DISINFORMATION AND THE RESILIENCE OF DEMOCRATIC SOCIETIES

EDITORS
ROBERT KUPIECKI
AGNIESZKA LEGUCKA

PISM | POLSKI INSTYTUT SPRAW MIĘDZYNARODOWYCH
THE POLISH INSTITUTE OF INTERNATIONAL AFFAIRS

The Polish Institute of International Affairs

DISINFORMATION AND THE RESILIENCE OF DEMOCRATIC SOCIETIES

Editors
Robert Kupiecki, Agnieszka Legucka

Warsaw 2023

Reviewer
Agata Włodkowska-Bagan

Cover photo
a-arrow / Canva.com

Cover designer
Tomasz Białkowski

Proofreading
Brien Barnett

Technical editor
Dorota Dołęgowska

ISBN 978-83-67487-20-7 (pb)
e-ISBN 978-83-67487-21-4 (pdf)

Publisher
Polski Instytut Spraw Międzynarodowych,
ul. Warecka 1a, 00-950 Warszawa
www.pism.pl

Print
Centrum Poligrafii Sp. z o.o.
ul. Michała Spisaka 37
02-495 Warszawa

List of Contributors:

Filip Bryjka, Ph.D., analyst at the Polish Institute of International Affairs and adjunct professor at the Institute of Political Studies, Polish Academy of Sciences.

Tomasz Chłoń, policy expert and leader of the Platform for Countering Disinformation, a research and education group of independent scholars, former ambassador of Poland to Estonia and Slovakia, and former director of the NATO Information Office in Moscow.

Jędrzej Czerep, Ph.D., head of the Middle East and Africa Programme at the Polish Institute of International Affairs

Krzysztof Kozłowski, vice-rector of the Warsaw School of Economics and associate professor, Institute of International Studies, Warsaw School of Economics.

Robert Kupiecki, associate professor at the Faculty of Political Science and International Studies, University of Warsaw, a career diplomat and former ambassador of Poland to the USA and former deputy minister of National Defence.

Agnieszka Legucka, senior analyst at the Polish Institute of International Affairs and associate professor at the Faculty of Business and International Relations, Academy of Finance and Business at Vistula University in Warsaw.

Wojciech Lorenz, Ph.D., senior analyst at the Polish Institute of International Affairs.

Jan Misiuna, adjunct professor at the Institute of International Studies, Warsaw School of Economics.

Justyna Podemska, Ph.D., historian and high-school teacher.

Piotr Podemski, Ph.D., adjunct professor at the Oriental Studies Faculty, University of Warsaw.

Marcin Przychodniak, Ph.D., senior analyst at the Polish Institute of International Affairs.

Table of Contents

Introduction

We live surrounded by information, which we process to meet both individual and collective needs. Based on these needs, we make decisions about key matters in our lives and the communities to which we belong. This is why it is crucial that our information environment is replete with correct facts and data that are neither intentionally distorted nor falsified, thus establishing the baseline for making rational and optimal decisions. In our daily lives, however, we are confronted with an unprecedentedly large and constantly growing amount of information that we must not only sift through and select but also verify and assess in terms of truthfulness. We use modern electronic tools and media platforms, which guarantees that the amount of information keeps increasing, its sources multiplying and spreading quickly, having an ever-greater societal impact. With all the social, technological, and political factors combined, people in a modern setting may be now more aware of their reality that surrounds them while also vulnerable to new risks and threats.

Among these risks and threats is the problem of disinformation, which is increasingly intertwined with reality. It comes in many forms, stemming from the physical limitations of humans, their analytical weaknesses, or multiple cognitive biases. Without

systematic work on the development and consolidation of skills to detect it and forming habits of fact-checking, disinformation can relatively easily find its way into our schools, academic or state institutions, and social interactions as a legitimate part of discussions, with all its negative consequences, from personal safety to international security. The threat is all the greater because democratic societies operate with open and diversified information systems that not only tolerate differing points of view but also even protect the right to express them. However, this space of social freedom obscures risks, eagerly used against this freedom by the perpetrators of disinformation.

Disinformation, reinforced by the rapid expansion of technology, including the internet and artificial intelligence, manifests itself as a tool of advertising, political marketing, or a "weapon" in the political activities of modern states seeking to influence the individual and collective behaviour of other states and societies. Why? The same reason that has held for thousands of years: power, world domination, or simply to sell more products, regardless of the damage done to the object of the disinformation. Of course, each of these general reasons, and their hierarchy, may change over time and evolve into more nuanced justifications for what disinformers do.

Disinformation can undermine democratic societies, their institutions, and popular choices. In recent years, societies, governments, international organisations, and technology companies have stepped up their efforts to counter it. Whether they will be effective depends on how determined they are to continue their efforts, starting from strengthening societal resilience and media literacy.

These issues are at the heart of this publication. Its goal is to support media education by presenting scientifically verified knowledge about the dangers of disinformation and how to combat it. The book was prepared as part of a project financed

by the 2020 NATO Headquarters research grant ***Counter-Disinformation Platform—Building Social Resilience. Research and Education*** **and co-sponsored by the Polish Institute of International Affairs.** The authors responsible for its content are researchers from SGH Warsaw School of Economics, the University of Warsaw, the Polish Institute of International Affairs, and practitioners in the fields of education, diplomacy, and combating international disinformation. The aim of the *Counter-Disinformation Platform, Research and Education* project is to raise the general societal competence to thrive in the modern information environment, to understand and neutralise the impact of disinformation.

The project constitutes a proposal for a nationwide model that ultimately will cover all levels of schooling and higher academic education. To achieve this aim, the proposed operation should be guided by the following principles:

- civic spirit: social "ownership" and independence from government agencies, but willingness to cooperate with them;
- networking: horizontal (inter-university) and vertical (primary school, high school, university),
- mass participation: ultimately covering as many educational institutions as possible, students and pupils as well as other recipients;
- applicability: operationalisation of research, which will translate into practical activities; and,
- media coverage: dissemination of the project's outcomes by patrons and partners in national and local media.

The *Counter-Disinformation Platform—Building Social Resilience. Research and Education* programme and the plans for its implementation meet the expectations of the North Atlantic Treaty Organisation (NATO), which emphasises the need to actively involve the societies of the Member States in counteracting

the disinformation directed against them. Spreading the understanding of NATO's role, the values on which it is based and which it protects, and increasing support for the Alliance's mission among the younger population is also an important element of the strategic goals of this project.

The authors and editors of this publication hope that its content may be useful in public education in Poland and abroad. Their intention is, first of all, to fill a significant educational gap in counteracting disinformation (present in the vast majority of countries confronted with this threat).

They have made an attempt to provide readers with a concise and linguistically friendly way to lead them through the genesis and difficulty of defining disinformation and its manifