki pożar…*, 2024), and Omsk (Tymchenko, 2024). The use of these agents and means has threefold effects. Firstly, it is the destruction of Critical Infrastructure installations, particularly scientific and research objects (Bojanowska, 2024). Exceptionally, the Crimean Bridge was considered a target and was hit relatively successfully at least once (*Czym wysadzono…*, 2022). From this perspective, these actions have slight effectiveness, mainly due to the limited means of destruction. The specificity of sabotage activities means the need for significant mobility with a small number of subunits, almost constantly exposed to the risk of clashes with security forces, which means their elimination (Matecki, 2024). This translates into low destructiveness of the tools, which are relatively ineffective against extensive and durable installations. Even a spectacular attack by a truck filled with explosives was unable to damage the structure of the Crimean Bridge and put it out of use for a long time (*Naprawa Mostu…*, 2022). The diversion was most effective against single, relatively vulnerable, undefended installations.

The second function of sabotage is an essential tool of psychological warfare. The fear of witnessing or falling victim to sabotage creates pressure among the

civilian population and, thus, exerts political pressure on the government, even one of authoritarian origin. After the first few mysterious fires, any similar event, such as an accidental forest fire, may seem to the public as another attack by the all-powerful Ukrainian commandos. However, it is imperative to remember that this effect is relatively short-lived, as the narratives describing warfare and the successes and failures of one's troops change. This function has little impact on Critical Infrastructure, except dispersing resources to create and propagate counter-narratives into transnational social space.

The third function became important, especially in implementing the first deliveries of missile systems with an effective operational range of up to 300 kilometers (Palowski, 2024) and lifting restrictions on attacks on Russian territory, excluding the Crimean Peninsula. Western Powers consented to limited strikes in the Russian Federation, mainly the Rostov and Belgorod Oblasts (*Ukraina potwierdza…*, 2024), especially in light of the recent offensive on Kharkiv. In this context, covert operations units are intended to observe and transmit information necessary for precise strikes on designated targets, including Critical Infrastructure and military facilities such as ammunition and fuel depots, refineries, command centers, and air defense installations. In this context, this is the most effective use of this tactic. Combined with other means, it is highly effective; however, it is short-range and limited only to the immediate vicinity of one's territory.

To sum up, this tactic has mainly psychological significance. It cannot paralyze or weaken Critical Infrastructure systems without combining it with other tactics, usually airpower. This tactic is only effective against selective, vulnerable, and poorly defended targets. As a clearly localized tactic, it has the least potential for escalation.

A specific form of sabotage, the perpetrator of which has still been unspecified, was the destruction of three of the four pipes of Nord Stream I and II. The attack was carried out on September 26, 2022 (Kardaś & Łoskot-Strachota, 2022). There are three suspects identified by various parties, namely Russia, Ukraine in cooperation with Poland, and the United States. This sabotage is one of the most extensive and unique operations against Critical Infrastructure installations globally. It required highly advanced tools and knowledge to shut down the pipeline effectively. The identification of and access to the attacked infrastructure elements in the hostile environment is particularly impressive. Destroying these elements required resources available only to a few nation-states and their agencies. Carrying out an operation without leaving anything more than circumstantial evidence is extremely rare. It seems that this operation indicates the direction from which the greatest threat to the Critical Infrastructure network will come, rendering it inoperable for a specified period of time and permanently eliminating its entire sectors. However, it requires enormous capabilities and knowledge that are available only to a few nations particularly interested in this investment.

Airpower

This tactic is used by both sides effectively; however, due to the expanses that those tools demand, it is used predominantly by the Russian Federation in this conflict. The designated tools of deliberate destruction of Critical Infrastructure systems, i.e. strategic air bombers, intermediate ballistic missiles, including the famous Iskander missiles (9K720, NATO code: SS-26 Stone) (Ciastoń, 2022), cruise missiles, including the famous Kindzhal system missiles (Kh-47M2, NATO code: AS-24 Killjoy) (Pomper & Tuganov, 2023, pp. 69–93) and, increasingly, unmanned air vessels designed by Iran. From this perspective, an increasingly growing share of this type of means can be observed in warfare. This partly corresponded to a change in the priorities of the operation, from usurpation of indirect control over the Ukrainian government by replacing key personnel towards deepening the chronic economic crisis by depriving the Ukrainian society of access to the global network of Critical Infrastructure and limiting the functionality of the network in meeting social needs to the point of an outbreak of social dissatisfaction. These actions did not bring the expected results in the short term. However, with hindsight, it turns out that this goal is slowly being achieved, for example, by limiting access to electricity, which causes a sense of chronic wearinessin a society accustomed to a certain standard of living.

Activities of this type have three most important advantages and two disadvantages. The first advantage is the possibility of a relatively cost-free attack (or with relatively small losses in own personnel – *What Is…*, 2024),[3] especially regarding the potential operational range covering the entire territory of the attacked country. The so-called deep rear areas, i.e. relatively safe areas, are located outside the area of direct presence of the aggressor's armed forces, including artillery and frontline aviation. This has enormous psychological and social consequences and requires the dispersion of defensive assets from key locations or from frontlines. The second advantage is that using three factors limits the defense against these measures. Firstly, limiting the time for counteraction, i.e. effective defense or evacuation. For example, in the case of Russia's first use of 3M22 Zirkon hypersonic missiles (NATO code: SS-N-33) (*Ukraine Says…*, 2024), the activation of air defense in Kyiv was only possible due to warnings from other cities that had been attacked earlier. And those missiles pass through the air defense perimeter without hindrance. Secondly, the tactics of airpower require constant modification of anti-aircraft defense. It is enough for only a few missiles to slip through to destroy completely, for example, the Tripol thermal power plant or the Yemiyovsky thermal power plant (Dura, 2024), despite launching numerous volleys at both targets. Thirdly, despite their cost, these weapons are still relatively cheap compared to others currently available in the arsenal.

[3] This does not mean the complete lack of losses in equipment and people, evident in the form of the shooting down of a Tu-22M3 aircraft while operating near Ukrainian airspace.

Additionally, their use will strain the attacker's resources due to the need to observe and destroy all deployed missiles, which also means using more expensive Western counter missiles and increasing one's vulnerability to SEAD (Suppression of Enemy Air Defense) operations and mechanical fatigue of weapons systems. The third advantage is that the ability to use this tactic means the ability to perform relatively precise airstrikes on designated targets. It enables limiting casualties, assuming this was the attacker's intention. For example, the military means used in the raid on Kyiv, where, among others, two hospitals were attacked, seem to have been a deliberate action because the means of attack used were extremely precise by Russian standards.

This tactic also has some disadvantages. Firstly, the construction of devices of this type is a long and complicated process, and additionally, it requires the provision of components that only a few national economies are able to produce. This mainly concerns microchips and precision optical mechanisms. Campaigns of this type will consume ballistic missiles, cruise missiles, hypersonic missiles, and drones faster than the Russian economy can supply. This tactic is unsustainable in the long term. Secondly, as can be indicated by the example of the attack on Kyiv hospitals, it should be particularly emphasized that such attacks, either intentional or unintentional, may result in legal and moral consequences, which, in favorable political conditions, may turn into more severe sanctions of a political, economic and military nature.

Ukraine takes a different attitude to this tactic. It can be observed that the central command is mainly focused on various unmanned vehicles, both air and sea, which are used in attacks on strategic objectives. In most cases, the targets are installations intended for military and paramilitary purposes, except for oil refineries. However, due to the lack of specialized resources, the solutions used are instead emergency solutions, created on the basis of national technical thought or derived from civilian projects. Nevertheless, this tactic brought a few spectacular results, such as the attack on the transport air base in Pskov (Szopa, 2023a), symbolic because it was from this base that Russian paratroopers took off in order to capture Kyiv in the first days of the war; attack on the air force bases in Morozovsk and Engels (Szopa, 2024), which serves as a point for refueling, rearming and repairing of for strategic bombers participating in operations aimed at Ukrainian Critical Infrastructure; or the attack on the air force bases Jejsk and Rostov-on-Don (Szopa, 2023b), which performs similar functions to Russian tactical aviation, and recently also against refineries in the Russian Federation, which unofficially sparked protests from the United States (*„FT": USA nalegają…*, 2024). It should be noted that these attacks have a much more significant psychological effect due to more limited assets on the Ukrainian side. However, because Ukraine is dependent on external aid, it often has to face externally imposed restrictions, for example, the ban on attacking targets on Russian territory, excluding Crimea (Niedziński, 2024), which has only recently been lifted.

Kinetic attacks using classic armed forces (mainly engineer units)

The last tactic used to paralyze Critical Infrastructure segments is classic armed forces units, with particular emphasis on engineering and sappers units. This is due to the simple fact that this can only occur in the area controlled by these armed forces, which may limit the offensive and defensive of other units and contribute to significant material and human losses. Typically, this tactic is used as a sign of desperation, with the losing side destroying Critical Infrastructure, especially bridges, roads, and dams, to buy time for remaining troops to retreat in an orderly manner or organize a coherent defensive perimeter. This was used both by the Ukrainian military during the fighting north of Kyiv and the offensive from Crimea towards Odesa and Melitopol, as well as by the Russian military during the Ukrainian offensive in the Mokry Yar river valley and during the recapture of the eastern Kharkiv region.

In this context, two objects are at the forefront of using this tactic: the dam on the Dnipro in Nova Kakhovka and the Zaporizhia Nuclear Power Plant. The first object had already been destroyed, most likely by Russian sappers who wanted to stop the offensive of Ukrainian troops and the crossing of the Dnipro River. However, due to the lack of appropriate skills, they led to a catastrophe on a global scale and the collapse of the defensive line of Russian troops on the eastern river bank. Paradoxically, this also resulted in the drying up of the Kakhovka Reservoir, below the mouth of the canal, which supplies fresh water to Crimea. In the case of the second object, the largest nuclear power plant in Ukraine and Europe, with six VVER-1000/320 reactors (pressurized water reactor) with a capacity of 950 MWe each, situations are much more sophisticated and dangerous. Since March 4, 2022, the power plant has been entirely under the control of Russian forces. Paradoxically, the power plant also drew water from the Kakhovka reservoir, which means that the launch of this object may result in a disaster incomparably greater than the Chornobyl disaster. Currently, the reactors are disconnected from the network and supervised by the International Atomic Energy Agency. However, from time to time, there are discussions about how Russia could use the fact that it owns the facility and transfer it to the international administration or the Ukrainian government. Also, suppose the Russian armed forces decide to use a scorched-earth policy and cause a mass failure of all reactors. In that case, it will be necessary to rethink the Ukrainian operation and consider retaking it. However, Russian strategists are refraining from admitting these considerations until this particular stalemate persists. More importantly, those objects are so significant that they are already subject to international protection under the United Nations Charter and the law of war. However, this is not a significant factor for the Russian command, which often bypasses these regulations for strategic benefits.

Protection of Critical Infrastructure objects

These considerations should be summarized to defend and protect critical infrastructure systems. These are international legal regulations, camouflage, active defense (using classic means, such as anti-aircraft defense and cybersecurity), and redundancy of Critical Infrastructure systems. All of them were used in the Ukraine conflict, but each presented both advantages and disadvantages. The only practical solution seems to be simultaneously using at least two of the proposed tactics. However, the problem seems to be that in any case, this tactic becomes extremely expensive.

International legal regulations

The first tactic is to establish and strictly enforce the relevant international legal provisions, among which the most important are the following documents: Convention on the Laws and Customs of War on Land (Hague Convention IV) of 1907 (Konwencja…, 1927), Charter of the United Nations (Karta…, 1949) and the Additional Protocol (I) to the Geneva Conventions of August 12, 1949 from 1977 (Protokół…, 1992). They constitute the fundamental principles limiting and regulating actions toward Critical Infrastructure systems during armed conflict. However, it should not be forgotten that this solution is not perfect. In this respect, two primary challenges related to creating international legal norms should be pointed out. The first is that the development of law has not kept pace with the international situation and circumstances.

On the one hand, the development of Critical Infrastructure objects is still ahead of the legal context; for example, the development of cyberspace and its consequences are only being recognized and introduced into the international legal order (Konwencja Rady Europy…, 2001). On the other hand, especially in cases of armed conflict, the goals of military action tend to obscure the intentions of the legislator, as was the case with the blowing up of the Kakhovka dam. In this context, the law becomes as effective as the Nation-States are willing to enforce it.

Camouflage

Another example of a Critical Infrastructure systems protection tactic is camouflage. It was evident in the case of Nord Stream and other underwater installations, such as pipelines, telegraph cables, and optical fibers, which, after some time, become overgrown with silt and underwater vegetation, making it challenging to identify and reach these systems to destroy them. As it turned out in the case of Nord Stream and some sub-ocean cables (Sharpe, 2024), it turns out that this protection is not entirely adequate. In the case of above-sea-level installations, it is even more difficult. While camouflage can be used in the case of underground installations, such as the Ukrainian

liquefied natural gas storage facilities (Junko, 2024), much of it cannot even be mentioned, either because of the size or because of the need to disclose their location due to function they fulfill in the global system. In this approach, camouflage may be partially effective, but their location and size can be corrected mainly by local collaborators or social media (*Docent uniwersytetu…*, 2023).

Active defense

This is one of the most promising tactics for protecting Critical Infrastructure hubs and nodes. It is also one of the most effective but also very expensive. It means active defense in all scopes of all major structures of Critical Infrastructure against known threats: cyberattacks, sabotage, airpower, and classic conquest. There are two main disadvantages of this solution.

First, it is a costly solution, mainly due to the cost of creating and maintaining multi-level defense coverage in all scopes of the indicated installations and systems. For this reason, only a few Nation-States can generate the so-called anti-access/area denial (A2AD) bubble over all crucial installations. For example, such a bubble in Ukraine was spread only over the Kyiv agglomeration. Work is underway, motivated mainly by the importance of the Black Sea trade routes, to construct a similar bubble over Odesa. But, for example, Kharkiv, the second largest city in Ukraine, is deprived of it, mainly for three reasons. Firstly, the proximity of the border limits the effectiveness of warning systems. Ballistic missile launchers were pulled up to the border to reduce the arrival time to the necessary minimum. Secondly, due to losses suffered in the first days of the war, most of the installations that formed the basis of the active defense system were largely destroyed. As a result, the defense of this city has to be created literally from scratch, which is not easy, especially given the constant countermeasures of Russian forces. Thirdly, the possibilities of producing defensive systems, especially air defense systems, are limited. The technical possibilities of saturating the entire territory of Ukraine with these systems in a short time are limited. As a result, active protection can only be constructed in precisely defined places. For example, the government of Ukraine is still struggling with the dilemma of defending what is most desirable: cities or troops.

Secondly, the effectiveness of this defense is never complete. This is evidenced by the July 8 air attack on Kyiv hospitals. It was successfully carried out by applying means to suppress Ukrainian capabilities in order to defeat the desired targets effectively. Russian troops were conducting reconnaissance of the air defense system, conducting failed but exhausting assaults with small UAVs, and conducting SEAD operations until they cleared a path through which the missiles could hit essential facilities in the city center. Additionally, especially in such situations, the defense systems themselves may be targeted and suffer losses, which affects the consistency and scope of

the A2AD bubble. Moreover, because attackers know which targets they will attack, they can concentrate enough resources to break active defense systems, as was the case at the Zaporizhzhia Nuclear Power Plant, where a Ukrainian territorial defense battalion had to face several subunits superior in terms of numbers and firepower. As a result, the bubble broke and the installation fell into the hands of Russian forces.

In conclusion, this tactic is the most effective when protecting Critical Infrastructure subsystems, although it is costly and ineffective in every situation. Moreover, it increases the cost of access to selected systems, but the bubble will be broken with a suitably motivated and equipped opponent.

Redundancy

The last and most effective tactic for protecting Critical Infrastructure hubs and nodes is costly. In this regard, "redundancy" means: "an excess of something in relation to what is required or sufficient. This concept can be applied to many scientific fields, such as engineering, management, economics, and linguistics. Very often, however, this procedure is used in a positive sense. It is treated as a security system in the event of damage to the equipment, project, or unit" (Kowalski, 2024). The term refers to two dimensions. The first is to increase the system's output about needs so that none of its segments will work under the full possible load. The second is to have enough spare elements to recreate its shape after the attack. The second understanding was evident in the "war of currents" case when the Ukrainian services restored the functioning of the power grid after each Russian airstrike.

Moreover, although the energy system in Ukraine is still functioning, it is much less efficient and has a higher failure rate than before the attacks. Even with international assistance, achieving full redundancy of Critical Infrastructure networks is extremely difficult and expensive, especially without extensive prior preparation. However, compared to other defensive tactics, this one has the best chance of success.

Instead of forecast

The war in Ukraine, which has been ongoing since February 24, 2022, will not end in the foreseeable future. Even the mythical presidency of Donald Trump will have a very limited impact on these events. However, lessons about the role of Critical Infrastructure in the contemporary world, its incalculable value to society, and tactics to attack and defend it must be learned and remembered. It should be analyzed very carefully because of the development of technology and civilization and the dissemination of technological achievements in almost every area of life. Nation-States will discover new layers of vulnerability as they rely on these systems

in their activities. Furthermore, as the international environment becomes more and more turbulent, protecting one's access to these capabilities and denying them to the opponent will become an increasingly important part of any military operation.

The Ukrainian lesson is clear. The best methods for destroying Critical Infrastructure are cyberattacks and sabotage. They require the least resources to carry out and can bring the most spectacular results, even if they are temporary in the case of a cyberattack and relatively light in the case of sabotage. However, these are the tactics that, compared to the others, are relatively the least burdensome. Furthermore, as time passes and global systems integrate into one coherent whole, the effectiveness of these tactics will only increase. Active defense (creating an anti-access bubble) and passive redundancy, i.e. constant damage reconstruction, come to the fore when defending Critical Infrastructure. These tactics are costly, but the benefit of uninterrupted access to the full range of global Critical Infrastructure facilities and functions will fully offset the costs incurred. However, to be fully effective, they must be implemented years before the actual beginning of the conflict.

Finally, it is vital to consider the extent to which an attack on Critical Infrastructure hubs and nodes can cascade into a situation that would initiate the response from a mutual defense system such as NATO. Global Critical Infrastructure does not appear to be sufficiently integrated to create these conditions. Therefore, it mainly depends on political decisions. However, as critical infrastructure networks evolve and become more sophisticated, these types of situations will re-emerge in the future and will require further analysis.

References

Bojanowska, M. (2024, June 24). *Ogromny pożar pod Moskwą. Media: Płonie instytut powiązany z ministerstwem obrony Rosji*. Gazeta.pl. Wiadomości.

Bounaoui, S. (2024, April 16). *Pożar w Moskwie. W ogniu stanął kluczowy dla Rosjan zakład zbrojeniowy*. Wiadomości WP.

Ciastoń, R. (2022). Russian Federation's use of ballistic and cruise missiles in the Ukrainian conflict. *Pulaski Policy Papers*, *6*.

Co to jest cyberatak?. Microsoft, 2024.

Commission of the European Communities, Communication from the Commission on a European Programme for Critical Infrastructure Protection, COM(2006) 786, 2006, December 12.

Cooper, T. (2024, July 11). Ukraine War, July 11, 2024: Mobutu Syndrome, Part 1. *Sarcastosaurus*.

Czym wysadzono w powietrze Most Krymski i jakie są tego konsekwencje. Belsat.pl, 2022, October 8.

Docent uniwersytetu w Charkowie pracował dla rosyjskiego wywiadu. Został zatrzymany. Radio dla Ciebie, 2023, November 15.

Dura, M. (2024, July 17). *Prezes Radugi się chwali, a rakiet w Rosji brakuje*. Defence24.pl.

Fiszer, M., & Fiszer, J. (2023, December 30). *675. dzień wojny. Co zrobić z obroną powietrzną po tym, jak „odwiedził" nas rosyjski pocisk?*. Polityka.pl.

„FT": USA nalegają, by Ukraina wstrzymała ataki na rosyjskie. Bankier.pl, 2024, March 22.

Grzeszak, A. (2023, February 9). *Rosja bombarduje, ale Ukraina nie gaśnie. Jakim cudem uniknęła blackoutu?*. Polityka.pl.

Junko, J. (2024, May 8). *Wojna w Ukrainie. Rosja zaatakowała magazyny gazu w obwodzie lwowskim*. Bankier.pl.

Kardaś, S., & Łoskot-Strachota, A. (2022). *Dywersja na gazociągach Nord Stream 1 i Nord Stream 2*. Ośrodek Studiów Wschodnich.

Karta Narodów Zjednoczonych z 1945 roku, Dz.U. 1949, nr 23, poz. 90.

Kettl, D.F. (2014). *System under Stress. The Challenge to 21st Century Governance*. CQ Press.

Konwencja dotycząca praw i zwyczajów wojny lądowej z 1907 roku, Dz.U. 1927, nr 21, poz. 161.

Konwencja Rady Europy o cyberprzestępczości, sporządzona w Budapeszcie dnia 23 listopada 2001 roku, Dz.U. 2015, poz. 728.

Kowalski, D. (2024). Redundancja. *Encyklopedia zarządzania*.

Lewis, A.M., Ward, D., Cyra, L., & Naouma, K. (2013). European reference network for critical infrastructure protection. *International Journal of Critical Infrastructure Protection*, *6*(1), 51–60.

Matuszak, S. (2023, January 18). Na krawędzi – Ukraina wobec ostrzału systemu elektroenergetycznego. *Komentarze OSW*.

Mątecki, K. (2024, March 1). *Nieudany desant ukraińskich sił specjalnych*. Special Ops.

Melkozerova, V. (2024, April 22). *Kharkiv TV tower destroyed in Russian missile attac*k. Politico.

Microsoft twierdzi, że awaria dotknęła 8,5 mln urządzeń z systemem Windows. Business Insider, 2024, July 20.

Misiągiewicz, J. (2015). Teoria sekurytyzacji w analizie energetycznego wymiaru bezpieczeństwa narodowego. In E. Stadtmüller & Ł. Fijałkowski (Eds.), *Normy, wartości i instytucje we współczesnych stosunkach międzynarodowych* (vol. 2, pp. 393–411). Rambler.

Multiple Futures Project. Navigating towards 2030. Final Report. Allied Command of Transformation, 2009, April.

Multiple Futures Project. Navigating towards 2030. Findings and Recommendations. Allied Command of Transformation, 2009, April.

Naprawa Mostu Krymskiego potrwa przynajmniej do września 2023 r., Forsal.pl, 2022, November 9.

Niedziński, B. (2024, July 12). *Brytyjski rząd nie dawał zgody na atakowanie celów w Rosji pociskami Storm Shadow*. Bankier.pl.

Official statement of the ATESH movement, "Cybershafarat", 2022, September 11.

Palowski, J. (2024, May 20). *Amerykanie przyspieszają wprowadzenie rakiet sprawdzonych na Ukrainie.* Defence24.pl.

Placha, K. (2014, January 21). *Radary w lotnictwie cywilnym. Rok 2014.* Polot.

Pomper, M., & Tuganov, V. (2023). Role of missiles in Russia's war on Ukraine and its implications for the future of warfare. In A. Vicente, P. Sinovets, & J. Theron (Eds.), *Russia's War on Ukraine: The Implications for the Global Nuclear Order* (pp. 69–93). Springer.

Protokół dodatkowy (I) do Konwencji Genewskich z 12 sierpnia 1949 z 1977 roku, Dz.U. 1992, nr 41, poz. 175.

Regulamin działań wojsk lądowych. Warszawa 1999.

Rosja atakuje kolejne obiekty energetyczne. Uszkodzone dwie elektrociepłownie. Energetyka24.pl, 2024, June 1.

Rosyjskie media rozpowszechniają nieprawdziwe wiadomości o włamaniu się do ukraińskiego systemu „Delta". Militarnyi, 2022, November 2.

Sharpe, T. (2024, February 27). *Russia may have just carried out its first direct action against the West*. The Telegraph.

Szopa, M. (2023a, August 30). *Pogrom rosyjskiego lotnictwa transportowego*. Defence24.pl.

Szopa, M. (2023b, March 14). *Czy w Jejsku doszło do masakry Su-34?*. Defence24.pl.

Szopa, M. (2024, April 5). *Zmasowany atak dronów. Ukraińskie uderzenie w rosyjskie lotniska*. Defence24.pl.

Tarter, A. (2015). Securing critical infrastructure. *The Military Engineer*, *107*(697).

The White House Office of the Press Secretary, Presidential Policy Directive/PPD-21 – Critical Infrastructure Security and Resilience. The White House. President Barrack Obama, 2013, February 12.

Tymchenko, O. (2024, April 25). *W rosyjskim mieście Omsk wybuchł potężny pożar, w którym płoną zbiorniki z produktami naftowymi. Zdjęcia i wideo*. OBOZ.UA.

Ukraina potwierdza zgodę na atakowanie celów w Rosji. USA wyznaczyły granice. Rzeczpospolita, 2024, May 31.

Ukraine Says Russia Has Fired Five Zircon Missiles at Kyiv This Year. Reuters, 2024, April 1.

Watling, J. (2025) *Long-range precision fires in the Russo-Ukrainian war.* In D. Henriksen & J. Bronk (Eds.), *The Air War in Ukraine – the First Year of Conflict*. Oxon.

What Is the Russian Bomber Plane That Ukraine Says It Shot Down?. Reuters, 2024, April 19.

Wielki pożar w Petersburgu. Przeciwnicy mobilizacji do wojska podpalili „rosyjski Amazon"?. Money.pl, 2024, January 24.

Wilk, A., Żochowski, P., & Ber, J. (2023, June 6). Wysadzenie tamy na Dnieprze w Nowej Kachowce. 467. dzień wojny. *OSW. Analizy*.

Wilton, P. (2022, June 10). *Kyiv TV tower attack evokes echoes of Ukraine's tragic past*. University of London.

Wyciszkiewicz, E. (Ed.). (2008). *Geopolityka rurociągów. Współzależność energetyczna a stosunki międzypaństwowe na obszarze postsowieckim.* PISM.

ZDENĚK ROD

UNIVERSITY OF WEST BOHEMIA, PILSEN

Reconstruction Roadmap: Current Perspectives on Ukraine's Post-Conflict Recovery

Abstract: This chapter thoroughly examines the considerations and anticipations for Ukraine's post-conflict reconstruction, shedding light on pivotal facets of this complex issue. The initial segment presents an overview of the present devastation in Ukraine, delineating extensive destruction across various sectors. The subsequent section emphasises the principles guiding reconstruction endeavours, focusing on integrating environmentally sustainable policies and the imperative of transparency. Moreover, the chapter delves into the significant challenges rendering Ukraine's reconstruction uniquely formidable. These encompass the staggering financial requirements, the escalation in mental health disorders, the menace of landmine contamination, and the economic strains exacerbated by labour shortages. Despite these hurdles, international entities such as the EU, World Bank, and IMF have pledged considerable support, although projected costs will likely surpass initial estimations. Central to Ukraine's revival is the emphasis on environmental consciousness and transparency, essential for its alignment with EU standards and aspirations. Furthermore, the chapter delineates the intricate path of Ukraine's reconstruction, incorporating tasks such as landmine clearance, infrastructure repair, healthcare system overhaul, veteran reintegration, security sector reform, sustainable development governance, and reconciliation efforts. Addressing these multifaceted challenges necessitates persistent international cooperation and strategic planning to steer Ukraine towards a peaceful and prosperous future.

Keywords: post-conflict reconstruction; Ukraine; financial support; governance; security sector reform; reconciliation; international cooperation

Introduction

Ukraine has been embroiled in high-intensity warfare for over two years, facing relentless daily artillery bombardments, drone assaults, and continued Russian kinetic operations. Russia has been consistently reinforcing its efforts with increased ammunition, weaponry, and manpower. Regrettably, there are no signs that the conflict

will conclude in the near future. In May 2024, Russia launched several successful offensive campaigns, primarily in the Kharkiv region (ISW, 2024). This has led to expectations that Russian forces may advance even further. Some analysts, such as Sergey Vakulenko (2024), argue that Russia possesses the resources necessary to sustain a prolonged conflict in Ukraine. Why should we pay attention to post-conflict reconstruction efforts in Ukraine during an ongoing conflict with no foreseeable end? The reason is clear. First, the West needs a realistic perspective on what it would entail to reconstruct Ukraine if the war were to end suddenly.

Second, the reconstruction of Ukraine is poised to be one of the largest and most challenging reconstruction efforts in human history, presenting the West with an unprecedented task. Some might argue that this is not entirely true, noting that the West has undertaken various reconstruction efforts before – from the rebuilding of Germany and Japan in the 1940s, to efforts in Bosnia and Kosovo in the 1990s, and more recently, in Afghanistan and Iraq during the 2000s and 2010s. However, the scale and complexity of Ukraine's reconstruction are expected to surpass these past efforts. Despite the West's substantial reconstruction know-how, it largely lacks valid and recent experience in rebuilding a modern state, with the exception of efforts in Europe during the 1940s and 1950s. For example, the reconstruction of Afghanistan, given its development level, was an entirely different endeavour compared to Ukraine. Ukraine is a complex, modern Eastern European state, making its reconstruction a significant challenge.

Third, the reconstruction of Ukraine is a core strategic interest for the West, particularly for the European members of the EU and NATO. The reasoning is clear: a weak and potentially failing Ukraine would generate numerous insecurities for its neighbouring countries. Failing states often produce uncontrolled migration, gun and human trafficking, organized crime, and other destabilizing factors. Therefore, it is in the West's best interest to support the rebuilding of Ukraine, whatever it takes, to prevent these negative externalities. It is crucial for Western interests that Ukraine emerges as a modern, functioning state to prevent instability between EU/NATO countries and Russia.

This chapter holistically assess what the West should expect and consider when planning the post-conflict reconstruction of Ukraine. Therefore, the following sections will address key aspects of this complex issue. The first section presents an overview of the current destruction in Ukraine. The second section focuses on the principles of reconstruction, emphasizing the importance of incorporating "green" policies and ensuring transparency. The third section delves into the most significant factors that make Ukraine's reconstruction uniquely challenging. The conclusion discusses the importance of these reconstruction efforts in the context of European security.

Moreover, the chapter contends that Ukraine's reconstruction faces formidable hurdles spanning multiple sectors, with an estimated expenditure of approximately USD

500 billion essential for infrastructure rehabilitation. The harrowing toll of conflict has precipitated a surge in mental health afflictions, compounded by assaults on vital healthcare facilities, while the looming spectre of landmine contamination imperils both agricultural productivity and civilian well-being. The economic landscape further complicates matters, with a projected deficit of USD 41 billion in 2024 exacerbating the strain wrought by labour shortages stemming from population displacement. Nevertheless, international bodies such as the EU, World Bank, and IMF have stepped forward with considerable commitments of support, although prognostications indicate that the requisite funds may soar as high as USD 1 trillion. At the helm of Ukraine's rejuvenation lie the twin tenets of environmental conscientiousness and transparency, foundational to its aspirations for EU integration. Noteworthy endeavours like the Ukraine Facility and the commendable DREAM initiative highlight global solidarity, yet simultaneously underscore the indispensable need for sustained backing. In addition to fiscal exigencies, the labyrinthine path of Ukraine's reconstruction is beset by myriad intricacies, encompassing landmine eradication, infrastructure refurbishment, healthcare system overhaul, veteran reintegration, security sector reform, governance for sustainable development, and the delicate task of fostering reconciliation. Addressing these multifaceted challenges necessitates unwavering international collaboration and strategic foresight to guide Ukraine towards a tranquil and prosperous future.

Estimates of damage

The current losses are staggering. As Igor Dunayev et al. (2024, p. 15) highlight, the damage to Ukraine's infrastructure necessitates approximately USD 500 billion for reconstruction, a figure that continues to climb, particularly in frontline regions. Beyond the Kakhovka Dam, the bulk of these losses have affected residential buildings, presenting a significant future budgetary challenge.

The latest report from February 2024 by the Kyiv School of Economics (KSE, 2024) underscores that the most significant losses have been sustained by residential buildings. Specifically, the report indicates that approximately 250,000 houses have been destroyed, along with 212,000 vehicles, 16,000 public transportation vehicles, 3,800 educational buildings, 1,300 healthcare institutions, and 426 private and state enterprises. Additionally, there are substantial losses in trade, tourism, digital infrastructure, and the social sphere. The KSE estimates that these losses amount to USD 155 billion. However, as Dunayev et al. (2024) point out, rebuilding Ukraine will require three times that amount.

Furthermore, despite the huge infrastructure losses, houses and roads can still be rebuild with extensive financial injections. What cannot be so easily rebuild is the psychic of people who have been affected by this war. As the recent scholarship points out (Seleznova et al., 2023), the conflict in Ukraine has exacerbated a mental

health crisis, revealing weaknesses in the country's mental health care system and highlighting the economic challenges of providing services during wartime. Traumatic experiences, displacement, and financial struggles have led to high rates of mental disorders among Ukrainians. Attacks on healthcare facilities have further strained mental health services, exacerbating existing shortages of resources and personnel. Addressing this crisis requires comprehensive planning, international collaboration, and research into the economic dimensions of mental health care to ensure effective support for the population.

Another striking issue is the sheer volume of landmines that Russian troops have managed to disseminate over the years. Since Russia's full-scale invasion began two years ago, Ukraine has become one of the most heavily mined countries in the world, with landmines documented in 11 of its 27 regions. This crisis is having a devastating impact on Ukraine's agriculture, resulting in over 1,000 civilian casualties and rendering millions of acres of farmland unusable. The extent of contamination is particularly severe in areas like Hrakove near Izium (Tsirkin & De Luce, 2024), where over 15% of Ukraine's farmland is now contaminated. Clearing these mines is extraordinarily complex and will take decades to complete, mainly as the conflict shows no signs of abating. This situation poses immediate risks to civilians and threatens long-term economic stability and recovery in Ukraine (Farmer, 2024).

Moreover, the Ukrainian economy has endured several significant shocks. Notably, in 2022, Ukraine's gross domestic product (GDP) plummeted by nearly 30%. Furthermore, the 2024 state budget projects an unprecedented deficit of USD 41 billion, marking a 19% increase from 2023. This situation shows no signs of improvement in the near future (Rakic, 2024, p. 1, 6).

Another significant impediment to economic recovery is the shortage of labour. With approximately one-fifth of the population having fled the country and many men conscripted into the armed forces, there will be a substantial deficiency in the labour force available to support the remaining operational businesses across the nation. Many people have also died. Ukrainian government sources estimate between 33,000 and 41,000 civilian fatalities, with the battle for Mariupol alone accounting for approximately 25,000 deaths. Additionally, as of June 26, 2023, the UNHCR data portal recorded over 5,977,000 Ukrainian refugees across Europe. The ongoing state of emergency and conflict in Ukraine will likely complicate the return and rehabilitation of these refugees in a post-war Ukraine (Samore, 2023). At the time, around 30% of businesses had ceased production. Trade was severely disrupted by the blockade in the Black Sea, and although agricultural exports resumed in August 2022, they did not reach their pre-blockade levels. The World Bank reports that the real value of goods and services exports in 2022 decreased by 60% compared to the previous year, while imports fell by 30%. Furthermore, the unemployment rate in 2023 stood at 20% (Mills et al., 2023, pp. 14–15).

Financing the costs of the Ukrainian recovery

Before delving into the subsequent parts of this chapter, it is crucial to outline the financial perspective. Various international organizations, including the EU, World Bank, and IMF, have pledged substantial financial support for Ukraine's recovery. Focusing on the EU as the principal actor in Ukrainian reconstruction, the EU has committed a significant sum of EUR 49.4 billion to bolster Ukraine's economic, social, and financial resilience. While the EU lags behind the US in military support, it has contributed and will continue to contribute considerable funds for stabilization and reconstruction initiatives (European Commission, 2024a).

Additionally, to support Ukraine's recovery, reconstruction, and modernization efforts, the EU will launch a new support mechanism from 2024 to 2027. Known as the Ukraine Facility, this initiative will provide Ukraine with up to EUR 50 billion in stable and predictable financial assistance during this period. The Facility demonstrates the EU's dedication to aiding Ukraine amid Russia's ongoing aggression and its journey towards EU membership (European Commission, 2024a). This support will be funded through a mix of loans and grants. The EU aims to raise up to EUR 33 billion on the financial market by the end of 2027 by issuing EU bonds under a unified funding strategy. Grants will be financed through the EU's annual budget via a new special instrument called the Ukraine Reserve. This instrument will be activated each year as part of the budget process, based on Ukraine's progress in implementing reforms and utilizing investments. To receive this support, Ukraine must follow its recovery and reform plan and uphold essential democratic principles. These include maintaining democratic mechanisms like a multi-party parliamentary system, the rule of law, and the protection of human rights, including the rights of minorities (European Commission, 2024b).

Focusing on the World Bank, since February 2022, the World Bank Group has mobilized over USD 42 billion in financial support for Ukraine, with nearly USD 36 billion disbursed as of May 17, 2024. Notably, 95% of this financing was provided by development partners (World Bank, 2024). Meanwhile, the IMF Executive Board has concluded the third review of Ukraine's Extended Fund Facility (EFF) arrangement, approving the disbursement of approximately USD 880 million for budget support. Despite operating under challenging conditions, Ukrainian authorities have performed robustly under the EFF, meeting nearly all quantitative performance criteria, structural benchmarks, and indicative targets. The Ukrainian economy exhibited significant resilience in 2023, though the resurgence of war-related challenges has led to an outlook of exceptionally high uncertainty. Sustained reform efforts are crucial to maintaining macroeconomic stability, achieving fiscal and debt sustainability, advancing institutional reforms, and laying the groundwork for reconstruction and eventual EU accession (IMF, 2024).

In addition to the main players highlighted above, there are other actors who have pledged individual support. For instance, Japan has committed USD 10 billion to Ukraine (VOA News, 2024). The UK mounted an effective and flexible civilian aid response to the crisis in Ukraine, including bilateral aid of GBP 228 million, making it now the UK's largest country programme, and a 5-year commitment of GBP 4 billion in loan guarantees (ICAI, 2024).

In a nutshell, Ukraine will require even more funds than have been provided thus far. Some experts, such as Daniel Feldman et al. (2023), estimate that the reconstruction of Ukraine will demand an unprecedented USD 1 trillion. In other words, Ukraine's needs amount to a Marshall Plan multiplied by ten. While some might argue that such a vast sum is unattainable, this is not entirely accurate. For instance, if we consider the financial outlay by the United States in Afghanistan, we find that the US spent USD 2 trillion overall, with approximately USD 141 billion allocated specifically for reconstruction tasks (Almukhtar & Nordland, 2019). However, much will also depend on how successful Ukrainian diplomacy will be in securing additional funds from around the world. Mobilizing resources will be critical.

Environmentally conscious and transparent

Before moving on, it is crucial to outline the two main principles guiding Ukrainian reconstruction: environmental consciousness and transparency. Implementing these principles will be of utmost importance for Ukraine's efforts to join the EU. The Ukrainian government must align with the EU Green Deal objectives and place a strong emphasis on transparency to meet the standards required for EU membership. The EU also requested the EU fund allocated to Ukrainian recovery have to focus on focus on environmental sustainability (European Commission, 2023). Moreover, though war inevitably brings unimaginable horrors, its aftermath presents opportunities for profound transformation. Numerous NGOs began advocating for a recovery strategy prioritizing the advancement of the green economy and the integration of targeted environmental and climate policies throughout Ukrainian society. Activists emphasized that Ukraine's recovery must not merely restore the pre-war *status quo* but should represent a definitive stride towards a European and environmentally sustainable future (Ecoaction, 2022).

Environment and green principles have already been also reflected by the Ukrainian Ministry of Environmental Protection and Natural Resources (2023). The Ministry has outlined several goals to be achieved and created a slogan "Build Back Better, Build Back Greener". The Ukrainian government is directing its efforts towards green initiatives, aiming to mitigate the impacts of the war and propel the country towards European integration. Firstly, focusing on green projects is anticipated to

generate up to 4.2 million jobs, offsetting the losses incurred during the conflict. Secondly, the adoption of European integration laws seeks to align Ukraine with EU standards, making the country more appealing to potential investors. Notably, investment is being solicited for the construction of new waste processing plants built to European standards, with twenty projects already underway across several cities despite facing ongoing shelling. Additionally, a Climate Office has been established in collaboration with German partners to facilitate the mobilization of green finance for post-war recovery efforts. Efforts are also underway to restore forests, with Ukraine aiming to plant 1 billion trees, having already completed almost 44% of the program. Furthermore, the establishment of seedling growth centers and a comprehensive reform of the forestry sector are part of the government's initiatives. Lastly, the digitalization of the forestry sector has been pursued through the implementation of electronic services for effective timber management.

Nevertheless, according to certain civil society experts, while there is vocal endorsement for green reconstruction, tangible actions are yet to materialize. They argue that upon scrutinizing Ukraine's current recovery documents, there is a prevailing sentiment that green efforts are secondary. Sustainability, they contend, has not emerged as a fundamental guiding principle in the recovery agenda. Green initiatives appear disjointed, and environmental considerations are still perceived merely as sectoral matters (Mishchuk, 2023, p. 2). Moreover, Examining the tasks feasible prior to the war's conclusion, the March 2023 Ukraine Rapid Damage and Needs Assessment offered a thorough account of the existing damages. Subsequently, in April 2023, Kyiv delineated its immediate recovery priorities for 2023, encompassing areas such as energy infrastructure, critical and social infrastructure, housing, and support for the private sector. These priorities hold significant implications for green reconstruction. By endorsing initiatives like renewable energy sources or incorporating environmentally friendly materials in the reconstruction of damaged housing, Ukraine can already set out on the crucial journey towards a more resilient and environmentally sustainable future (World Bank, 2023a; EEAS, 2023). Lastly, these efforts should not be seen as a new policy, but rather as a part of a pre-existing wider commitment of the developed countries towards fighting climate change and protecting the environment.

Transparency is a fundamental principle that must be upheld in Ukraine, particularly given the country's significant corruption challenges. It is consistently highlighted as a critical issue in discussions surrounding Ukraine's reconstruction. Referenced in the Lugano Declaration (AALEP, 2022), transparency underscores the need for accountability and openness throughout the recovery process, ensuring fairness in all funding allocations. Concerns related to transparency span various areas, including the implementation of anti-corruption reforms, access to information, monitoring of reconstruction funds, and the governance of state-owned

enterprises. Notably, several organizations convened a conference to address these issues on the sidelines of the Ukraine Recovery Conference in London (EBRD, 2023). While Ukraine has made some strides in combating corruption in recent years, it remains a significant concern. According to the Corruption Perceptions Index (CPI) for 2023, Ukraine scored 36 out of 100, placing it among the countries with the lowest rankings in the region, with only Russia faring worse (Transparency International, 2023).

Acknowledging transparency as a pressing issue, funders of reconstruction efforts are taking steps to address it. For example, Members of the European Parliament (2023) have proposed amendments to the Ukraine Facility proposal, aimed at enhancing transparency. They advocate for the establishment of a web portal detailing financial operations granted to Ukraine, along with its objectives and the country's milestones for aid eligibility. An initiative worth noting in the pursuit of transparency is the Digital Restoration Ecosystem for Accountable Management (DREAM). Developed by Ukraine with support from donor organizations, DREAM is an online platform designed to manage projects aimed at rebuilding the country's economy. It facilitates real-time collection, organization, and publication of open data across all stages of reconstruction projects. Recognized with the People's Award at the Copenhagen Democracy Summit, DREAM sets high standards for transparency and accountability (DREAM, 2024).

Key factors hindering reconstruction efforts

Having addressed the present situation, financial aspects, and guiding principles, this section will now delve into the intricacies of eight key challenges complicating Ukraine's reconstruction. These include extensive landmines, the need for infrastructure repairs, a comprehensive overhaul of the healthcare system, the reintegration of veterans, concerns regarding security and governance and fostering national cohesion. Each of these factors poses significant obstacles that must be carefully navigated to ensure the success of Ukraine's reconstruction efforts.

First, one of the critical issues Ukraine currently faces is the extensive presence of landmines. In other words, Ukraine is the world's largest minefield. The Ukrainian government estimates that approximately 174,000 square kilometres of the country's territory, which is more than twice the size of Czechia, may need demining. This accounts for nearly a third of Ukraine's total area. Although this estimate might be exaggerated, the danger posed by mines and unexploded ordnance, particularly in the eastern and southern regions, is significant. Nearly six million Ukrainians live in areas at risk of mine-related incidents. Russian forces have deliberately placed mines on Ukrainian farmland, and both Russian and Ukrainian forces have scattered

mines in coastal waters. This situation hampers agricultural activities and the export of Ukrainian goods, exacerbating the country's economic crisis (Nieczypor, 2023).

Extensive landmine contamination profoundly impacts Ukraine's agricultural sector, severely hindering production and adversely affecting food security. The danger in eastern Ukraine is so pervasive that it is unsafe for farmers to operate tractors in many areas. This situation is particularly concerning given Ukraine's crucial role as one of the world's leading grain exporters. Ukraine boasts some of the most fertile land globally, with 25–30% of the world's black soil reserves and over 100 million acres of agricultural land (Yang, 2024). To address this issue, the World Food Programme (WFP) has partnered with Ukrainian authorities to support farmers as part of a broader initiative to clear large swathes of contaminated land. The scale and cost of this endeavor are staggering, with the World Bank estimating that the required funds could exceed USD 37 billion (Abdelmageed et al., 2024). Moreover, clearing Ukraine's territories of mines currently costs USD 300 million annually (UNDP, 2023). Recognizing the enormity of this challenge, Kyiv acknowledges it cannot shoulder the financial burden alone and is intensifying efforts to secure equipment, personnel, and financial support from international partners (Nieczypor, 2023).

There are also several NGOs involved in the demining efforts, with one of the most prominent being the HALO Trust. Since 2022, HALO's operations have cleared over 3.15 million square meters of land, including crucial agricultural areas, thus enhancing food security. Before the war, Ukraine and Russia collectively played a significant role in global exports of wheat, grain, and sunflower oil. HALO has also cleared over 19,000 mines and conducted 1,550 explosive ordnance disposal callouts. Their extensive surveys have assessed explosive hazards in nearly 1,600 communities, with almost half of these now deemed safe for habitation. To protect people, particularly in newly liberated areas, HALO has conducted risk education sessions, reaching nearly 245,000 individuals in-person and online, along with a social media campaign that engaged over 34 million people (HALO, 2024).

Moreover, according to the United Nations (2023) and its UNDP programme, the extensive landmine contamination in Ukraine necessitates the rollout of a new demining approach. This strategy should initially focus on the issue of rubble removal. In just 40 settlements in the Kyiv region, the rubble from fighting could pave a road from Ukraine's capital to Berlin, according to UNDP estimates. Although the exact volume remains unknown, the safe processing and disposal of hazardous waste are imperative. Typically, 30 to 50% of unexploded ordnance remains active, posing a significant risk of explosion upon impact. Secondly, raising public awareness and education about demining is essential. Mine action goes beyond merely clearing explosives; it requires comprehensive public education. The UNDP stresses the importance of informing Ukrainians about the dangers of mine-contaminated areas. This is particularly crucial for residents of western regions, returnees, and refugees, considering

that demining efforts have been ongoing in eastern Ukraine since 2014. Thirdly, it is necessary to cultivate a mine action culture. The UNDP advocates for integrating mine action into Ukraine's cultural fabric, acknowledging its long-term importance. The key safety message – "Stay away! Don't touch! Call 101!" – should become a societal norm. Instead of relying on fear-inducing images, education should focus on imparting practical safety knowledge. By addressing these three key areas – rubble removal, public education, and cultural integration – Ukraine can better manage the pervasive threat of landmines and ensure safer living conditions for its citizens.

Second, another key challenge will be the vast task of infrastructure repair. The West and Ukraine must undertake an immense effort to repair or rebuild heavily damaged transport, energy, environmental, social, and housing infrastructure. This endeavour will require extensive amounts of money and workforce. According to the World Bank (2023b), Ukraine's infrastructure recovery will take several years and necessitate continuous public and private funding. Furthermore, based on Sander Winckel's (2023) analysis, Ukraine should consider several areas before delving into infrastructure repair. Firstly, the Ministry of Finance (MOF) should prioritize projects and align them with budgetary and technical resources, implementing a robust framework to evaluate and rank projects based on strategic importance and feasibility. Enhancing the quality of strategic planning documents and integrating comprehensive planning processes that consider long-term financial implications are essential. Secondly, building the technical capacity of project promoters and regulatory bodies is crucial for effective implementation. Ukraine should ensure feasibility studies are thorough and conducted by qualified professionals, setting standards for costs in line with international norms. Establishing an independent oversight body to review and appraise project feasibility studies will help identify issues early. Thirdly, simplifying approval processes and focusing on meaningful project approvals rather than mere regulatory compliance can prevent delays. Developing a clear, integrated permitting procedure and addressing specific challenges like archaeological permits and environmental impact assessments will improve efficiency. Lastly, encouraging proactive risk management and providing clear guidance to project managers can reduce delays and cost overruns. Improving procurement processes to focus on quality and suitability, and establishing clear guidelines for competitive bidding, will enhance project implementation. By addressing these areas, Ukraine can better manage its public investment projects and achieve more effective outcomes.

Thirdly, the Ukrainian government and its health sector will need to undertake a comprehensive overhaul of the healthcare system to address the surge in amputations and mental health issues among the population. While infrastructure can be relatively straightforward to repair with adequate funding, the same cannot be said for the human body and psyche. Focusing on the issue of amputations, the scale in Ukraine has now reached levels reminiscent of the aftermath of World War I, where

widespread use of field artillery resulted in numerous soldiers from all sides losing limbs. Due to the war, it is estimated that between 20,000 and 50,000 Ukrainians have undergone amputations, frequently losing one or more limbs. In stark contrast, fewer than 2,000 US veterans of the Afghanistan and Iraq conflicts had amputations. The Ukrainian government has kept precise statistics on amputations secret to prevent demoralizing the populace (Nova Ukraine, 2023; Pancevski, 2023). The Ukrainian healthcare system is not equipped to handle the immense pressure of a large number of disabled individuals requiring post-amputation care and specialized prosthetics. Frankly, many Western governments would struggle with such a challenge as well. Furthermore, disabled individuals also need psychological support, which the Ukrainian healthcare system is currently unable to provide to the necessary extent. Fortunately, many NGOs are stepping in to fill this gap. For example, Doctors Without Borders has provided more than 19,000 physiotherapy sessions to 668 patients (MSF, 2024). In addressing these complex and pressing needs, Ukraine must leverage both domestic and international resources to build a healthcare system capable of supporting the physical and mental recovery of its citizens.

Fourthly, Ukraine will need to address the crucial task of veteran reintegration by creating civilian job opportunities and psychological support programmes for the hundreds of thousands of veterans transitioning back to civilian life. This issue should not be underestimated. Examining the post-war situation in Bosnia after 1995, for instance, reveals that Bosnia had to demobilise and reintegrate 400,000 soldiers (Pietz, 2004, p. 34). Unfortunately, this reintegration did not go as planned, with many Bosnian veterans experiencing neurological disorders, psychotic conditions, and substance abuse (Sarač-Hadžihalilović et al., 2008; Pavlović et al., 2013). The Bosnian government, despite support from NGOs, lacked the capacity to adequately support its veterans. Veterans struggling with personal issues often find it difficult to maintain employment and lead normal lives, a situation that could similarly affect Ukraine. The longer the conflict continues, the more severe the psychological damage to Ukraine's combatant population will be. Lessons from the United States are also pertinent. In 2021, research from Brown University (Suit, 2021) revealed that 30,177 active duty personnel and veterans who served post-9/11 died by suicide, a stark contrast to the 7,057 service members killed in combat over the same period. This indicates that the suicide rate among military personnel is four times higher than combat-related deaths, a deeply concerning trend for military families who already sacrifice much for the protection of freedoms. Thus, Ukraine must prioritise robust reintegration strategies, drawing on international experiences to avoid similar pitfalls. Comprehensive mental health services and employment support will be essential in helping veterans rebuild their lives and contribute positively to society.

Fifthly, a matter of profound significance lies within the realm of security sector reform (SSR). Since 2014, the European Union Advisory Mission Ukraine (EUAM)

has been at the forefront of SSR endeavors. However, the mission's operations have been temporarily suspended amidst the persisting conflict. Nonetheless, EUAM remains steadfast in its commitment to resuming support post-conflict until 2027, as per the extant mandate (Council of the EU, 2024). The forthcoming SSR initiatives hold particular importance, notably in the imminent restructuring of Ukraine's vast armed forces, comprising approximately 800 thousand personnel, once hostilities cease. The rationale behind the European Union's substantial engagement in SSR, facilitated through EUAM, is unequivocal. With Ukraine's prospective accession to the EU on the horizon, alignment of its security sector with EU standards becomes imperative. EUAM, thus, endeavors to furnish strategic counsel and tangible assistance in effectuating specific reform measures congruent with EU norms and overarching principles of good governance and human rights. This includes bolstering Ukraine's fulfillment of accession-related commitments. In pursuit of these objectives, EUAM assumes the role of advisor, trainer, and supporter to pertinent Ukrainian entities, notably the Ministry of Internal Affairs and the National Police of Ukraine (Council of the EU, 2024).

The concept of sustainable development is intricately linked with the notion of good governance, particularly in the context of post-conflict scenarios. In such settings, governance frameworks often draw upon diverse theoretical underpinnings to navigate the transition from conflict to peace. Central to this approach is the recognition of sustainable development as a pivotal framework, which emphasises the delicate balance between economic growth, social advancement, and environmental preservation. This framework prioritises meeting the immediate needs of the current generation while safeguarding the ability of future generations to meet their own needs without compromise. Crucially, it underscores the interconnectedness between peace building and development, highlighting the imperative of addressing underlying social, economic, and environmental factors to effectively resolve conflict. The success of post-conflict governance for sustainable development hinges on several critical factors. Firstly, the state must prioritise establishing security and upholding the rule of law to cultivate an environment conducive to economic expansion and social progress. This entails initiatives such as the partial demobilisation and reintegration of former combatants into society, alongside ensuring the safety and security of civilian populations (Kruhlov, 2023, pp. 106–107).

Lastly, Ukraine finds itself at a crossroads where the daunting task of reconciliation looms large, reminiscent of similar challenges witnessed in conflict-ridden regions like the Balkans, Iraq, and Afghanistan. Dismissing the significance of reconciliation would be a grave error, as its impact on societal harmony can reverberate for generations to come. Central to Ukraine's post-war trajectory is the intricate process of reconciliation, navigating the delicate balance among Russian, Ukrainian, and other communities that will shape the nation's future. Elena Baylis (2023) offers

invaluable insights into this complex web of societal discord, tracing its origins to historical, identity, and legitimacy disputes stretching back from the days of Kievan Rus through the tumultuous Soviet and post-Soviet epochs. Baylis underscores the socio-psychological underpinnings of inter-community strife, highlighting the intertwined and antagonistic nature of these relationships. Reconciliation emerges as an indispensable tool to untangle these deep-seated social dynamics, steering the course towards mutual understanding and positive interdependence, thereby averting future conflicts. In her work, Baylis delineates three pivotal categories of reconciliation mechanisms: instrumental, historical, and structural. Instrumental measures, aimed at fostering positive experiences and dialogue, serve as the initial step in disrupting hostility. Historical mechanisms delve into past grievances through truth commissions, war crimes trials, and educational initiatives, offering a cathartic reckoning with history. Meanwhile, structural reforms stand as the bulwark of societal equality, safeguarding the rights of minority groups. While instrumental measures provide immediate respite, it is the historical and structural mechanisms that hold the promise of lasting peace and alignment with European values. Navigating this terrain is not without peril, as the inherent risks of these approaches underscore the high-stakes nature of Ukraine's reconciliation journey. However, by embracing these challenges with diligence and foresight, Ukraine can chart a course towards a future where peace and prosperity reign supreme.

Conclusions

The reconstruction of Ukraine post-conflict holds strategic significance for the West, rooted in the imperative of fostering stability in the region. This necessity arises from the need to prevent potential discord between EU and NATO countries and Russia. It is crucial for Western interests that Ukraine emerges as a modern, functional state capable of navigating complex geopolitical dynamics. However, achieving effective post-conflict reconstruction in Ukraine necessitates substantial support from the West. This support should encompass assistance in maintaining macro-financial stability and facilitating the country's recovery, modernization, and rebuilding efforts. One key area of focus for the West lies in addressing the challenges related to funding. There are legitimate concerns surrounding the sourcing of adequate financial resources for Ukraine's reconstruction, particularly against the backdrop of prevailing global economic pressures and existing financial commitments by the US and EU. Thus, concerted efforts are needed to navigate these challenges and ensure that Ukraine receives the necessary support for its reconstruction endeavours. Western assistance must extend beyond financial aid to include technical expertise, institutional strengthening, and policy guidance.

The success of Ukraine's reconstruction will depend not only on the amount of funding provided but also on the efficiency and transparency with which these resources are managed. Therefore, it is essential that the West commits to a long-term partnership with Ukraine, fostering an environment conducive to sustainable development and democratic governance. Moreover, the reconstruction of Ukraine presents an opportunity for the West to demonstrate its commitment to upholding international norms and supporting nations in their pursuit of sovereignty and stability. By playing a pivotal role in Ukraine's recovery, the West can reaffirm its dedication to promoting peace and security in a geopolitically sensitive region, ultimately contributing to a more stable and prosperous Europe.

References

AALEP. (2022, May 7). *Lugano Declaration for the Reconstruction of Ukraine*. http://www.aalep.eu/lugano-declaration-reconstruction-ukraine

Abdelmageed, N., Vallas, A., & Bryant, E. (2024, February 13). *War in Ukraine: How a demining project is bringing hope to farmers two years on*. World Food Programme. https://www.wfp.org/stories/war-ukraine-how-demining-project-bringing-hope-farmers-two-years.

Almukhtar, S., & Nordland, R. (2019, December 9). *What Did the U.S. Get for $2 Trillion in Afghanistan?*. New York Times. https://www.nytimes.com/interactive/2019/12/09/world/middleeast/afghanistan-war-cost.html.

Baylis, E. (2023). Post-conflict reconciliation in Ukraine. *4 Revue européenne du droit*, *71*(2023), 71–75.

Council of the EU. (2024). *EUAM Ukraine: Council extends the mandate of the EU Advisory Mission for Civilian Security Sector Reform until 2027*.

DREAM. (2024, May 31). *Digital Restoration Ecosystem for Accountable Management*. https://dream.gov.ua/ua

Dunayev, I., Kuchma, M., Byelova, L., Jatkiewicz, P., Bilichenko, O., & Poberezhets, H. (2024). Wartime destruction: regional assessment of damage to Ukraine's infrastructure. *International Journal of Environmental Studies*, *81*(1), 8–17. https://doi.org/10.1080/00207233.2024.2314862

EBRD. (2023). *Building a transparent and accountable Ukraine: key steps to recovery*. https://www.ebrd.com/news/events/building-a-transparent-and-accountable-ukraine-key-steps-to-recovery.html

Ecoaction. (2022, May 5). *Green Reconstruction of Ukraine: Position of Civil Society*. https://en.ecoaction.org.ua/green-reconstruction-ukraine.html

EEAS. (2023, April 6). *Multi-agency Donor Coordination Platform ramps up efforts to help Ukraine address priority recovery needs in 2023*. https://www.eeas.europa.eu/delegations/ukraine/multi-agency-donor-coordination-platform-ramps-efforts-help-ukraine-address_en

European Commission. (2023, November 27). *EU and Ukraine outline plans for sustainable reconstruction in a high-level conference*. https://ec.europa.eu/commission/presscorner/detail/en/ip_23_6055

European Commission (2024a). *Recovery and reconstruction of Ukraine*. https://eu-solidarity-ukraine.ec.europa.eu/eu-assistance-ukraine/recovery-and-reconstruction-ukraine_en#:~:text=At%20the%20Ukraine%20Recovery%20Conference,investment%20for%20the%20recovery%20and

European Commission (2024b). *The Ukrainian facility*. https://eu-solidarity-ukraine.ec.europa.eu/eu-assistance-ukraine/ukraine-facility_en

European Parliament. (2023, October 17). *A long-term solution for Ukraine's funding needs*. https://www.europarl.europa.eu/news/en/press-room/20231013IPR07125/a-long-term-solution-for-ukraine-s-funding-needs

Farmer, B.M. (2024, April 7). *Ukraine's landmine crisis*. CBS News. https://www.cbsnews.com/news/ukraines-landmine-crisis-60-minutes/

Feldman, D., Larson, A., Spiegel, D.L., & Szewczyk, B. (2023). *Ukraine's reconstruction*. Global Policy Watch. https://www.globalpolicywatch.com/2023/07/ukraines-reconstruction/

HALO. (2024). *Where We Work. Ukraine*. https://www.halotrust.org/where-we-work/europe-and-caucasus/ukraine/

ICAI. (2024, April 30). *UK aid to Ukraine has been fast, flexible and responsive but post-war reconstruction will need careful management*. https://icai.independent.gov.uk/uk-aid-to-ukraine-has-been-fast-flexible-and-responsive-but-post-war-reconstruction-will-need-careful-management/

IMF. (2024, March 21). *IMF executive board completes the third review of the extended fund facility arrangement for Ukraine*. https://www.imf.org/en/News/Articles/2024/03/21/pr2496-ukraine-imf-executive-board-completes-third-review-eff

ISW (2024, May 21). *Russian offensive campaign assessment*. https://www.understandingwar.org/backgrounder/russian-offensive-campaign-assessment-may-21-2024

Kruhlov, V.V. (2023). *Post-Conflict Governance in Ukraine*. National Technical University Kharkiv.

KSE. (2024, February 12). *$155 billion – the total amount of damages caused to Ukraine's infrastructure due to the war, as of January 2024*. https://kse.ua/about-the-school/news/155-billion-the-total-amount-of-damages-caused-to-ukraine-s-infrastructure-due-to-the-war-as-of-january-2024/#:~:text=As%20of%20January%202024%2C%20there,has%20increased%20by%20%244.8%20billion

MSF. (2024, January 3). *The long road to recovery for Ukraine's war wounded*. https://msf.org.au/article/project-news/long-road-recovery-ukraines-war-wounded.

Mills, C., Brien, P., & Butchard, P. (2023). *Post-Conflict Reconstruction Assistance to Ukraine*. House of Commons.

Ministry of Environmental Protection and Natural Resources of Ukraine. (2023, November 28). *Build Back Better, Build Back Greener – key principles of Ukraine's recon-*

struction. https://www.kmu.gov.ua/en/news/mindovkillia-build-back-better-vuild-vack-greener-kliuchovi-pryntsypy-vidbudovy-ukrainy

Mishchuk, Z. (2023). *The Green Recovery of Ukraine: a Challenging but Non-Negotiable Way to Succeed in the World of Tomorrow*. GLOBSEC.

Nieczypor, K. (2023, November 22). *Ukraine: The world's biggest minefield*. Ośrodek Studiów Wschodnich. https://www.osw.waw.pl/en/publikacje/osw-commentary/2023-11-22/ukraine-worlds-biggest-minefield

Nova Ukraine. (2023, September 7). *Ukraine's Amputee Numbers Surge, Echoing World War I Era*. https://novaukraine.org/ukraines-amputee-numbers-surge/#:~:text=The%20number%20of%20amputees%20in,losing%20one%20or%20more%20limbs

Pancevski, B. (2023, August 1). *In Ukraine, amputations already evoke scale of World War I*. Wall Street Journal. https://www.wsj.com/articles/in-ukraine-a-surge-in-amputations-reveals-the-human-cost-of-russias-war-d0bca320

Pavlović, S., Hasanović, M., Kravić-Prelić, N., & Pajević. I. (2013). Alcoholic beverages abuse of war veterans during and after the Bosnia-Herzegovina 1992–1995 war. *European Psychiatry*, *28*(1), 1.

Pietz, T. (2004). *Demobilization and Reintegration of Former Soldiers in Post-war Bosnia and Herzegovina*. Universität Hamburg.

Rakic, D. (2024). *Two years of war: The state of the Ukrainian economy in 10 charts*. European Parliament.

Samore, S. (2023, July 4). *Post-conflict Reconstruction in Ukraine: Challenges and Opportunities*. Instituto Affari Internazionali. https://www.iai.it/en/pubblicazioni/post-conflict-reconstruction-ukraine-challenges-and-opportunities.

Sarač-Hadžihalilović, A., Kulenović, A., & Kučukalić, A. (2008). Stress, memory and Bosnian war veterans. *Bosnian Journal of Basic Medical Sciences*, *8*(2), 135–140.

Seleznova, V., Pinchuk, I., Feldman, I., Virchenko, V., Wang, B., & Skokauskas, N. (2023). The battle for mental well-being in Ukraine: mental health crisis and economic aspects of mental health services in wartime. *International Journal of Mental Health Systems*, *17*(28), 1–5. https://doi.org/10.1186/s13033-023-00598-3

Suit, T.H. (2021). *High Suicide Rates among United States Service Members and Veterans of the Post-9/11 Wars*. Brown University.

Transparency International. (2023). *Ukraine*. https://cpi.ti-ukraine.org/en/

Tsirkin, J., De Luce, D., & Santaliz, K. (2024, February 20). *Two years after the Russian invasion, land mines plague one-third of Ukraine*. NBC News. https://www.nbcnews.com/investigations/two-years-russian-invasion-landmines-plague-one-third-ukraine-rcna138517

UNDP. (2023, October 11). *Innovative technologies could rid Ukraine of landmines in 10 years*. https://www.undp.org/ukraine/blog/innovative-technologies-could-rid-ukraine-landmines-10-years

United Nations. (2023, July 8). *Demining Ukraine: Bringing lifesaving expertise back home*. https://news.un.org/en/story/2023/07/1138477

Vakulenko, S. (2024, May 16). *Russia has the resources for a long war in Ukraine*. Carnegie Endowment for International Peace. https://carnegieendowment.org/research/2024/05/v-usloviyah-voennogo-bremeni-glavnye-voprosy-o-nastoyashem-i-budushem-rossijskoj-ekonomiki?lang=en

VOA News (2024, February 19). *Japan pledges support for Ukraine reconstruction*. https://www.voanews.com/a/japan-pledges-support-for-ukraine-reconstruction/7493152.html

Winckel, S. (2023, April 5). *Ukraine reconstruction: Preventing pitfalls in infrastructure investments*. CEPR. https://cepr.org/voxeu/columns/ukraine-reconstruction-preventing-pitfalls-infrastructure-investments

World Bank. (2023a). *Second Ukraine rapid damage and needs assessment (RDNA2): February 2022 – February 2023 (English)*.

World Bank. (2023b). *Updated Ukraine recovery and reconstruction needs assessment*. https://www.worldbank.org/en/news/press-release/2023/03/23/updated-ukraine-recovery-and-reconstruction-needs-assessment

World Bank. (2024). *World Bank group financing support mobilization to Ukraine since February 24, 2022*. https://www.worldbank.org/en/country/ukraine/brief/world-bank-emergency-financing-package-for-ukraine#:~:text=Since%20February%202022%2C%20the%20World,was%20provided%20by%20development%20partners

Yang, R. (2024, February 28). *Improving Food Security in Ukraine Through Demining*. U.S. Department of State. https://www.state.gov/improving-food-security-in-ukraine-through-demining/

PART VI

Security Issues and Threats

MIROSLAV PLUNDRICH

UNIVERSITY OF WEST BOHEMIA, PILSEN

How Foreign Activities of Hamas Strengthen Its Capacity Against Israel

Abstract: This chapter investigates the critical role of foreign diplomatic and financial support in Hamas's operational and political strengthening from 2006 to October 7, 2023. Utilizing the concept of antodiplomacy, developed by Plundrich, the research examines how non-state actors like Hamas engage in foreign policy activities similar to states. Through a qualitative quasi-meta-analysis of ten diverse sources, this study identifies Iran and Qatar as primary supporters of Hamas. The analysis reveals that Iran's extensive financial aid, military training, and provision of advanced weaponry have been pivotal in enhancing Hamas's military capabilities and enabling its asymmetric warfare against Israel. Additionally, Qatar's substantial economic assistance, infrastructure development, and diplomatic efforts have bolstered Hamas's governance in Gaza and its international legitimacy. This study addresses two key research questions: how diplomatic ties and foreign activities have supported Hamas's governance and *modus operandi*, and how these activities have facilitated its conflict with Israel. The findings underscore the importance of understanding the complex diplomatic and financial networks that empower non-state actors, highlighting the significant impact of antodiplomacy on global security dynamics.

Keywords: antodiplomacy; Hamas; Israel; foreign relations; diplomacy; non-state armed groups

Introduction

The current international system represents a comprehensive structural chest game where non-state actors confront states in many fields more than ever. Significantly, many non-state armed actors (NSAs) have strengthened their positions worldwide and are the leading challengers in past decades. They challenge interstate as well as intrastate environments. We could witness, for example, how the Taliban once again succeeded in its power in Afghanistan (2021), how Hezbollah has had a safe-rooted role in Lebanon (since 2006) and is an inherent part of the Middle Eastern game, or how Columbian, as well as Mexican drug cartels, profit from an enormous drug economy

(since 1980). The current notoriously well-known example is Hamas, which was able to launch coordinated attacks and surprise Israeli authorities on 7 October 2023.

During the last decades, many NSAs have achieved territorial gains, started governance, and actively joined the international stage. NSAs enter the intrastate environment in two different ways. On the one hand, NSAs traditionally represent predators with their armed attacks and/or terrorist attacks, as well as illegal parasites in economic systems. On the other hand, NSAs are capable, just like states, of having foreign connections in the military, financial, and political fields. However, to be so successful, as given in the examples above, those organizations must have qualitative and quantitative resources. More preciously, knowing where and from whom to get them is essential. It leads me to come up with the claim that the second outlined line of foreign activities today makes NSAs far more lethal, dangerous, and competitive actors in the international environment than ever before. It helps them be more lethal and efficient (first way). Hence, the central claim of the presented text is that this was precisely the case with Hamas. Therefore, the presented article aims to determine who supported Hamas via foreign policy activities from 2006 to 7 October 2023, how, and if it helped its capacity to fight against Israel. The article aims to provide answers to the two following research questions:

Q1: How did diplomatic ties and foreign activities help Hamas in its *modus operandi* and power over Gaza?

Q2: In which way did diplomatic activities and income help the Hamas fight Israel?

The presented text will draw on the theory of diplomacy of non-state armed actors – the so-called antodiplomacy. Miroslav Plundrich (2024) constructed the research approach of antodiplomacy at the University of West Bohemia in Pilsen, Czechia, using a method-focused, structured theoretical framework of diplomatic activities to answer the presented research question/s.

The following text is organized into six parts. In the first part, I present the context of the debate about foreign diplomatic activities of non-state armed actors and some evidence. The second part will draw the theoretical framework of previous research for the application. The third part presents the research design and answers to the chosen cases of Iran and Qatar. The other two parts present the highlights of the Hamas-Iran and Hamas-Qatar cases. In conclusion, the final part discusses the collected data corpus of Hamas diplomatic income in the context of research questions.

The debate of non-state armed actors' behavior on the international stage

Standard research of non-state armed actors usually describes their actions as threats in interstate and intrastate (terrorism, transnational organized crime, insurgencies, etc.). However, not every international activity of NSAs must be in violation

connotation. There is plenty of evidence. One can mention the line of string representatives between Hezbollah and Syria since 2000, foreign connections between Hezbollah and the Russian Federation in the context of the Syrian crisis (Szakola, 2016), or a 2012 meeting between a delegation of the Egyptian Muslim Brotherhood and representatives of the White House in the U.S (Tau, 2012), and a 2014 a secret summit, during which representatives of the Egypt Muslim brotherhood met with a delegation of the Iranian Revolutionary Guard Corps (Staff, 2019). In addition to diplomatic talks and actions, we can astonishingly mention activities such as participating in or organizing various international events such as conferences, forums, and exhibitions. One example could be from Beirut in 2004, where the conference "Where Next for the Global Anti-War and Anti-Globalization Movements?" occurred (Karmon, 2009). Other evidence could also be financial flows and investments. The commonly known flows are, for example, mutual financial support between the groups Boko Haram, Al-Shabab, al-Qaeda, or the former Islamic State. Next to those groups, the Hezbollah-Iran joint investment activities in Latin America should be highlighted (Neumann, 2011). For instance, their investments flow to Venezuela into oil and gas projects, etc. (see Plundrich 2024).

It is evident that the global environment, much more than before, stands for the NSAs as an opportunity to find their allies, finances, materials, public support, new members/recruits, etc. The excellent note came from Bridget Coggins (2015), who was one of the first authors to have paid attention to the foreign activities of NSAs. She referred to the situation "when rebels engage in strategic communication with foreign governments or agents, or with an occupying regime; they deem foreign". Such a foreign move is due to Coggins, usually essential for rebels. Groups, via such activities, are searching for legitimacy for the new regime, war, or support for a new state-building process. She also mentioned that "rebels seem to use diplomacy, or talk, in much the same way state leaders do".

Other scholars, such as Coggins (2015) and Arves et al. (2019), highlighted the so-called public diplomacy of NSAs. Rebels use direct and indirect tools, including media such as magazines, newspapers, radio, television, or the Internet, to target foreign governments and external public opinions. However, Darwich (2021) and then Plundrich (2024) have underlined the research above tendencies. Darwich expanded research on all types of NSAs (not only mentioned rebel groups) and claimed the need to revitalize Foreign Policy Analysis FPA). He constructed a thesis on how studying NSAs' foreign policies can revitalize FPA and drive its agenda into new labeled directions. Then Plundrich (2024) followed up in the context of Darwich and others mentioned above and constructed a theoretical approach to the diplomacy of non-state armed actors, called "antodiplomacy", which we use in our work.

The theoretical approach of antodiplomacy and its application

Others and our previous research have led us to claim that NSAs[1] behave internationally as states do. NSAs go international with the aim of diplomatic relations for many reasons, primarily for benefits from economic, military, political, or ideological areas. As we see below in the first table, the considered and submitted foreign policy with its tools of non-state armed actors is very similar to that of states.

Table 1. Comparison of foreign policy activities: States and non-state armed actors

Foreign policy activities of states	Comparison	"Foreign policy" activities of non-state armed actors
(HP) Exercise of military force, violent actions	≐	Exercise of military power, violence, actions – but moreover in asymmetric position and practice
(HP) Economic sanctions, boycotts, embargoes, etc.	≠	Cutting financial support
(HP) Breaking off diplomatic relations, bilateral contacts, the expulsion of diplomats, etc.	≐	Breaking of primarily unofficial partnerships – in the sense of law and jurisdiction
(SP) Military-to-military contacts	=	Military-to-military contacts
(SP) Development assistance, foreign direct investment, loans, etc.	≐	Financial support
(SP) Diplomatic tools: public diplomacy, diplomatic meetings, declarations, etc.	≐	Public diplomacy/propaganda, meetings of representatives, etc.

Source: Based on (Plundrich, 2024).

Hence, the antodiplomacy of non-state armed actors is here according to Plundrich (2024, pp. 216–217), defined as

> foreign contacts, activities, relations and actions of non-state armed actors with other units to achieve economic, ideological, military or political and any other types of advantages, while these actions may be different from or in opposition to the official foreign policy of the state in whose territory they are located.

Then, the conceptualization of antodiplomatic foreign tools to identify is classified as soft and hard power activities/tools. Soft power, antodiplomatic tools, and indicators are:

[1] In the context of this research, a non-state armed actor with a propensity to engage in foreign relations is defined as any entity that (1) operates independently of official state structures, (2) typically possesses the willingness and capacity to employ violence to achieve its objectives, and (3) can serve as a significant challenger to the authority of the state in which it is based (see Schneckener, 2007, pp. 10–11; Schneckener & Hoffman, 2011, pp. 2–3).

I. establishment of so-called cells abroad;
II. visits by representatives of non-state groups to representatives of other states or non-state actors;
III. participation in peace negotiations and processes abroad, outside their state;
IV. participation or organization of various international events, such as international conferences, forums, exhibitions, etc.;
V. formation and involvement in financial flows and investments with diverse actors abroad;
VI. military-to-military contacts, such as the exchange of military technologies and training of units with various foreign partners and
VII. public diplomacy.

And the hard tools of antodiplomacy stand as follows:

I. the exercise of military force, violence, and actions – but moreover in asymmetric position and practice;
II. cutting financial support;
III. breaking of primarily unofficial partnerships – in the sense of law and jurisdiction.

Together, the described conceptualization of antodiplomacy and its indicators will help us analyse Hamas's case. We focus on soft power activities and tools to answer research questions there.

Research design

The research investigates the primary supporters of Hamas, with a particular emphasis on Iran and Qatar. These two nations have emerged as pivotal actors in maintaining active foreign relations with Hamas, a conclusion drawn from an extensive dataset of 256 antodiplomatic connotations. This dataset was meticulously compiled through a qualitative quasi-meta-analysis of data from ten diverse and reputable sources: Al-Jazeera, *The Times of Israel*, Reuters, BBC, the Middle East Institute, the Brookings Institution, the Center for Strategic and International Studies (CSIS), the Middle East Monitor, Routledge, and *Foreign Affairs*.

The dataset consists of 186 antodiplomatic connotations, gathered through a rigorous manual qualitative content analysis of article titles and news reports from 2006 to 2023, where available. This analysis utilized specific keyword combinations relevant to the antodiplomacy of Hamas, including terms such as "aid", "military", "cooperation", "financial", "support", "partnership", "meetings", "alliance", and "assistance". The selected connotations were then subjected to a detailed content analysis, revealing the intricate dynamics of support and cooperation between Hamas and its key backers, Iran and Qatar. Qatar and Iran represent 52% together with

Hezbollah, then 18% Syria, 14% Turkey, 8% Saudi Arabia, 2% EU and 6% other NSAs from the Middle East.

To selected sources: We assert the necessity for a comprehensive and balanced approach to understanding Hamas's foreign activities and the connotations associated with its supporters. To achieve this, our data set incorporates information from ten diverse sources, ensuring transparency and a holistic perspective. First, we selected Al-Jazeera and *The Times of Israel* to represent contrasting viewpoints from the Arab world and Israel, respectively. These sources provide invaluable insights into regional narratives and biases, highlighting differing perceptions and rhetoric surrounding Hamas. Al-Jazeera, known for its extensive coverage of Middle Eastern affairs, often presents perspectives that resonate with Arab audiences. At the same time, *The Times of Israel* offers an Israeli viewpoint, crucial for understanding how Hamas is viewed within and concerning Israeli policy and public opinion. In the pursuit of impartiality, Reuters was included as a globally recognized news agency known for its neutral stance. Its reports offer a balanced view critical for cross-referencing and validating information, free from the heavy influence of regional or political biases. The inclusion of the BBC provides a Western media perspective. The BBC is highly regarded for its comprehensive international coverage and is instrumental in understanding how Western nations perceive and report on Hamas's activities.

Additionally, we incorporated insights from three leading think tanks that have long-term engagements with Middle Eastern issues: the Middle East Institute, the Brookings Institution, and the Center for Strategic and International Studies (CSIS). These institutions provide deep analytical perspectives and policy-oriented research that offer a nuanced understanding of the geopolitical dynamics influencing and influenced by Hamas.

To enrich our analysis further, we referred to *Foreign Affairs*, known for its in-depth essays on international relations, and Routledge, a premier academic publisher whose scholarly articles offer rigorous analyses and historical context. Lastly, the Middle East Monitor was selected for its focus on current events and issues affecting the region, providing timely and relevant updates on developments related to Hamas.

We aim to present a well-rounded and substantiated understanding of Hamas's foreign activities by curating information from a diverse and reputable source. This approach ensures the inclusion of multiple perspectives and allows for a thorough examination of the complex web of regional and international relations surrounding Hamas and its supporters. For the presented article, two case studies of antodiplomacy of Hamas-Iran and Hamas-Qatar were chosen based on the high percentage of antodiplomatic connotations from the dataset.

Case study: Hamas-Iran

Hamas and Iran's relationship is a prime example of strategic alignment between a state and a non-state actor, collaborating to achieve mutual ideological, military, and political goals. This partnership highlights antodiplomacy in action, with Iran providing substantial support to enhance Hamas's operational capabilities against Israel. Since its formation in late 1987, Hamas has consistently received significant financial and other forms of support from Iran, as noted by Ziad Abu-Amr (1994, p. 12). Thus, the following text examines this relationship.

Financial support

For years, Iran's financial contributions were vital for Hamas's operations in Gaza, funding both military and governance activities. Iran provided direct financial aid to Hamas, which was used to fund military operations, pay salaries, and support social services within Gaza. Historically, funds raised from Iran ranged from USD 22 million to USD 70 million annually until 2011 (Levitt, 2006, p. 171; Vittori, 2011, p. 73). However, relations between Hamas and Iran deteriorated over Hamas's decision to break with the Assad regime during the Syrian civil war due to the Assad regime's targeting of Sunni Muslims.[2] This rift led to a reduction in funding for Hamas's political activities, although Iran continued to support the group's military wing (Hinz, 2021).

By early 2014, relations between Hamas and Iran began to improve. During the 2014 Gaza War, Iran pledged USD 250 million in aid to Hamas. By August 2017, Yahya Sinwar, the newly elected Hamas leader in Gaza, stated that Iran was once more "the largest backer financially and militarily" of Hamas's military wing. In 2019, Iran provided USD 22 million in financial aid to Hamas for its "resistance" efforts, and in 2020, it reportedly allocated USD 30 million. Today, US and Israeli officials estimate that Iran provides Hamas at least USD 70 million to USD 100 million annually. In a 2022 interview with Al Jazeera, Hamas leader Ismail Haniyeh claimed the group receives USD 70 million a year from Iran. Reports suggest that Iran has provided Hamas with an annual budget of around USD 100 million to USD 200 million (Levin, 2018; Katzman, 2021, pp. 34–35; Nakhoul, 2023).

[2] For years, ever since Jordan expelled the Hamas leadership from Amman, Jordan, in 1999, Hamas had maintained the headquarters of its external leadership in Damascus. But in January 2012, Hamas leader Khaled Mishal abandoned the group's Damascus base. By February 2012, Hamas deputy leader Mousa Abu Marzouk, then located in Egypt, commented (cited according to Sherwood, 2014): "The Iranians are not happy with our position on Syria, and when they are not happy, they do not deal with you in the same old way".

Iranian aid is often channelled through complex networks to avoid international detection and sanctions, ensuring a steady flow of resources to Hamas. For example, funds are frequently transferred through Hezbollah intermediaries and other proxies to mask the money flow. Iran's Islamic Revolutionary Guards Qods Force (IRGC-QF) funds are likely provided directly to Hamas's armed wing, the Izz-Al-Din Al-Qassam Brigades (see Vittorio, 2011; Al-Muhrabi, 2017; Zehorai, 2018). Primarily, Iranian funds have been used to build and maintain infrastructure in Gaza, including tunnels[3] for smuggling and military purposes. These tunnels are a crucial component of Hamas's strategy, allowing for the movement of weapons and fighters, as evidenced during the 2014 conflict (Clarke, 2023).

Military-to-military contacts

Iran has been a significant supplier of weapons to Hamas, including rockets, small arms, and advanced missile technology. These arms have been crucial in enabling Hamas to conduct military operations against Israel. The provision of rockets, for example, has significantly enhanced Hamas's capability to strike important targets throughout Israel. Already in 1994, Palestinian author-turned-legislator Ziad Abu-Amr (1994, p. 88) noted that Iran provided logistical support and military training to Hamas members, estimating Iranian assistance at tens of millions of dollars.

The support from Iran has grown over time, particularly after Hamas seized control of the Gaza Strip in 2007. A 2010 U.S. Department of Defense report highlighted that Iran provided funding, weapons, and training to Hezbollah and several Palestinian terrorist groups, including Hamas, to oppose Israel and disrupt the Middle East Peace Process. This assistance was smuggled into Gaza through tunnels under the Philadelphi corridor along the Gaza-Egypt border. In 2012, the U.S. State Department noted that Hamas used smuggling tunnels from Egypt and maritime routes to import weapons from Iran into Gaza. Since 2007, Hamas has focused on solidifying its control in Gaza, hardening its defenses, building its weapons caches, tightening security, and conducting limited operations against Israeli military forces (US Department of State, 2013; Shine & Catran, 2017, p. 152).

In financial terms, since 2007, Hamas has reportedly spent USD 100 million annually on military infrastructure, with USD 40 million dedicated to tunnel-digging activities that employ 1,500 Palestinians (Issacharoff, 2016). Iran has provided

[3] Hamas also financed the construction of tunnels for military purposes. In 2016, nearly USD 40 million of the annual military budget was allegedly allocated for digging these tunnels. The average salary for an excavator was reported to be between USD 250 and USD 400 per month, with veteran diggers receiving higher salaries. Excavators were incentivized to meet deadlines through the offering of bonuses. These tunnels were used to smuggle weapons from Iran, cash, and other materials (Martynova, 2023).

Hamas with technology and materials to produce rockets locally in Gaza. After the 2014 Hamas-Israel conflict, Iran sought to rebuild its relationship with Hamas by providing missile technology, which Hamas used to construct its own rockets and rebuild tunnels destroyed during the conflict (Hinz, 2021).

Iranian-supplied rocket technology has allowed Hamas to enhance its striking power and sustain prolonged military engagements with Israel. Notable rockets include the Qassam, the more advanced M-75, and Fajr-5 rockets, which have been used in various conflicts, most recently in 2021. Iran's military support also includes training and tactical support.[4] The Iranian Revolutionary Guard Corps (IRGC) and Hezbollah operatives have provided training to Hamas operatives in guerrilla warfare, urban combat, and advanced tactics, both in Iran and Lebanon. This training encompasses underground tunnel construction and improvised explosive devices (Clarke, 2023; Shine & Catran, 2017, p. 152).

Iranian experts have assisted Hamas in developing more sophisticated weapons systems, including drones and long-range missiles. Iran also provides strategic advice and intelligence support, helping Hamas plan and execute military operations more effectively. This strategic coordination enhances Hamas's ability to conduct complex operations, as demonstrated in the 2021 conflict, where over 4,000 rockets were fired into Israel (Warrick et al., 2023).

In summary, Iran has been a critical military supporter of Hamas, providing Fajr-5, Grad, and Qassam rockets, mortars, anti-tank missiles, and technical expertise for homemade rocket production. The IRGC has also reportedly provided training on rocket manufacturing and warfare tactics to Hamas operatives.

Public diplomacy and political support

Iran's diplomatic backing of Hamas has been crucial for its political legitimacy and its ability to garner support from other international actors. Iran has given Hamas significant political leverage and international legitimacy through international advocacy, political coordination, and public diplomacy.

Iran consistently advocated for Palestinian rights and supported Hamas's objectives in international forums, providing a platform for Hamas to gain international sympathy and legitimacy. Utilizing its position in bodies like the United Nations, Iran highlighted the Palestinian cause and supported Hamas's political stance. This advocacy helped counteract Hamas's diplomatic isolation from Western countries, providing it with a degree of international legitimacy. Iran's backing in forums such

[4] Iran has played a crucial role in developing Hamas into a formidable organization, transforming it from a rag-tag militia into a force that now boasts 40,000 fighters, a naval commando unit, and cyber warfare capabilities (Clarke, 2023).

as the Organization of Islamic Cooperation was particularly influential (see Seurat, 2021; Skare, 2023).

Regular meetings between Hamas and Iranian officials ensured coordinated political and military strategies, reinforcing their alliance and shared goals. These high-level meetings, involving top leaders from both sides, focused on strategic coordination and mutual support. Such engagements ensured that Hamas's military and political actions aligned with Iran's broader regional strategic objectives (see Muslih, 1999; Skare, 2021). Meetings often occurred in Tehran and Beirut, involving senior Hamas officials like Ismail Haniyeh and Khaled Meshaal. Next to them, Yahya Sinwar, a significant actor with close connections to Iran, played a crucial role in maintaining and strengthening these ties. Through these various forms of support, Iran has effectively enhanced Hamas's political standing and operational capabilities on the international stage (Levitt, 2023). Since 2017, Tehran has become a frequent destination for Hamas's visits (Abu-Amer, 2019).

Iran also employed public diplomacy to support Hamas and promote its narrative globally. Iranian media outlets, such as Press TV, broadcast content that supported Hamas and criticized Israeli policies, helping shape public opinion in favor of Hamas. These media campaigns were designed to bolster Hamas's image and support its recruitment efforts by portraying it as a legitimate resistance movement against occupation (see TOI, 2021). The narratives often emphasized the humanitarian crisis in Gaza and depicted Hamas's actions as defensive rather than aggressive.

Case study: Hamas-Qatar

Qatar's relationship with Hamas represents a sophisticated form of antodiplomacy, where economic and political support is provided under the guise of humanitarian aid. This strategy enabled Qatar to back Hamas while maintaining an image as a mediator in the conflict. Crucially, Qatar's support was vital for Gaza's economic stability and served as a counterbalance to the isolation imposed by Israel and other countries.

Qatar's investments in the Gaza Strip reflect its opportunistic foreign policy and ambitions to expand its influence in the Middle East. As a key benefactor and diplomatic of Hamas, Qatar has leveraged its financial resources and diplomatic clout to support the group's activities both in Gaza and beyond. By providing substantial financial assistance for infrastructure projects, social welfare programs, and humanitarian relief efforts in Gaza, Qatar has significantly contributed to Hamas's survival and governance in the territory.

Financial support

Since 2012, Qatar has played a pivotal role in supporting Gaza's economic stability, which indirectly bolsters Hamas's governance and operational capabilities. Following a then-Emir Hamad bin Khalifa visit to Gaza, Qatar pledged over USD 1.4 billion in aid, focusing on infrastructure development and humanitarian assistance. This substantial economic aid has been instrumental in stabilizing Gaza's economy and supporting Hamas's governance through direct financial support for social programs and investments in infrastructure (Rudoren, 2012; Guzansky, 2017, pp. 160–161).

From 2014 onwards, Qatar deepened its involvement by providing hundreds of millions of dollars to Gaza. At one point, Qatar was spending USD 30 million per month to help operate the enclave's sole power plant and support needy families and public servants in the Hamas-run government. A Qatari official highlighted that this aid provided USD 100 to the poorest Palestinian families and extended electricity availability in Gaza, thus helping to maintain stability and improve the quality of life for Palestinian families (Sayegh et al., 2023).

In 2018, Qatar began providing periodic cash injections to Gaza's Hamas rulers, with Israel's approval, to pay for fuel for the power plant, civil servant salaries, and aid for impoverished families. This assistance has been critical in mitigating the worsening humanitarian situation in Gaza. By 2021, Qatar had increased its annual aid to USD 360 million, allocated to employee salaries, financial aid for needy families, and operating power stations (see Guzansky & Zalayat, 2023; AP, 2023).

Qatar's investments in infrastructure projects, including homes, schools, and hospitals, have significantly improved living conditions and bolstered Hamas's control over the region. These reconstruction efforts have aided the local population and enhanced Hamas's legitimacy as a governing body. Qatar's investment in Gaza's infrastructure has been pivotal in maintaining Hamas's authority by providing essential services and improving living conditions (Elbagir et al., 2023).

By 2023, Hamas reportedly paid approximately USD 34.5 million per month in salaries, largely relying on international donors, with Qatar being a significant contributor. This ongoing financial support has been essential for Hamas to pay its municipal and military employees, demonstrating Qatar's crucial role in sustaining Gaza's economic stability and indirectly supporting Hamas's governance and operational capabilities (Al-Mughrabi, 2023).

Public diplomacy and political support

Doha's relationship with Hamas began around Sheikh Hamad bin Khalifa's ascension to power in 1995. Following the September 11, 2001, terrorist attacks in the U.S., Saudi Arabia clamped down on contributions to Islamic causes, and Western countries

stopped aid to the secular Palestinian Authority after Hamas's 2006 electoral victory and subsequent takeover of Gaza in 2007. Seizing the opportunity, Qatar committed USD 50 million to Gaza that year. According to informed sources, Qatar first opened a channel of communication with Hamas in 2006 at the request of the United States and has since helped broker ceasefires between Israel and Hamas in 2014, 2021, and 2022. Qatar has also provided significant economic and humanitarian assistance to Gaza, allowing the U.S. to engage indirectly with Hamas despite its designation as a terrorist organization by U.S. law (Kaussler, 2015, pp. 14–15; Cafiero, 2023).

In 2011, the Syrian uprising against President Bashar al-Assad led Hamas to break with Assad and, for a time, with Iran. By early 2012, Hamas had divorced itself from Damascus and aligned with Syrian Sunni Islamist groups opposing Assad. The exiled political bureau of Hamas moved to Qatar and Egypt (BBC, 2012). However, following the 2013 military overthrow of Egypt's Muslim Brotherhood president, Egypt became a less hospitable base for Hamas. Hamas subsequently repaired its relationship with Iran after it became clear that Assad's regime, supported by Russia and Iran, would survive (Levitt, 2023). Currently, Hamas's political leaders operate out of Doha, frequently appearing on Qatar's state-run satellite network, Al Jazeera, and granting interviews to the Western press (see Said & Kalin, 2024).

Qatar's diplomatic engagement with Hamas aims to bolster its influence within the Palestinian political arena and position itself as a mediator in intra-Palestinian disputes, as well as a regional power broker in Israeli-Palestinian negotiations. Since 2012, following a visit by then-Emir Hamad bin Khalifa to Gaza, Qatar has notably increased its support for Hamas. In its bid to replace Egypt as the primary mediator between Palestinian factions, Qatar provided refuge to Khaled Mashal, who relocated to Doha to manage Hamas's political arm. This support, the largest from any Arab country, has strengthened Hamas's capabilities in Gaza through salary payments and humanitarian projects, often with Israeli approval (Guzansky, 2017; Guzansky & Zalayat, 2023).

Qatar has used its diplomatic influence to give Hamas significant political leverage and international legitimacy. Acting as a mediator in negotiations between Hamas and Israel, Qatar has given Hamas a platform for diplomacy and international recognition. During ceasefire negotiations in 2014 and 2021, Qatar was critical in brokering temporary peace agreements, underscoring its position as a key intermediary in the conflict. Leveraging its membership in international organizations such as the United Nations and the Arab League, Qatar has consistently advocated for Palestinian rights and supported Hamas's political stance (Cafiero, 2023).

Public diplomacy is another tool Qatar employs to support Hamas and promote its narrative globally. Through media outlets like Al Jazeera, Qatar has enhanced Hamas's image and support base by portraying it positively and highlighting its role in the Palestinian resistance. These media campaigns have shaped public perception and increased international support for Hamas.

Regular high-level meetings between Hamas and Qatari officials have facilitated coordination and strategic planning. These meetings, often involving leaders like Ismail Haniyeh, focus on financial support and diplomatic strategies, ensuring that aid and diplomatic efforts align with Hamas's needs. These discussions have underscored the depth of Qatar's involvement in supporting Hamas, both financially and politically. Haniyeh has appeared alongside other Hamas leaders in his office in Doha since 2017 (Daou, 2024).

Conclusions

The evolving international system reveals a complex landscape where non-state actors (NSAs) increasingly challenge state actors across various fields. The strengthening of many NSAs in recent decades underscores their significant role in interstate and intrastate environments. Examples such as the Taliban's resurgence in Afghanistan, Hezbollah's entrenched position in Lebanon, and the economic power of drug cartels in Colombia and Mexico highlight this trend. Hamas, with its coordinated attacks on Israel in October 2023, serves as a pertinent case study of an NSA utilizing foreign diplomatic and financial support to enhance its capabilities.

This article has focused on identifying the key foreign supporters of Hamas from 2006 to October 7, 2023, and examining how these diplomatic and financial activities have contributed to Hamas's operational strength against Israel. Two primary research questions guided this analysis: Q1: How did diplomatic ties and foreign activities help Hamas in its modus operandi and power over Gaza? and Q2: In which way did diplomatic activities and income help Hamas fight Israel?

Through a detailed exploration of antodiplomacy – a concept developed by Plundrich (2024) – this study has highlighted how NSAs like Hamas engage in foreign policy activities similar to states. The research has drawn on a comprehensive dataset, utilizing a qualitative quasi-meta-analysis of ten diverse sources, to uncover the intricate dynamics between Hamas and its key supporters, Iran and Qatar.

The financial and political backing from Iran has been crucial in transforming Hamas into a formidable organization, enhancing its military capabilities and providing substantial financial aid for governance and social services in Gaza. Iranian funding has sustained Hamas over time, building up the group's terrorist capabilities. Iran's terrorist training programs and consistent efforts to arm Hamas are the reasons Hamas has been able to carry out attacks targeting Israel, including the October 7 massacre. For decades, Iran, a US-designated state sponsor of terrorism, has provided a wide range of material support to Hamas, without which Hamas could never have become the capable and deadly terrorist organization it is today. As Jake Sullivan rightly pointed out, "they have provided training, they have

provided capabilities". Tehran played a critical role in creating the monster that is Hamas, which is why Iran shares the blame and responsibility for the brutal attack.

Similarly, Qatar's role as a benefactor and diplomatically has been instrumental in sustaining Gaza's economic stability and bolstering Hamas's governance. Through substantial financial assistance, infrastructure development, and diplomatic engagement, Qatar has reinforced Hamas's position in Gaza and its legitimacy on the international stage.

Foreign diplomatic activities and relationships have been key to Hamas's success. The financial aid and military support from Iran and Qatar have been crucial for Hamas to survive and conduct asymmetric warfare with Israel. Hamas's military capabilities and tactics have steadily advanced from rudimentary *guerilla* and suicide attacks to more sophisticated operations. This support has allowed Hamas to establish a strong political presence in Gaza and build an extensive system of tunnels used for protecting and transporting personnel and weapons, complicating Israeli targeting efforts. Hamas could also be perceived as a proxy ally for several actors against Israel.

The antodiplomacy and analyzed data indicate that foreign support has significantly increased Hamas's capacity to fight against Israel and to carry out attacks, demonstrating the importance of understanding these dynamics. Table 2 summarizes the key findings of this study.

Table 2. Impact of foreign activities between Hamas-Iran and Hamas-Qatar cases

Aspects	Iran-Hamas	Qatar-Hamas
Financial foreign support	Significant financial aid ranging from USD 22 million to USD 100 million annually. Pivotal in funding military operations, salaries, and social services	Pledged over USD 1.4 billion since 2012. Up to USD 360 million annually for infrastructure, salaries, and humanitarian aid
Military-to-military contacts	Supplied weapons, including rockets and missile technology. Provided military training and strategic advice	N/A (Primarily financial and infrastructural support)
Political support and public diplomacy	Regular high-level meetings. Advocated for Hamas in international forums, enhancing political legitimacy and used media to support Hamas's narrative and shape public opinion	Acted as a mediator in ceasefires. Provided a platform through media outlets like Al Jazeera. Enhanced Hamas's image and support base through media campaigns

Source: Author's own study.

In conclusion, the strategic alliances and foreign support from Iran and Qatar have been critical in shaping Hamas's capabilities and influence. This study underscores the importance of understanding the diplomatic and financial networks that empower NSAs, providing insights into the complex interplay of international relations and non-state actors.

References

Abu-Amer, A. (2019, January 14). *The Hamas-Iran alliance remains and expands*. Middle East Monitor. https://www.middleeastmonitor.com/20190114-the-hamas-iran-alliance-remains-and-expands/

Abu-Amr, Z. (1994). *Islamic Fundamentalism in the West Bank and Gaza: Muslim Brotherhood and Islamic Jihad*. Indiana University Press.

Al-Mughrabi, N. (2017, August 28). *After Syria Fall-out, Hamas Ties with Iran Restored: Hamas Chief*. Reuters. https://www.reuters.com/article/us-palestinians-hamasiran-idUSKCN1B81KC

Al-Mughrabi, N. (2023, July 16). *Hamas unable to pay salaries in Gaza after Qatari aid delay, officials say.* Reuters. https://www.reuters.com/world/middle-east/hamas-unable-pay-salaries-gaza-after-qatari-aid-delay-officials-say-2023-07-16/

AP. (2023, January 31). *Qatar pledges $360 million in aid to Hamas-ruled Gaza*. AP NEWS. https://apnews.com/general-news-49a1591f50b183920b5d4310c2098683

Arves, S., Cunningham, K.G., & McCulloch, C. (2019). Rebel tactics and external public opinion. *Research & Politics*, *6*(3), 1–7. https://doi.org/10.1177/2053168019870672

BBC. (2012, February 28). *Hamas political leaders leave Syria for Egypt and Qatar*. BBC News. https://www.bbc.com/news/world-middle-east-17192278

Cafiero, G. (2023). *The future of Hamas in Qatar*. Stimson. https://www.stimson.org/2023/the-future-of-hamas-in-qatar/

Clarke, C.P. (2023, October 27). *Iran and the 'Axis of Resistance' vastly improved Hamas's operational capabilities*. Foreign Policy Research Institute. https://www.fpri.org/article/2023/10/iran-and-the-axis-of-resistance-vastly-improved-hamass-operational-capabilities/

Coggins, B.L. (2015). Rebel diplomacy: Theorizing violent non-state actors' strategies use of talk. In A. Arjona, N. Kasfir, & Z. Mampilly (Eds.), *Rebel Governance in Civil Wars* (pp. 98–117). Cambridge University Press.

Daou, M. (2024, March 18). *Who's who: Top Hamas leaders on Israel's radar*. France 24. https://www.france24.com/en/middle-east/20231103-most-wanted-the-hamas-leaders-on-israel-s-radar

Darwich, M. (2021). Foreign policy analysis and armed non-state actors in world politics: Lessons from the Middle East. *Foreign Policy Analysis*, *17*(4), 1–20. https://doi.org/10.1093/fpa/orab002

Elbagir, N. et al. (2023, December 12). *Qatar sent millions to Gaza for years – with Israel's backing. Here's what we know about the controversial deal*. CNN. https://edition.cnn.com/2023/12/11/middleeast/qatar-hamas-funds-israel-backing-intl/index.html

Guzansky, Y. (2017). *The Gulf states, Israel, and Hamas*. Institute for National Security Studies. https://www.inss.org.il/publication/gulf-states-israel-hamas/

Hinz, F. (2021). *Iran transfers rockets to Palestinian groups*. Wilson Center. https://www.wilsoncenter.org/article/irans-rockets-palestinian-groups

Issacharoff, A. (2016, September 8). *Hamas spends $100 million a year on military infrastructure*. The Times of Israel. https://www.timesofisrael.com/hamas-spends-100-million-a-year-on-military-infrastructure/

Karmon, E. (2009). *Iran and its proxy Hezbollah: Strategic penetration in Latin America*. International Institute for Counter-Terrorism. https://www.ict.org.il/Article.aspx?ID=1060#gsc.tab=0

Katzman, K. (2021, January 11). *Iran's foreign and defense policies*. Congressional Research Service. https://sgp.fas.org/crs/mideast/R44017.pdf

Kaussler, B. (2015). *Tracing Qatar's foreign policy trajectory and its impact on regional security*. Arab Center for Research & Policy Studies. http://www.jstor.org/stable/resrep12689

Levin, D. (2018). *Iran, Hamas and Palestinian Islamic Jihad*. Wilson Center. https://www.wilsoncenter.org/article/iran-hamas-and-palestinian-islamic-jihad

Levitt, M. (2006). *Hamas: Politics, Charity, and Terrorism in the Service of Jihad*. Yale University Press. https://search.ebscohost.com/login.aspx?authtype=shib&custid=s1240919&profile=eds

Levitt, M. (2023, November). *The Hamas-Iran Relationship*. The Jerusalem Strategic Tribune. https://jstribune.com/levitt-the-hamas-iran-relationship/

Martynova, E. (2023, October 19). *How does Hamas spend its nearly half a billion dollar budget?* Insight Threat Intel. https://newsletter.insightthreatintel.com/p/how-does-hamas-spent-its-nearly-half

Muslih, M. (1999). *The Foreign Policy of Hamas*. Council on Foreign Relations.

Nakhoul, S. (2023, October 16). *How Hamas secretly built a 'mini-army' to fight Israel*. Reuters. https://www.reuters.com/world/middle-east/how-hamas-secretly-built-mini--army-fight-israel-2023-10-13/

Neumann, V. (2011, December 3). *The new nexus of narcoterrorism: Hezbollah and Venezuela*. Foreign Policy Research Institute. https://www.fpri.org/article/2011/12/the-new-nexus--of-narcoterrorism-hezbollah-and-venezuela/

Plundrich, M. (2024). Diplomacy of non-state armed actors: A new reality in international relations? *Diplomacy & Statecraft*, *35*(1), 206–223. https://doi.org/10.1080/09592296.2024.2303861

Rudoren, J. (2012, October 23). *Qatar's Emir visits Gaza, pledging $400 million to Hamas.* The New York Times. https://www.nytimes.com/2012/10/24/world/middleeast/pledging-400-million-qatari-emir-makes-historic-visit-to-gaza-strip.html

Said, S., & Kalin, S. (2024, April 20). *Hamas Explores Moving Political Headquarters Out of Qatar*. The Wall Street Journal. https://www.wsj.com/world/middle-east/hamas-explores-moving-political-headquarters-out-of-qatar-8a3a794b

Sayegh, H.A., O'Donnell, J., & Howcroft, E. (2023, October 16). *Who funds Hamas? A global network of crypto, cash and charities.* Reuters. https://www.reuters.com/world/middle-east/hamas-cash-to-crypto-global-finance-maze-israels-sights-2023-10-16/

Seurat, L. (2021). *The Foreign Policy of Hamas*. I.B. Tauris.

Shine, S., & Catran, A. (2017). Iran's policy on the Gaza Strip. Institute for National Security Studies. https://www.inss.org.il/publication/irans-policy-gaza-strip/

Schneckener, U. (2007). Armed non-state actors and the monopoly of force. In A. Bailes, U. Schneckener, & H. Wulf (Eds.), *Revisiting the State Monopoly on the Legitimate Use of Force* (pp. 10–18). Geneva Centre for the Democratic Control of Armed Forces.

Schneckener, U., & Hofmann, C. (2011). Engaging non-state armed actors in state- and peace-building: Options and strategies. *International Review of the Red Cross*, *93*(883), 1–19. https://doi.org/10.1017/S1816383112000262

Skare, E. (2021). *A History of Palestinian Islamic Jihad: Faith, Awareness, and Revolution in the Middle East*. Cambridge University Press.

Skare, E. (2023, December 18). *Iran, Hamas, and Islamic Jihad: A marriage of convenience*. European Council on Foreign Relations. https://ecfr.eu/article/iran-hamas-and-islamic-jihad-a-marriage-of-convenience/#_ftnref5

Staff. (2019, July 20). *Delegation of senior Hamas officials arrives in Tehran*. The Times of Israel. https://www.timesofisrael.com/delegation-of-senior-hamas-officials-arrives-in-tehran/

Szakola, A. (2016, November 24). *Hezbollah and Russia in first direct military meeting: Report.* NOW. http://now.mmedia.me/lb/en/NewsReports/567517-hezbollah-and-russia-in-first-direct-military-meeting-report

Tau, B. (2012, April 4). *Muslim Brotherhood delegation meets with White House officials*. Politico. https://www.politico.com/blogs/politico44/2012/04/muslim-brotherhood-delegation-meets-with-white-house-officials-119647

TOI. (2021, June 22). *US seizes Iranian, pro-Hamas news websites in major crackdown*. The Times of Israel https://www.timesofisrael.com/iran-says-government-news-sites-seized-by-us/

U.S. Department of State. (2013, May 30). *Chapter 6. Foreign terrorist organizations*. https://2009-2017.state.gov/j/ct/rls/crt/2012/209989.htm

Vittori, J. (2011). *Terrorist Financing and Resourcing*. Palgrave Macmillan.

Warrick, J., et al. (2023, October 9). *Hamas received weapons and training from Iran, officials say.* The Washington Post. https://www.washingtonpost.com/national-security/2023/10/09/iran-support-hamas-training-weapons-israel/

Zalayat, I., & Guzansky, Y. (2023). *The Gulf States and the Israel-Hamas War*. Institute for National Security Studies. http://www.jstor.org/stable/resrep54871

Zehorai, I. (2018, January 24). *The richest terror organizations in the world*. Forbes. https://www.forbes.com/sites/forbesinternational/2018/01/24/the-richest-terrororganizations-in-the-world/

AGATA WIKTORIA ZIĘTEK

MARIA CURIE-SKŁODOWSKA UNIVERSITY, LUBLIN

ELIZABETH FREUND LARUS

MARY WASHINGTON UNIVERSITY

Taiwan: One of the Most Dangerous Places in the World

Abstract: The process of securitization in China-Taiwan-U.S. relations has been evident for several years. Speeches and actions by politicians from these three entities have led some analysts to say that Taiwan is the most dangerous place on Earth. The World Economic Forum's (WEF) 2022 Global Risk Report labeled Taiwan as a dangerous place due to PRC activity near its border. The WEF's 2023 Global Risk Report on East and Southeast Asian countries indicates that Taiwan and China are among the world's top-five interstate conflict hotspots. In its 2024 Report, the WEF highlighted three specific hotspots: the war in Ukraine, the Israel-Gaza conflict, and tensions over Taiwan. Why is Taiwan considered one of the most dangerous places on Earth? If so, what predicates this condition? What is Taiwan's future? To better understand the potential for conflict, we need to examine the conditions contributing to tensions in the Taiwan Strait. Specifically, we can distinguish between internal conditions in both Taiwan and China, and third-country activities.

Keywords: Taiwan Strait; China; United States; grey zone tactics

Introduction

On April 12, 2021, twenty-four Chinese military aircraft entered Taiwan's air defense zone in the single largest incursion of Taiwan's defense space. Up to a dozen warplanes, including eight nuclear-capable bombers, had penetrated Taiwan's airspace in previous months, leading *The Economist* on May 1, 2021 to declare on its cover that Taiwan is "the most dangerous place on Earth". In 2024, can Taiwan still be counted among the most dangerous places on Earth? If so, what predicates this condition? Will Taiwan's situation look similarly precarious in the future?

Located 120 kilometers off China's southeastern coast, Taiwan (formally the Republic of China, or ROC) is widely regarded as the most dangerous potential flashpoint with both regional and global consequence. Why is that? For more than seventy years it has been a place of dynamic social, economic, and political change which has tried to maintain an asymmetrical balance with its neighbor to the west, the People's Republic of China (PRC, hereafter "China"). Today, China views this modern society and vibrant democracy of some 24 million people as a breakaway province that must be returned to the mainland as soon as possible. Chinese leader Xi Jinping has said that uniting Taiwan with China is a matter for the Chinese to resolve without interference from a third party. Like his predecessors, Xi has pledged to seek peaceful reunification but has not renounced the use of force to unite Taiwan with China. Xi has publicly stated that he reserves the option of "taking all measures necessary" (White paper: The Taiwan Question and China's Reunification in the New Era, 2022) for unification to happen.

Many analysts share the opinion that there is a high probability of conflict between Taiwan and China. In March 2021, Admiral Phil Davidson, the outgoing commander of the U.S. Indo-Pacific Command (INDOPACOM) forces, told the Senate Foreign Relations Committee that the PRC was likely to attack Taiwan within six years (Davidson, 2021). Others believe 2049 is a critical date as Xi Jinping has emphasized that unification with Taiwan is essential to achieving what he calls the Chinese Dream, which sees China's great-power status restored by that year. In 2023, U.S. Central Intelligence Agency Director William J. Burns said PRC leader Xi Jinping had instructed the PLA to be ready by 2027 to conduct a successful invasion. Burns emphasized that it does not mean that Xi plans to conduct an invasion in 2027 or any other year, but it brings to the forefront the seriousness of Xi's focus and his ambition (Congressional Research Service, 2024). However, Biden Administration officials state that a PRC invasion of Taiwan is "neither imminent nor inevitable".

The process of securitization in China-Taiwan-U.S. relations has been evident for several years. Speeches and actions by politicians from these three entities led the World Economic Forum's 2022 Global Risk Report to label Taiwan as a dangerous place because of PRC activity next to its border (The Global Risk, 17th ed., 2022). The WEF's 2023 Global Risk Report on East and Southeast Asian countries indicates Taiwan and China as one of the world's top-five interstate conflict hotspots (The Global Risk, 18th ed., 2023). In its 2024 Report, the WEF cited three hotspots in particular: the war in Ukraine, the Israel-Gaza conflict, and tensions over Taiwan (The Global Risk, 19th ed., 2024).

To better understand the potential for conflict, we need to examine the conditions contributing to tensions in Taiwan Strait. Specifically, we can distinguish between internal conditions, in both Taiwan and China, and external third-country activity.

Internal conditions

Prestige-symbolic consideration

The first consideration is Beijing's intransigent stance on Taiwan's status and China's determination to unify or annex Taiwan and merge it into the PRC. This stance is conditioned by prestige-symbolic considerations (for Beijing, the "return" of Taiwan to China is a symbolic as well as a prestige issue) and China's military position toward Taiwan.

Two distinct political entities evolved following the ROC's retreat to the island of Taiwan during the Chinese civil war. For many years, the two governments recognized a single Chinese state, but left unsaid if China meant the Republic of China or the People's Republic of China, the issue open to interpretation. In 1992, representatives of the Chinese Communist Party (CCP) and Taiwan's Kuomintang (KMT) party, reached an informal, tacit agreement that both sides adhered to the principle of one China but with different meanings. This so-called 1992 Consensus was achieved during ROC President Lee Teng Hui's administration. In 1999, however, Lee began talking about a "Two States Theory," which defined relations between Taiwan and mainland China as "between two countries" as opposed to the previous view of between two equal political entities. This move drastically cooled cross-Strait relations. Relations further cooled in June 1995 after Lee offered a political speech at Cornell University during what was supposed to be a private visit to his alma mater. In response, The China's People's Liberation Army (PLA) launched a missile weapons test near Taiwan, further demonstrating China's threat to Taiwan's security. In March 1996, China conducted missile tests in the waters surrounding Taiwan in an attempt to dissuade Taiwan voters from reelecting Lee in that year's ROC presidential election (Gacek & Trojnar, 2023; Larus & Ziętek, 2021). After his election to the presidency in 2000, Taiwan independence advocate Chen Shui-bian (2000–2008) touted "Two Different Countries separated by the Taiwan Strait". After his 2008 election, Ma Ying-jeou (2008–2016), returned to the spirit of the 1992 Consensus. He favored cooperation with China and maintaining the *status quo*. He referred to a "Three No" formula of no unification, no independence, no use of force (Gacek & Trojnar, 2023). Since Tsai Ing-wen's election to the presidency in 2016, official dialogue in the Taiwan Strait has been suspended. The primary reason for the suspension is Tsai's refusal to support the 1992 Consensus, which she associated with "one country, two systems". In her 2016 inaugural address, Tsai noted she was "elected president in accordance with the Constitution of the Republic of China," and said that she would "safeguard the sovereignty and territory of the Republic of China" (Office of the President Republic of China (Taiwan), 2016).

Beijing rejected this formulation and cut off official contacts with Taiwan. At that same time China started to use "gray zone" tactics, including cyber-attacks, selective

trade embargoes, military incursions into Taiwanese airspace, naval exercises in the waters around the island. As a result, a "new normal" is evolving in the Taiwan Strait, in which the PLA Air Force (PLAAF) regularly sends large contingents of fighters, strategic bombers and air reconnaissance aircraft crossing the centerline of Taiwan's Air Defense Identification Zone (ADIZ), which raises the possibility of actual hostilities (Heath et al., 2023). Western defense analysts have pointed out the "normalization" of PLA operations ever closer to Taiwan's islands in peacetime could undermine Taipei's ability to assess whether the PLA is using "routine" operations or exercises to obscure preparations for an attack (Congressional Research Service, 2024).

These moves are consistent with declarations by China's leadership to realize the country's revitalization as a great power by midcentury, thereby realizing Xi Jinping's China Dream (Góralczyk, 2021). From China's perspective, Taiwan among its core interests, which the Chinese Communist Party (CCP) considers essential to the country's survival and development. The PRC government historic mission is to protect its core interests. Tsai's insistence that Beijing treat Taiwan as an equal as a precondition for talks with China was an obstacle to cross-Strait talks and further exacerbated tension between Taiwan and China. Tsai's successor, Lai Ching-te, in his 2024 presidential election victory speech called for reopening dialogue with China to "replace confrontation" and pledged to maintain the "cross-strait *status quo*" (The Straits Times, 2024). Although Lai signaled broad continuity with his predecessor Tsai and committed to maintain the *status quo* in cross-Strait relations, he departed from Tsaiby not explicitly pledging to conduct cross-strait relations in accordance with the Republic of China Constitution, which embodies a one-China framework (Council on Foreign Relations, 2024).

Military consideration

Facing an existential threat from across the Strait, Taiwan has made efforts to modernize its military. Three key areas of military modernization are reform of the armed forces, robust foreign arms acquisitions, and strengthened development of indigenous defense systems and platforms.

In the 1990s, Taiwan's arms expenditures ranked fourth in East Asia behind Japan, China, and the Republic of Korea (ROK) and peaked at USD 14 billion in 1992. When we look at the military expenditure in East Asian countries as percentage of GDP in 1988, we see that Taiwan spent 5.1% of its GDP on defense, while Japan spent only 0.9% and South Korea 4.3%. By 2010, however, Taiwan's defense outlays had decreased to only 2.0% of GDP, while Japan spent 1.0%, ROK 2.5% and China 1.9% of GDP, each having much larger economies than Taiwan. In 2019, Taiwan's defense spending as percentage of GPD had fallen to 1.7%. Although Japan spent only 0.9%, South Korea spent 2.7% and China 1.9% of their respective GDP's on defense in 2019

(Stockholm International Peace Research Institute, 2021). Taiwan's military spending in actual dollars was far below its and China's current military spending is nearly equal to that of the United States. The US intelligence community estimates that, when accounting for economic differences and hidden expenditures, China spends some USD 700 billion to the US's USD 742 billion (Mackenzie, 2024). According to SIPRI, China's 2023 military spending was an estimated USD 296 billion, much smaller than the US's USD 916 billion for that year (SIPRI Fact Sheet, 2024). Lack of transparency makes estimating difficult. Estimates aside, China's military budget is clearly 15 to 37 times greater than Taiwan's. Consequently, China's growing military power is changing the balance of power in the Western Pacific in its favor is creating a security dilemma in relations between China, the U.S., and Taiwan. China's behavior is the main driver of spending trends in the Indo-Pacific region since many of its neighbors including Taiwan perceive China's growing military power as a reason to enhance their own military capabilities. PRC aggressive posture toward Taiwan could provoke the island to react with counterbalancing behavior and resistance.

Patterns in Taiwan and Chinese public opinions

The second factor shaping tensions in the Taiwan Strait is public opinion. People in Taiwan do not want to unify with China or be annexed by it. According to a 2021 survey, 57.6% of respondents said they worry that war is a distinct possibility (Brookings, 2021). Since 1994, National Cheng-chi University's Election Study Center has tracked annual changes in Taiwan residents' stance on the unification or independence issue. In a 2023 survey titled "Changes in the Unification-Independence Stances of Taiwanese," increasing support for the continuation of cross-strait *status quo* was observed (Election Study Center, National Chengchi University, 2024). Only 1.2% of respondents prefer unification with the PRC as soon as possible. A mere 5% prefer to keep the *status quo* and move toward unification compared to over 32% who would like to keep the *status quo* indefinitely, 21.5% maintain the *status quo* and move toward independence and 27.9% keep the *status quo* and decide later. Since 1995, a growing number of people who seriously think about independence, up from 8% in 1995 to 21.5% in 2023. This tendency is not in China's favor. Surveys show that 61.7% of Taiwanese in 2023 identified themselves as Taiwanese. That self-identification preference has grown from 17.6% in 1992 to more than threefold in 2023. Such results could legitimize the government's moves in Taiwan toward independence. It is still an open question whether the Taiwanese are prepared to resist militarily under attack from China? Previous surveys of Taiwanese people's readiness to fight China have shown widely varying results, with as little as 15% of respondents indicating willingness to fight (from the 2017 Taiwan National Security Study survey) to nearly 80% indicating willingness

(from the 2020 Taiwan Foundation for Democracy survey). Although differences may be due to the adopted methodology, an important factor influencing greater mobilization for defense is the belief that Taiwan can count on support from other countries, mainly the United States (Taiwan Politics, 2023).

What is the attitude of the continent's population toward war? A study released in 2023 by the 21st Century China Center at the University of California at San Diego indicates that many Chinese citizens oppose a war over Taiwan. The survey analyzed the Chinese public's support for various policy steps aimed at reunification with Taiwan. It found that a third of Chinese respondents found it unacceptable to start a war to achieve reunification. The findings challenge the widespread belief that reclaiming Taiwan is the collective will of almost all Chinese residents (Liu & Li, 2023).

Economy

The third factor is Taiwan's economic reliance on trade with China, which is the island's largest trading partner. Under Ma Ying-jeou, Taiwan signed more than twenty agreements with the PRC. Tsai and the DPP, on the other hand, diversified Taiwan's trade relationships, mostly with countries in Southeast Asia and the Indo-Pacific through the New Southbound Policy. For decades, China has attempted to isolate Taiwan internationally. For instance, Beijing has pressed countries not to sign free trade agreements with Taiwan. Consequently, only a few countries have signed free trade pacts with the island, e.g. New Zealand and Singapore. Beijing has also pressed for Taiwan's exclusion from multilateral trade blocs, including the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) and the Regional Comprehensive Economic Partnership (RCEP). Taiwan also is not part of the Biden administration's Indo-Pacific Economic Framework (Maizland, 2024). According to official reports, Taiwan's exports to China and Hong Kong last year dropped 18.1% compared to 2022, the biggest decrease since they started recording this set of statistics in 1982. In contrast, Taiwanese exports to the U.S. and Europe rose by 1.6% and 2.9%, respectively, with the trade volumes reaching all-time highs (Politico, 2024). Nevertheless, China continues to be Taiwan's biggest trading partner, with many Taiwanese businesspeople living and working in the mainland. Taiwan is aware that its economic ties with the mainland are based on a delicate balance. On the one hand, it is profitable and beneficial, on the other hand they are aware of China's growing competitiveness including technological process. Nowhere was this tension more evident than in semiconductors. Taiwan's critical role in global supply chains – above all semiconductor production – acts as a brake to hostilities but probably does not diminish completely China's desire to gain control over Taiwan and its technology. According to the Independent Task Force Report, conflict between Taiwan and China would trigger a global economic depression

(Gordon et al., 2023). It could cost around USD 10 trillion, equal to about 10% of global GDP (Bloomberg, 2024). Despite this cost, China and Taiwan are still strongly linked economically. Taiwan must face the reality that its most important supply chains run through China, and cross-Strait trade remains the main driver of Taiwan's economic growth (Mark & Graham, 2023).

External conditions

The fourth factor is conditions external to Taiwan. External conditions include the international situation, including conflicts in Ukraine and Gaza, US-China competition for primacy in the Indo-Pacific, and the strength of the US abroad.

Russia's invasion of Ukraine in early 2022 has sparked debate over Taiwan's future. Some analysts have followed the logic of "today Ukraine tomorrow Taiwan", believing that Moscow's moves could embolden Beijing to launch a similar invasion of Taiwan. Such thinking was justified by the tense situation in China-Taiwan relations. Not insignificant was the strengthening of cooperation between China and Russia on the eve of Russia's invasion of Ukraine. In February 2022, Xi and Russian leader Vladimir Putin signed a "no limits" partnership, which one US senior official described as the "coming out party" for their growing allegiance. Others argue that Beijing may become more cautious after learning of Russia's challenges. Council on Foreign Relations (CFR) Fellow David Sacks wrote that Russia's actions will not affect China's willingness to use force, but "Chinese leaders will analyze Russia's failures and adjust their operational plans to avoid making similar mistakes" (Gordon et al., 2023).

The most crucial factors are US relations with China and Taiwan. The normalization of relations between US and China started in 1972 under Richard Nixon's presidency with the 1972 Shanghai Communiqué. This document included Chinese and U.S. statements on Taiwan. It was a broad agreement indicating that relations should be conducted under the principle of "equality and mutual benefit, and peaceful coexistence", with both sides agreeing to respect "national sovereignty and territorial integrity" (Joint Communique of the United States of America and the People's Republic of China (Shanghai Communique), 1972). On the matter of Taiwan, China reaffirmed its position that Taiwan is a part of the PRC, and that the Chinese government opposes any activities which aim at the creation of "one China, one Taiwan", "one China, two governments", "two Chinas", and "independent Taiwan" or advocate that "the status of Taiwan remains to be determined" (Trojnar, 2019). The U.S and China are still following different but carefully crafted lines. In the 1972 Shanghai Communiqué and the 1979 Normalization Agreement between the U.S. and China, both countries agree that Taiwan is part of China. However, the U.S. and China hold different views on how the Taiwan issue should be resolved. China insists that it is an internal matter of China that does not tolerate foreign

interference; the U.S. position is to assert its interests in a peaceful resolution of the Taiwan issue by the Chinese themselves.

The U.S. government officially recognized the PRC in 1979 but has maintained unofficial relations with Taiwan based on the Taiwan Relations Act (TRA). The 1979 TRA legally requires the United States to sell military arms to Taiwan to help Taiwan defend itself. The TRA was followed in 1982 with "Six Assurances" to Taiwan, which stipulate that the United States would not set a date for termination of arms sales to Taiwan; would not alter the terms of the Taiwan Relations Act; and would not consult with China in advance before making decisions about U.S. arms sales to Taiwan (Taiwan Documents Project, 2024). The terms of the assurances indicate that U.S. willingness to reduce arms sales to Taiwan is contingent on the continued commitment of the PRC to a peaceful solution of cross-Strait differences. Conversely, if the PRC were to become hostile, the United States would increase arms sales to Taiwan (Larus & Ziętek, 2021). The ambiguity in the US commitment to Taiwan's national security paved, at that time, the way to the ROC Army's isolation and finally its self-expansion, with limited procurement from the United States (Trojnar, 2019).

Since 1950, the United States has been Taiwan's most significant security guarantor. At the outbreak of the Korean War in 1950, U.S. President Truman sent the Seventh Fleet to the Taiwan Strait to prevent China from attacking Taiwan and stationed troops on the island as guarantee of the security. This event was called the First Island Crisis. Following China's 1954 bombing of the ROC's outlying islands of Kinmen and Matsu (the Second Island Crisis), the United States and the ROC signed a mutual defense treaty. The United States abrogated its defense treaty with Taiwan after it severed relations with Taiwan in 1979. In July 1995, the PRC conducted missile tests in demonstration against then-President Lee Teng-hui's political speech at Cornell University. Chinese actions strengthened the argument for further U.S. arms sales to the ROC. In 1999, the U.S. Congress passed the Taiwan Security Enhancement Act (TSEA), which allowed direct secure communications between the U.S. and Taiwan and allowed more Taiwan military officers to train at U.S. military schools, and also led to the strengthening of military ties between the United States and Japan.

Despite these factors, an important consideration in Taiwan's security calculus is the U.S. policy of strategic ambiguity. Under this policy of mutual deterrence, Washington assumes neutrality in a cross-Strait conflict, thereby leaving Beijing guessing if the United States will defend Taiwan in a cross-Strait conflict, but also rendering Taipei uncertain that the United States will come to Taiwan's aid if it provokes Beijing by declaring independence. The purpose of the policy is to encourage restraint on both sides of the Taiwan Strait.

U.S.-China relations deteriorated during the presidency of Donald Trump. The Trump administration carried out a bruising trade with China, whom Trump labelled a "strategic competitor". He also appeared to use Taiwan as a point of tension with

Beijing by making large arms sales to the island and supporting the exchange of visits of high-level US and Taiwan officials. Trump spoke with President Tsai by telephone ahead of his inauguration, the highest level of contact between the two sides since 1979. During his presidency, the State Department eliminated long-held restrictions governing where and how U.S. officials can meet with their Taiwanese counterparts. The Joe Biden administration appears no more enamored of China. His administration has continued arms sales to Taiwan and has allowed U.S. officials to meet with Taiwanese officials (U.S. Department of State, 2021). Biden even started to invite Taiwanese representatives to attend the presidential inauguration (Council of Foreign Relations, 2021). The United States participates in military training and dialogues with Taiwan, regularly sails ships through the Taiwan Strait to demonstrate its military presence. In August 2022, former House Speaker Nancy Pelosi visited Taiwan; she was the first Speaker to do so since 1997. She also met with President Tsai, eliciting a strong Chinese military response. Following the 2024 Taiwan presidential election, the U.S. sent an official delegation to Taiwan to congratulate President-elect Lai Ching-te and Tsai Ing-wen for the DPP's win and to celebrate the preservation of Taiwan's democracy (Al Jazeera, 2024).

Following the relaxation of COVID-19 restrictions, Biden and Xi met in November 2023 in San Francisco. It was first Xi's visit to the US since 2017. A Chinese communiqué following the summit called on the U.S. to take concrete steps to honor its commitment not to support an independent Taiwan, stop arming Taiwan and promote peaceful reunification. On the other hand, the U.S. press release reiterated that the U.S. has not changed its one-China policy, that it opposes any unilateral changes to the *status quo*, and that it expects both sides of the Taiwan Strait to resolve their differences peacefully (Przychodniak & Wnukowski, 2023).

Future scenarios

The Taiwan Strait remains one of the most sensitive and potentially volatile regions in the world. The outcome will be influenced by Taiwan and China's domestic politics, international relations, especially the U.S.-China relationship, and broader geopolitical trends in the region and globally. The situation in the Taiwan Strait is an issue that could potentially evolve from rivalry to direct confrontation. For many years, cross-Strait stability has allowed Taiwan to thrive and its people to build a democratic, pluralistic, and economically vibrant society. Today, China's increasingly assertive posture is more than verbal evidence that Taiwan must be prepared for different scenarios, just like its allies.

U.S. foreign policy scholars Robert D. Blackwill and Philip Zelikow in a 2021 CFR report proposed three scenarios concerning future situation in Taiwan Strait: China invades Taiwan's periphery, China quarantines Taiwan, and China invades Taiwan.

China is already invading Taiwan's periphery by implementing "gray zone" tactics (Blackwill & Zelikow, 2021). China's military aircraft regularly fly into Taiwan's ADIZ, organize cyber-attacks, impose selective trade embargoes, organize naval exercises in the waters around the island. Blackwill and Zelikow claim that China also could decide to more tangibly demonstrate its power by invading one or another offshore island controlled by Taiwan. The next possible scenario is quarantine, in which China takes control of Taiwan's air and sea borders. That is easy to implement even now after the Chinese government's National People's Congress passed in 2021 a new law, which expressly authorized coast guard ships to use "all necessary means" against foreign vessels, and to board and inspect such vessels in waters claimed by China. The bill empowered the China Coast Guard (CGG) to create temporary exclusion zones "as needed" to keep other vessels from entering (Standing Committee of the National People's Congress, 2021). The last proposed is invasion scenario. This could be implemented in one of two ways: more traditional siege and amphibious assault, aided by an armada of ships and landings at some of a dozen or so beach areas on the northern and western sides of Taiwan or invasion would rely much more on airborne/heliborne assault and special operations (Blackwill & Zelikow, 2021). In 2023, the Center for Strategic and International Studies (CSIS) developed a war game for a Chinese amphibious invasion of Taiwan and ran it 24 times. In most scenarios, the United States, Taiwan, and Japan in concert defeated a conventional amphibious invasion by China and maintained an autonomous Taiwan. However, this defense came at high cost for everyone. For the U.S. and Japan invasion will bring loss of life tens of thousands of service members and equipment. An invasion by China would devastate Taiwan's economy. China would suffer huge casualties, devastate its economy, and likely destabilize CCP rule (Cancian et al., 2023).

The future scenarios in the Taiwan Strait are complex and influenced by a range of political, economic, military, and social factors. Considering the above, the following potential scenarios can be proposed. The first on is *status quo* continuation. Such a scenario is in Taiwan's favor. As indicated above, most people on Taiwan prefer to maintain the *status quo* of neither unification nor independence. Taiwan would continue to exist as a *de facto* state, without formal independence with continued U.S. political and military support. Taiwan's economy would grow and maintain supremacy in semiconductor manufacturing and distribution. There would be periodic tensions and military posturing without escalation into full-scale conflict. However, Taiwan's *de facto* independent status could be threatened if Taiwan increased economic dependence on China, which might bring Taiwan more firmly into China's sphere of influence. Such a scenario also creates opportunities for further diplomatic efforts to manage the relationship, however. The second scenario is peaceful reunification, in which Taiwan and China come to a peaceful agreement on reunification. It could happen if China offers more attractive terms of unification, or

maybe after international mediation. This scenario shifts in regional power dynamics but it is difficult to imagine in current circumstances. The third scenario is Taiwan independence declaration. This could be the consequence of growing stronger Taiwanese identity and public support for pro-independence parties. But it is also based on the belief that international support, particularly from the U.S., would be sufficient to deter Chinese retaliation. In this scenario, we could expect a high risk of military conflict between Taiwan and China with potential involvement of the U.S. and other allies as well as economic sanctions and international diplomatic fallout. Another possibility is Chinese military action scenarios, including, in which China uses military force to attempt to bring Taiwan under its control. China might take such measures if Taiwan declares independence, which China sees as a threat to its sovereignty and integrity. Outward aggression could also be a consequence of increasing domestic pressure within China, such as due to the economic situation or a miscalculation of the international response. Consequence would be a large-scale conflict with significant casualties and destruction and long-term regional instability and economic disruption. If not kinetic military conflict, we can also consider scenarios of technological and asymmetric warfare as a consequence of cyber warfare use, economic disruption or other non-traditional means of conflict. To avoid a direct military confrontation, the two sides might try to implement asymmetric strategies, disrupting global supply chains (especially in the semiconductors sector) and creating cybersecurity threats. This new type of conflict could have unpredictable consequences. Another scenario is increased economic and diplomatic pressure. In this scenario, China increasingly uses non-military pressure, economic leverage, diplomatic isolation, and coercive tactics short of military action to force Taiwan to make political concessions. This could result in economic hardship for Taiwan, political unrest on Taiwan, but might draw international efforts to offset Chinese influence. A final scenario involves mediation and conflict resolution by international actors to solve or manage Taiwan Strait tensions. It could be conditioned by Taiwan's position in semiconductor technology and production. Many states are interesting to keep the *status quo* and stability in Taiwan Strait also because of global supply chain in semiconductors production, industry that relies on the cooperation of many players. For instance, world leading semiconductor foundry Taiwan Semiconductor Manufacturing Company (TSMC) is reliant on the Netherlands's ASML, whose lithography technology is fundamental to mass producing semiconductor chips, German optics and innumerable components from other countries. Protecting the semiconductor supply chain increases global focus on preventing conflict in Taiwan Strait, involving diplomatic initiatives from major powers, multilateral organizations, and international concerns. Any negotiated settlement would likely involve compromises from both China and Taiwan. It will bring stabilization of the region but also potential dissatisfaction within Taiwan and China.

These seven scenarios can be grouped according to two criteria: the consequences of the situation in the Taiwan Strait as either positive or negative and the probability of occurrence as either high or low (see Figure 1).

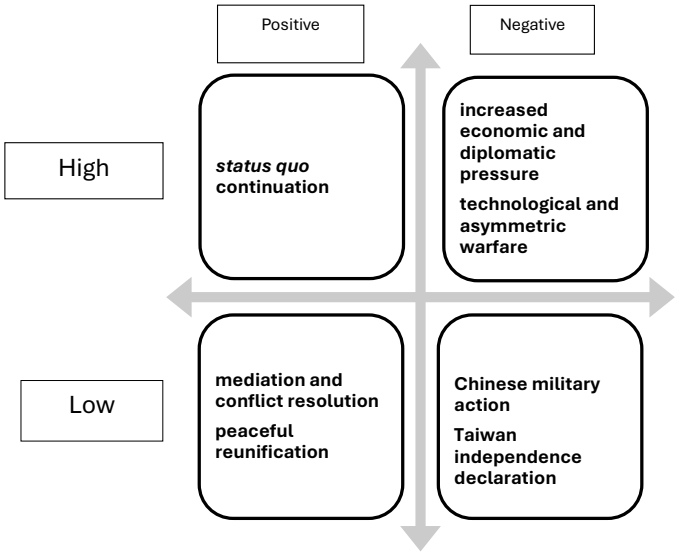

Figure 1. Scenario matrix

Source: Authors' own study.

Conclusions

The Taiwan Strait remains one of the most sensitive and potentially volatile regions in the world. The outcome will be influenced by internal politics within Taiwan and China, international relations, particularly with the U.S., and broader geopolitical trends. Each scenario presents significant risks and requires careful management to avoid escalation into open conflict.

References

Al Jazeera. (2024, January 15). Taiwan's Tsai and Lai welcome US support as Beijing fumes over election. https://www.aljazeera.com/news/2024/1/15/taiwans-tsai-and-lai-welcome-us-support-as-beijing-fumes-over-election

Blackwill, R.D., & Zelikow, P. (2021). The United States, China, and Taiwan: A strategy to prevent war. *Council Special Report*, *90*.

Bloomberg. (2024, January 9). *Xi, Biden and the $10 trillion cost of war over Taiwan*. https://www.bloomberg.com/news/features/2024-01-09/if-china-invades-taiwan-it-would-cost-world-economy-10-trillion?embedded-checkout=true

Brookings. (2021, October 13). *How are people feeling in the "most dangerous place on Earth"?* https://www.brookings.edu/articles/how-are-people-feeling-in-the-most-dangerous-place-on-earth/

Cancian, M.F., Cancian, M., & Heginbotham, E. (2023). *The First Battle of the Next War: Wargaming a Chinese Invasion of Taiwan*. CSIS.

Congressional Research Service. (2024, Agust 15). *Taiwan: Defence and military issues*. https://crsreports.congress.gov/product/pdf/IF/IF12481

Council on Foreign Relations. (2021, January 28). *Biden administration sends important signals for the future U.S.-Taiwan ties*. https://www.cfr.org/blog/biden-administration-sends-important-signals-future-us-taiwan-ties

Council on Foreign Realtions. (2024, May 21). *Analyzing Lai Ching-te's inaugural addess: More continuity than difference*. https://www.cfr.org/blog/analyzing-lai-ching-tes-inaugural-address-more-continuity-difference

Davidson, A.P. (2021, March 09). https://www.armed-services.senate.gov/imo/media/doc/Davidson_03-09-21.pdf

Election Study Center, National Chengchi University. (2024, July 8). https://esc.nccu.edu.tw/PageDoc/Detail?fid=7801&id=6963

Gacek, Ł., & Trojnar, E. (2013). *Pokojowe negocjacje czy twarda gra? Rozwój stosunków ponad Cieśniną Tajwańską*. Księgarnia Akademicka.

Gordon, S.M., Mullen, M.G., & Sacks, D. (2023). U.S.-Taiwan relations in a new era responding to a more assertive China. *Council on Foreign Relations, Task Force Report*, *18*.

Góralczyk, B. (2021). *Nowy długi marsz. Chiny ery Xi Jinpinga.* Dialog.

Heath, T.R., Robinson, E., Curriden, C., Grossman, D., Lilly, S., Egel, D., & Tarini, G. (2023). *Disrupting the Chinese Military in Competition and Low-Intensity Conflict.* https://www.rand.org/content/dam/rand/pubs/research_reports/RRA1700/RRA1794-2/RAND_RRA1794-2.pdf

Joint Communique of the United States of America and the People's Republic of China (Shanghai Communique). (1972, February 28). http://www.china.org.cn/english/china-us/26012.htm

Larus, E., & Ziętek, A. (2021). Taiwan's military posture toward China's confronational stance. In C.M. Clark, K. Ho, & A.C. Tan, *Taiwan Environmental, Political and Social Issues.* Nova Science Publisher.

Liu, A., & Li, X. (2023). Assessing public support for (non-)peaceful unification with Taiwan: Evidence from a nationwide survey in China. *21st Century China Center Research Paper*, *2023-1*.

Mackenzie, E. (2024). *Keeping Up with the Pacing Threat: Unveiling the True Size of Beijing's Military Spending*. https://www.aei.org/wp-content/uploads/2024/04/Keeping-Up-with-the-Pacing-Threat-Unveiling-the-True-Size-of-Beijings-Military-Spending.pdf

Maizland, L. (2024, February 8). *Why China-Taiwan relations are so tense*. Council on Foreign Relations. https://www.cfr.org/backgrounder/china-taiwan-relations-tension-us-policy-biden#chapter-title-0-9

Mark, J., & Graham, N. (2023). *Relying on Old Enemies: The Challenge of Taiwan's Economic Ties to China. Atlantic* Council.

Office of the President Republic of China (Taiwan). (2016). https://english.president.gov.tw/News/4893

Politico. (2024, Januray 13). *Taiwan's new pesident: 5 things you need to know about William Lai*. https://www.politico.eu/article/five-things-you-need-to-know-about-taiwan-new-president-william-lai-elections-dpp/

Przychodniak, M., & Wnukowski, D. (2023, November 20). *Spotkanie Xi-Biden w Kalifornii – postęp bez przełomu*. PISM. https://www.pism.pl/publikacje/spotkanie-xi-biden-w-kalifornii-postep-bez-przelomu

SIPRI Fact Sheet. (2024, April). https://www.sipri.org/sites/default/files/2024-04/2404_fs_milex_2023.pdf

Stockholm International Peace Research Institute. (2021, April). *Trends in world military expenditure, 2020*. https://www.sipri.org/publications/2021/sipri-fact-sheets/trends-world-military-expenditure-2020

Taiwan Documents Project. (2024). http://www.taiwandocuments.org/assurances.htm

Taiwan Politics. (2023, November 17). *Public support for self-defence in Taiwan. The current state of research*. https://taiwanpolitics.org/article/90278-public-support-for-self-defence-in-taiwan-the-current-state-of-research

The Global Risks, 17th Edition. (2022). https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf

The Global Risk Report, 18th Edition. (2023). https://www3.weforum.org/docs/WEF_Global_Risks_Report_2023.pdf

The Global Risk Report, 19th Edition. (2024). https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2024.pdf

The Straits Times. (2024, January 14). *Taiwan president-elect Lai Ching-te calls for dialogue with China to 'replace confrontation'*. https://www.straitstimes.com/asia/east-asia/taiwan-president-elect-lai-ching-te-calls-for-dialogue-with-china-to-replace-confrontation

Trojnar, E. (2019). Taiwan-China-United States relations: Taiwan's unique safe House for better or worse. In A. Rudakowska, E. Trojnar, & A. Ziętek (Eds.), *Taiwan's Exceptionalis* (p. 58). Jagiellonian University Press.

U.S. Department of State. (2021, April 9). *New guidelines for U.S. government interactions with Taiwan counterparts*. https://www.state.gov/new-guidelines-for-u-s-government-interactions-with-taiwan-counterparts/

White paper: The Taiwan Question and China's Reunification in the New Era. (2022, August 10). *Xinhua.* https://english.news.cn/20220810/df9d3b8702154b34bbf1d451b99bf64a/c.html

SARAH CERNIKOVA

UNIVERSITY OF WEST BOHEMIA IN PILSEN

Drugs and Organized Crime as a Non-Traditional Threat to National Security

Abstract: The chapter examines the intricate relationship between drugs, organized crime, and national security, emphasizing their intertwined impact on societal and geopolitical stability. Focusing on the Czech Republic and the United States, it explores how these countries are affected by and respond to drug trafficking, particularly methamphetamine in the Czech Republic and synthetic drugs like fentanyl in the U.S. The chapter discusses the operational dynamics of drug trafficking networks, the challenges in law enforcement, and the significant threat these activities pose to national security. Additionally, it highlights the importance of international cooperation in combating drug trafficking, addressing both the supply and demand sides of the drug crisis, and underscores the need for comprehensive strategies that include prevention, education, and rehabilitation. The analysis also considers the broader implications for national sovereignty, public trust in governmental institutions, and environmental impacts, making the case for a multifaceted approach to mitigating the threats posed by drugs and organized crime.

Keywords: drugs; organized crime; Czech Republic; national security

Drugs present a multifaceted issue, posing significant threats to human health, contributing to petty crimes and offenses, and ultimately jeopardizing national security. The proliferation and consumption of illicit drugs have far-reaching implications that extend beyond the immediate health effects on individuals to encompass a broader spectrum of societal and geopolitical consequences. This chapter aims to highlight the critical connection between drugs, organized crime, and national security, emphasizing the complex and intertwined nature of these elements.

Certain European states, such as the Czech Republic, the Netherlands, and Belgium face severe challenges related to drugs and their transit across these countries. These states, owing to their strategic locations within Europe, are prime candidates for establishing extensive drug distribution networks. Additionally, they are among the highest consumers of addictive substances in Europe, which further complicates the

issue. The Czech Republic, in particular, plays a pivotal role in the production and distribution of methamphetamine, earning its reputation as a central hub for this illicit activity (European Monitoring Centre for Drugs and Drug Addiction, 2019). The country's well-developed infrastructure and relatively porous borders make it an attractive site for traffickers looking to move their products across Europe.

Given the substantial threat that drug trafficking poses to national security in the Czech Republic, this chapter will provide an in-depth examination of the country's drug trafficking networks. It will analyze the structural and operational dynamics of these networks, shedding light on the methods used to produce, transport, and distribute methamphetamine. Furthermore, the chapter will assess the efficacy of law enforcement efforts in combating methamphetamine production, exploring the strategies and tactics employed by the Czech police and other relevant agencies. This examination will also consider the legal and policy frameworks in place and their effectiveness in addressing the drug problem.

It is important to note that Europe is not the only continent grappling with drug addiction and production, both of which exacerbate security challenges. This chapter will also consider the case of the United States, where synthetic drugs pose a significant issue that requires urgent attention from American authorities. The severity of the problem is underscored by statements from officials within the Drug Enforcement Administration (DEA), highlighting the growing concern over synthetic drugs. The deteriorating situation has prompted the implementation of new measures aimed at reducing the availability of these illegal substances. These measures are expected to lower the death rate and crime levels that have surged in recent years due to drug-related activities.

According to a 2023 analysis by the Department of Homeland Security, drug trafficking and usage are projected to be among the top threats to national security in the United States in 2024 (U.S. Department of Homeland Security, 2023). This projection underscores the gravity of the issue and the need for a comprehensive approach to tackling it. The chapter will delve into the specific challenges faced by the United States, including the routes and methods used for smuggling synthetic drugs, the impact on public health and safety, and the broader implications for national security.

This chapter will also explore the essential role of international cooperation in combating drug trafficking, recognizing it as a crucial component in addressing this pervasive global issue. Effective international collaboration involves the sharing of intelligence, joint operations, and the harmonization of legal frameworks to ensure that traffickers cannot exploit legal and regulatory discrepancies between countries. The chapter will examine existing international agreements and initiatives aimed at curbing drug trafficking and assess their success. It will also consider the potential for new forms of cooperation, particularly in light of evolving drug production techniques and trafficking methods.

In conclusion, the chapter will underscore the importance of a multi-faceted approach to addressing the drug problem, one that combines robust national policies with effective international cooperation. By examining the cases of Europe and the United States, it will provide a comprehensive overview of the challenges and opportunities in the fight against drug trafficking and its associated security threats. This perspective is essential for developing strategies that can effectively mitigate the impact of drugs on health, crime, and national security.

Drugs as a threat to national security

Drugs and drug trafficking represent significant global problems, but why should they be considered threats to national security? The issue extends beyond the economic and social consequences associated with drug use, which this chapter will also address. There are additional, severe concerns such as the utilization of traditional drug distribution routes for the smuggling of arms, explosives, and terrorists into various states. These routes are particularly advantageous for nefarious purposes because organized groups involved in drug trafficking ensure that these pathways remain outside the control of state security forces, making them highly attractive for other illicit activities. Several incidents underscore these concerns. For instance, the 1993 Mumbai bombings and the 2015 Pathankot attack in India saw terrorists exploiting established drug trafficking routes to transport explosives and personnel (Das, 2019, pp. 2–4).

The financial aspect of drugs and national security is also critical and multifaceted. There is a notable trend of terrorist groups using proceeds from drug trafficking to fund their activities against state structures. For instance, the Taliban financed their insurgency through profits from the opioid trade, illustrating how drug trafficking can sustain prolonged conflicts. Developing countries, in particular, face severe challenges where the power and financial resources of organized and terrorist groups, bolstered by drug trafficking, are substantial. These groups often attempt to infiltrate and dominate state structures, posing a significant threat to national sovereignty and stability. The extensive financial resources generated through drug trafficking can also be used to corrupt officials, further weakening the state's ability to enforce laws and maintain order.

Furthermore, the societal and economic impacts of drug addiction are well-documented. These issues, while more directly related to individuals with addiction rather than drug trafficking itself, result in a broad spectrum of illegal activities that can lead to social destabilization, widespread fear, and significant changes in societal behavior. The burden on social systems, which are aimed at prevention and support, and healthcare systems, strained by the health impacts of drug use, is considerable. The economic toll includes increased healthcare costs, loss of

productivity, and significant law enforcement expenses. These economic and social impacts can permeate state structures, influencing and potentially altering state policies and priorities.

In addition, the prevalence of drug trafficking and drug use can erode public trust in governmental institutions. As organized crime groups often operate with impunity, citizens may begin to lose confidence in their government's ability to protect and serve them effectively. This erosion of trust can lead to further societal destabilization, as people might turn to alternative, sometimes radical, sources of authority and support.

The Czech Republic – the methamphetamine empire

The case of the Czech Republic is particularly noteworthy, as it ranks first in the distribution and consumption of methamphetamine within the European Union, according to the European Monitoring Center for Drugs and Drug Addiction (EMCDDA). This esteemed institution provides comprehensive and reliable data on drug use and distribution across Europe. An analysis from 2021 indicates that the Czech Republic leads in methamphetamine use, with approximately five individuals per thousand consuming the drug (European Monitoring Center for Drugs and Drug Addiction, 2021). This statistic underscores the prevalence of methamphetamine consumption within the country, highlighting a significant public health crisis that necessitates comprehensive intervention strategies.

While consumption poses a significant issue, production presents an even greater challenge. The Czech Republic is frequently labeled an "empire" of methamphetamine production in media reports. This characterization is supported by the extensive distribution networks within the country, which facilitate the production and transport of methamphetamine. Precursor chemicals essential for methamphetamine production are sourced from countries such as India, Turkey, and Poland, demonstrating the transnational nature of this illicit trade. However, it is inaccurate to categorize the Czech Republic as a global leader in methamphetamine production, as its distribution primarily targets neighboring countries, particularly Germany and Poland, as well as relatively close states like the Netherlands. This regional focus underscores the need for coordinated cross-border law enforcement efforts to address the flow of drugs within and beyond Europe.

What distinguishes the Czech Republic is the unique nature of its distribution and production networks. Methamphetamine production in the country relies on small and medium-sized laboratories, which is notable given its prominence in European methamphetamine production. These laboratories are often clandestine, making detection and eradication efforts by law enforcement particularly challenging. The Czech Republic employs a distinctive production method known as the

"Czech way", which involves specific precursors such as iodine, red phosphorus, and pseudoephedrine, primarily imported from Poland and Turkey (Nožina & Vaněček, 2016, p. 47). This method is unique in its combination of these precursors and its production process, setting it apart from practices in other countries. Consequently, the Czech Republic advocates for a harmonized regulatory approach within the European Union, particularly regarding the control of iodine and red phosphorus sales, which are monitored within the country. This regulatory strategy is aimed at curbing the availability of key ingredients necessary for methamphetamine production, thereby disrupting the supply chain at its source.

Methamphetamine production also poses significant environmental threats, particularly to the Czech water ecosystem. The EMCDDA has documented the presence of methamphetamine in wastewater, with Czech cities occupying the top two positions in terms of concentration (European Monitoring Center for Drugs and Drug Addiction, 2024). This high level of methamphetamine significantly impacts aquatic ecosystems, especially fish, which face toxicity-related dangers. The toxic effects on fish populations disrupt the natural balance of the water ecosystem, leading to ecological imbalances that have far-reaching consequences for biodiversity and water quality. The contamination of water sources with methamphetamine and other chemicals used in drug production represents a pressing environmental issue that necessitates urgent attention and remediation efforts.

Transportation and logistics play a crucial role in the illegal drug trade. In the Czech Republic, organized groups frequently utilize tools such as shipping services, courier services, and online platforms for distribution. These methods are chosen for their efficiency and ability to evade detection. Courier services are particularly favored due to their anonymity, allowing drug traffickers to move large quantities of methamphetamine with minimal risk of interception. Despite regulations, regular checks by customs officials and other employees are not consistently performed unless there is specific suspicion or monitored threats by Czech or other state security structures. This irregularity in inspections, irrespective of whether shipments are custom or non-custom, facilitates the continued operation of these illicit networks. The lack of consistent enforcement and oversight highlights the vulnerabilities within the transportation and logistics sectors that organized crime groups exploit to their advantage.

International cooperation

The Czech Republic is actively engaged in reducing drug distribution chains and implementing comprehensive prevention measures. Our multifaceted approach, consisting of a three-tier strategy, includes efforts to diminish the number of

methamphetamine laboratories, provide support for individuals with addiction, and enhance overall prevention. These initiatives are coordinated at multiple levels: the state level involves international cooperation, the development of action plans, and rigorous assessments; the regional level focuses on prevention events and fostering police collaboration within the Czech Republic; and the local level is dedicated to public prevention activities such as workshops and courses, particularly aimed at assisting those struggling with addiction.

In addition to action plans and their subsequent evaluations, one of the measures implemented to curb the uncontrolled sale of medications, notably pseudoephedrine used in methamphetamine production, is the introduction of electronic prescriptions. However, the effectiveness of this measure in reducing methamphetamine production remains uncertain, as data collection and trend analysis were disrupted by the COVID-19 pandemic. During this period, the consumption and production of methamphetamine decreased significantly due to closed borders and reduced social interactions. This unprecedented situation highlighted the need for adaptable strategies that can withstand unforeseen global disruptions, ensuring that drug control measures remain effective under various circumstances.

Regional cooperation plays a crucial role in efforts to reduce methamphetamine production. Notably, collaboration with Germany has led to a continuous decline in methamphetamine distribution cases to Germany since 2014, with a marked decrease observed again in 2020, attributed to COVID-19 and border closures. The Czech-German cooperation has been instrumental in several successful operations, such as Operation Metzger, which dismantled an internationally organized group operating in the Czech Republic (Národní protidrogová centrála, 2020, p. 17). This group produced methamphetamine using precursors from Poland and distributed the drug in Germany primarily through courier services. Other notable operations include Operation MOI and Operations VANG I and VANG II, which not only dismantled several distribution networks but also led to the arrest of key individuals, predominantly of Vietnamese nationality (Národní protidrogová centrála, 2020, pp. 17–21). This demographic is significantly involved in drug trafficking, particularly in the northern and western border regions of the Czech Republic, where the Vietnamese community is concentrated. These operations underscore the importance of targeting specific ethnic and demographic groups that play pivotal roles in the drug trafficking landscape.

Operation Trouba-kufr stands out as a significant international effort (Národní protidrogová centrála, 2020, p. 19). In 2020, police departments from the Czech Republic, Germany, Israel, and the Netherlands collaborated to disrupt an amphetamine supply chain extending from the Netherlands to Israel. The organized group used courier services to transport the substance, concealing it in microwaves and labeling it as consumer goods in shipping documents. This operation exemplifies the complexity and ingenuity of drug trafficking networks and the necessity for

international cooperation to dismantle them effectively. Another notable case is Operation BAT, a 2015 joint effort between Czech police and Polish border guards (Policie České republiky, 2016). This operation targeted laboratories capable of producing 30 to 50 kilograms of methamphetamine every five days, with distribution networks extending from the Czech Republic and Poland to Germany, the Netherlands, Australia, and Albanian traffickers. The laboratories were primarily located in the Czech Republic and partly in Poland to minimize the risk of detection. These cross-border operations highlight the transnational nature of drug trafficking and the imperative for countries to work together to combat this pervasive issue.

Furthermore, the Czech Republic's approach to methamphetamine production and distribution involves not only law enforcement efforts but also comprehensive policies aimed at prevention and rehabilitation. This includes educational programs in schools, public awareness campaigns, and support services for individuals recovering from addiction. By addressing the root causes of drug addiction and providing resources for recovery, the Czech Republic aims to reduce the demand for methamphetamine, thereby weakening the drug trafficking networks.

The Czech Republic has developed its own policies and strategies to combat methamphetamine production and distribution. Nonetheless, regional and international cooperation remains of paramount importance, as the methamphetamine problem transcends national borders. These collaborative efforts are essential for effectively addressing the complex and transnational nature of methamphetamine trafficking and ensuring the security and well-being of communities across Europe. By fostering strong partnerships with neighboring countries and international organizations, the Czech Republic can leverage shared intelligence, resources, and strategies to create a unified front against drug trafficking.

The case of the United States of America

The case of the United States is particularly significant regarding illegal drug trafficking. The United States was among the first countries to identify illicit drug trafficking and the use of addictive substances as a top national security threat. This prioritization reflects the country's recognition of the profound impact that drug trafficking and abuse have on its social, economic, and security landscape. The issue of synthetic drugs has escalated in recent years, attracting attention from the Drug Enforcement Administration (DEA) and the U.S. Department of Homeland Security (DHS). The DHS has classified drugs and associated organized crime as significant threats alongside terrorism, cyber-attacks, and threats to critical infrastructure, underscoring the multifaceted nature of this challenge.

The most pressing threat is posed by synthetic drugs, particularly fentanyl and tramadol. These substances were responsible for over 75% of all overdose deaths in the United States in 2023, highlighting the severity of the crisis (U.S. Department of Homeland Security, 2023, p. 5). The rapid escalation of this threat is evidenced by the increasing seizures of fentanyl and its precursors at U.S. borders, which doubled in 2024 compared to 2022 and 2023. With 150 deaths per day, fentanyl represents the leading public health threat, a situation that demands immediate attention and action due to its implications for national security and public safety (U.S. Customs and Border Protection, 2024). The lethal nature of fentanyl, even in minute quantities, exacerbates the public health crisis, placing immense pressure on healthcare systems and law enforcement agencies.

The United States faces not only a high number of fentanyl users, but also significant risks associated with the supply chains of fentanyl and its precursor chemicals. These supply chains are often controlled by organized criminal groups, commonly referred to as cartels, which pose substantial challenges for U.S. law enforcement. These cartels are involved in the production, smuggling, and distribution of drugs and are known to support violent groups operating within the United States. These violent groups, which utilize force or the threat of force to achieve their objectives, contribute to elevated crime levels, posing immediate threats to the population and fostering societal instability. The financial resources generated from drug trafficking empower these cartels, enabling them to perpetuate violence and corruption, further destabilizing affected regions.

Most of these cartels operate in Central America, particularly Mexico, and have established distribution networks extending from the United States to Europe and Asia. This international dimension of the threat necessitates coordinated international measures, an initiative that the United States actively leads. U.S. authorities have identified cartel activities as a primary risk to the rule of law, citing increased crime levels and the associated societal instability as direct consequences. The transnational nature of drug trafficking requires a collaborative approach to dismantle these complex networks and disrupt the flow of illicit drugs.

These concerns led to the establishment of the Global Coalition to Address Synthetic Drug Threats, spearheaded by the United States (Global Coalition to Address Synthetic Drug Threats, n.d.). This initiative aims to enhance coordination between states in combating organized crime, uncovering drug supply chains, and dismantling synthetic drug production facilities. The coalition was formed in 2023 through a ministerial-level meeting. However, the coalition's effectiveness remains uncertain. Notably, China, a major supplier of precursor chemicals necessary for synthetic drug production, is not a coalition member. China's non-participation complicates efforts to reduce synthetic drug production, given its significant role as a supplier. The inclusion of all key players, including major

precursor suppliers, is crucial for the coalition's success in mitigating the synthetic drug threat.

However, the United States does not solely depend on international cooperation and globally accepted measures in its fight against synthetic drug trafficking. The U.S. is actively engaged in combating the distribution of fentanyl within its borders through various national strategies and enforcement efforts. The Department of Homeland Security (DHS), alongside its subordinate agency, U.S. Customs and Border Protection (CBP), has implemented significant measures to address this critical issue.

In 2023, the CBP released a comprehensive strategy specifically aimed at combating fentanyl and other synthetic drugs (U.S. Customs and Border Protection, 2023). This strategy encompasses four primary goals, each supported by specific tools and initiatives designed to reduce the production and distribution of these substances effectively. The goals include enhancing information sharing within the United States, deploying advanced technologies for drug detection at borders, exposing supply chains that lead to the U.S., and collecting global data on chemical suppliers and precursor sellers. This multi-pronged approach ensures a thorough and coordinated response to the escalating crisis.

The national strategy aligns closely with the principles and objectives established by the Global Coalition to Address Synthetic Drug Threats. This alignment is strategically advantageous as it enhances the potential for successful outcomes by harmonizing efforts at both national and international levels. The coalition, initiated by the U.S. in 2023, seeks to improve coordination between states in combating organized crime, uncovering drug supply chains, and dismantling synthetic drug production facilities.

Despite these robust measures, a critical evaluation of the national strategy reveals a significant omission: the absence of comprehensive prevention mechanisms. While the strategy addresses the current challenges posed by synthetic drugs, it lacks a clear plan to prevent the emergence of new addicts. Addressing the problem only after it has manifested is insufficient for achieving long-term resolution. The core issue lies in the persistent demand for synthetic drugs. Without proactive measures targeting vulnerable groups before addiction takes hold, the cycle of drug abuse will continue unabated.

The expansion of supply chains and illegal drug networks is a direct response to market demand. Consequently, it is imperative to dismantle existing networks, cartels, and organized groups involved in the production, smuggling, and distribution of synthetic drugs. This approach should encompass all aspects, including prevention, education, support for drug addicts, and the disruption of supply chains and organized crime networks.

The U.S. government's comprehensive strategy must also focus on prevention and education initiatives. By addressing the demand side of the equation, the U.S.

can create a more sustainable and effective strategy for combating the synthetic drug crisis. Prevention programs should target at-risk populations, providing education on the dangers of synthetic drugs and resources for those struggling with addiction. Additionally, enhancing community outreach and support services can help mitigate the factors that contribute to drug abuse.

Furthermore, international collaboration is crucial for addressing the transnational nature of synthetic drug trafficking. The U.S. must continue to work with international partners to disrupt supply chains and dismantle production facilities. Strengthening intelligence-sharing mechanisms and joint operations can enhance the effectiveness of these efforts. By fostering global cooperation, the U.S. can better tackle the complex and pervasive threat posed by synthetic drugs.

In summary, while the United States has made significant strides in combating the distribution of synthetic drugs through national strategies and international cooperation, a more comprehensive approach is needed. This approach should include robust prevention mechanisms, education initiatives, and support services for those affected by addiction. By addressing both the supply and demand sides of the equation, the U.S. can develop a more sustainable and effective strategy for combating the synthetic drug crisis, ensuring the safety and well-being of its citizens.

References

Das, P. (2019). Drug-trafficking as a non-traditional security threat: Emerging trends and responses. *Journal of Social Sciences*, *18*(4), 1–23. https://www.researchgate.net/publication/338213060_Drug-trafficking_as_a_Non-traditional_Security_Threat_Emerging_Trends_and_Responses

European Monitoring Centre for Drugs and Drug Addiction. (2019). *Methamphetamine in Europe*.

European Monitoring Centre for Drugs and Drug Addiction. (2021). *European Drug Report 2021: Trends and Developments*. https://www.emcdda.europa.eu/publications/edr/trends-developments/2021_en

European Monitoring Centre for Drugs and Drug Addiction. (2024). *Wastewater analysis and drugs — a European multi-city study*. https://www.emcdda.europa.eu/publications/html/pods/waste-water-analysis_en

Global Coalition to Address Synthetic Drug Threats (n.d.). *About us*. https://www.globalcoalition.us

Národní protidrogová centrála. (2020). *Výroční zpráva 2020*. https://www.policie.cz › vyrocni-zprava-npc-2020

Nožina, M., & Vaněček, M. (2016). *Národní protidrogová centrála 1991–2016*. Národní Protidrogová Centrála. https://www.policie.cz/clanek/narodni-protidrogova-cen-

trala-skpv-narodni-protidrogova-centrala-aktuality-narodni-protidrogova-centrala-1991-2016.aspx

Policie České republiky. (2016). *Mezinárodní operace „BAT"*. https://www.policie.cz/clanek/mezinarodni-operace-bat.aspx

U.S. Customs and Border Protection. (2023). *CBP strategy to combat fentanyl and other synthetic drugs*. https://www.cbp.gov/document/report/cbp-strategy-combat-fentanyl-and-other-synthetic-drugs

U.S. Customs and Border Protection. (2024). *Frontline against fentanyl*. https://www.cbp.gov/border-security/frontline-against-fentanyl

U.S. Department of Homeland Security. (2023). *DHS continues to see high risk of foreign and domestic terrorism in 2024 homeland threat assessment*. https://www.dhs.gov/news/2023/09/14/dhs-continues-see-high-risk-foreign-and-domestic-terrorism-2024-homeland-threat

About the Authors

Marek Pietraś – professor, political scientist, specialist in the discipline of international relations, graduate of the University of Warsaw, Director of the Institute of International Relations, at the Faculty of Political Science and Journalism of Maria Curie-Skłodowska University. His scientific achievements include over 230 publications, books, edited monographs, articles in journals also in English. He has experience in implementing 9 national and international research projects. He was a scholarship holder of many foundations, conducting research at universities in the United States, Great Britain, Germany, Italy (European University in Florence) and Hungary (Central European University). He completed several short-term study stays at the London School of Economics and Political Science. He delivered papers at IPSA, EISA, BISA and other congresses. In 2010–2013, he was appointed by the President of the Republic of Poland as a member of the National Security Strategic Review Commission, which prepared the first ever White Paper on Poland's National Security. In November 2021, Prof. Pietraś was honored by the National Academy of Sciences of Ukraine and the Union of Scientists of Ukraine with the title of "Best Foreign Scientist 2021 in Ukraine".

Ewelina Kancik-Kołtun – Doctor of Social Sciences in the field of Political Science, Assistant Professor at the Chair of Public Administration at the Faculty of Political Science and Journalism, Maria Curie-Skłodowska University in Lublin. In 2015, she received her doctorate from UMCS. She deals with the issues of the Visegrad Group, in particular the issues of democracy, civil society, local government, political parties, security, political and territorial marketing and new media. She specialises in social research and has participated in more than 80 scientific conferences (Poland, Ukraine, Slovakia, the Czech Republic, Hungary, Greece, the Netherlands, Estonia, the USA). As a manager, she has conducted international research projects and completed internships in Ukraine, Slovakia, the Czech Republic and Hungary. Author of numerous books and scientific articles. Editor of a series of publications about the Visegrad Group.

Jakub Olchowski – political scientist, academic teacher and international relations analyst. Assistant Professor at the Institute of International Relations, Maria Curie-Skłodowska University in Lublin (UMCS). Head of Eastern Department at Institute of Central Europe – a public think tank. Political commentator in

Polish and foreign media. Expert at the Center of Eastern Europe of UMCS, member of the UMCS Propaganda and Disinformation Research Team, member of Editorial Committee of *Yearbook of the Institute of East-Central Europe*. Author, co-author and editor of multiple publications (books, articles as well as analyses, expert opinions and reports for Poland's authorities) on international relations and international security; author of several hundred press articles. Participated in numerous international conferences and events. Participated and coordinated projects delivered in cooperation with universities in Germany, Lithuania, Slovakia and Ukraine. Visiting professor at universities in Ukraine, Lithuania, Latvia, Turkey and Portugal. As an IR analyst he mainly concentrates on security issues, Ukraine and Russia. In his university research and teaching focuses on: international relations, particularly in Central and Eastern Europe; evolution of international security; information warfare; international organizations; ethnic relations and cultural identity.

Agnieszka Demczuk – post-doctoral degree, lawyer and political scientist, professor at Maria Curie-Skłodowska University in Lublin in the field of political and administration sciences, has been working at the Department of Political Systems and Human Rights at the Institute of Political Science and Public Administration since 2008; from 2020, head of the Propaganda and Disinformation Research Team at UMCS; author of works on the protection of human rights, freedom of expression, disinformation, the COVID-19-related infodemic and an information society.

Tomáš Kolomazník – co-founder and director of Center for Security Consulting. He is dedicated to security policy, the defence industry, and cyber and information security. He is a member of the security community at the Geneva Center for Security Policy Alumni Association. He participates in international projects, speaks at conferences, and publishes on security topics at home and abroad. He previously worked at the Ministry of Defense in the Defense Policy and Strategy Section, where he was in charge of international relations. He is currently teaching at the private Ambis University in Prague and, at the same time, completing PhD studies at the Metropolitan University of Prague.

Ondřej Filipec – PhD, a Czech political scientist working at the Faculty of Law, Palacký University in Olomouc. He focuses mainly on security issues, EU affairs, institutions, and policies. He is an active member of several scientific societies, including the Czech Political Science Association and the Czech Association for European Studies, and editor of the *Slovak Journal of Political Sciences*. He published over 100 academic publications covering various aspects of security issues, including several monographs in prestigious publishing houses like Routledge or Springer.

Piotr Celiński – professor, media studies scholar affiliated with the Faculty of Political Science and Journalism, Maria Curie-Skłodowska University in Lublin. Interested in new media, the Internet, digital culture, social communication, visual and popular culture (www.postmedia.pl). Co-founder and board member of the Digital Culture Institute Foundation, co-creator of cultural events, exhibitions and educational activities (Mindware; EPCC), board member of the Polish Film and Media Research Association (ptbfm.org).

Daniel Šárovec – a Ph.D. student from the Department of Political Science and Anglophone Studies at Metropolitan University Prague, Czech Republic. In his dissertation, he focuses on the digitalization of political parties. Daniel has already published couple of works focused on political parties, new political parties, digitalization of political parties as well as on party systems. He regularly attends both international and domestic conferences.

Justyna Kięczkowska – PhD, a graduate of the Faculty of Political Science and Journalism, Maria Curie-Skłodowska University, an assistant professor in the Department of International Security and a postgraduate in Healthcare Management. She focuses her research interests on issues related to health security, cyber-security and multi-dimensional health threats. She is the author of publications analysing interdisciplinary approaches to health and health security. For the past 5 years, she has organised a regular conference on health security in cooperation with the Polish Academy of Sciences and the Foundation for International Research.

Michal Klíma – professor, a political scientist and the rector of Metropolitan University Prague. He obtained his professorship in the field of political science at the University of Economics, Prague. In addition to Metropolitan University Prague, Michal Klíma has lectured at the University of Economics in Prague, and the Faculty of Philosophy at Palacký University in Olomouc. His research interests include post-communism, comparative democracies, clientelism, and party and electoral systems. In 2020, he published the book *Informal Politics in Post-Communist Europe: Political Parties, Clientelism and State Capture* (London and New York: Routledge). He also appears in the media and publishes analyses of current political relations in the Czech Republic and Europe.

Katarzyna Marzęda-Młynarska – PhD, professor at Maria Curie-Skłodowska University, Head of the Department of International Security, Deputy Director of the Institute of International Relations at the Faculty of Political Science and Journalism, UMCS. Conducts research on non-military dimensions of security, with particular emphasis on food security and migrations. Author of numerous publications on

international relations, including monograph on global food security governance at the turn of the 20th and 21st centuries. Participant of international research projects devoted to broadly understood security issues, co-organiser of a cyclical international scientific conference on security threats in globalisation processes. Her current research interests focus on the impact of the war in Ukraine on global food security.

Adrian Szumowski – has an MA in International Relations, and graduated from the Faculty of Political Science, Maria Curie-Skłodowska University in Lublin. During his study years he participated in the Erasmus student exchange program at Salford University, Manchester. He is currently a PhD student in the Department of International Relations at the Faculty of Political Science at the Maria Curie-Skłodowska University in Lublin. He was the manager of a scientific project entitled "Dynamics of Power in late-Westphalian International Environment", funded by the National Science Center, Poland. His main field of study is the evolution of international relations.

Zdeněk Rod – assistant professor at the Department of Politics and International Relations at the University of West Bohemia in Pilsen. Zdenek specializes in security studies and conflict resolution. He also co-runs a security consulting firm, Centre for Security Consulting. Prior to his academic pursuits, Mr. Rod contributed to the Czech Ministry of Defence, bringing practical experience to complement his scholarly endeavours. He has a rich publication history, having authored and co-authored numerous academic and policy articles. His contributions extend to active involvement in national and international research projects, showcasing his commitment to advancing knowledge and understanding in his areas of expertise.

Miroslav Plundrich – assistant professor at the Department of Politics and International Relations of West Bohemian University in Pilsen. His primary focus is conflict management, and his Ph.D. thesis focused on recognizing negative non-state actors in the international system. He is also interested in migration, hybrid warfare, the politics of the US and the UK in world affairs, and the security affairs of the Middle East. Next to the academy, he is currently collaborating with the Chief of the Czech Armed Forces General Staff as a member of the Civilian Advisory Group and doing special analyses for the Ministry of Interior of the Czech Republic.

Elizabeth Freund Larus – Ph.D., Non-resident Senior Fellow at the Atlantic Council Global China Hub with co-affiliation with the Indo-Pacific Security Initiative, Adjunct Senior Fellow at the Pacific Forum, and Professor Emerita of Political Science and International Affairs at the University of Mary Washington. She is a 2020 Fulbright Research Scholar at Marie Curie-Sklodowska University in Lublin, Poland

and a 2015 Taiwan Fellow at National Cheng-chi University in Taipei. A China and Taiwan analyst for more than 30 years, she is author of the books *Politics and Society in Contemporary China* (1st and 2nd eds.) and *Economic Reform in China* (2005), as well as more than 25 academic articles and book chapters on politics in China, Taiwan's foreign policy, and US policy in Asia. She regularly offers commentary to BBC Chinese, Deutsche Welle, the Financial Times, France24, and WION News (India).

Agata Wiktoria Ziętek – Ph.D, associate professor at the Faculty of Political Science and Journalism, International Relations Institute, Maria Curie-Skłodowska University in Lublin. Author of two monographs, co-author and scientific editor of eight monographs, including two in English. Author of 15 articles in journals and monographs in English and 32 articles in Polish. Member of the Editorial and Program Boards of journals: *Teka of the Commission of Political Science and International Affairs* (until 2018); from 2023, *Asia-Pacific*. President of the Board of the Foundation for International Studies (2009–), President of the Lublin branch of the Polish Society for International Studies (PTSM) (2012–), Member: Scientific Advisory Board, "European Culture" (2008–2011), European International Studies Association (2013–), Member of the World International Studies Committee (2017–). She is a 2015 Taiwan Fellow at National Cheng-chi University in Taipei.

Sarah Cernikova – a Ph.D. student, University of West Bohemia in Pilsen. She deals with safety issues.

The book “Contemporary Security Problems of Poland and the Czech Republic” is a topical contribution to the contemporary research on European security. Both covered countries play an important role in regional relations, and threats to their external security are closely linked to internal security issues. The authors´ team identified and analyzed essential challenges and phenomena related to contemporary security events and processes.

The book is an essential part of contemporary scientific research in security , and it has developed various subdisciplines, such as security and strategic studies, international relations, foreign policy analysis, etc. It can serve in academics as well as in broader expert fields. It can be helpful for security analysts, decision-makers at various political levels, or journalists. The knowledge base for future research is included in the book.

Prof. JUDr. PhDr. Miroslav Mareš
Masaryk University in Brno

wydawnictwo.umcs.eu

UMCS
WYDAWNICTWO

ISBN 978-83-227-9860-7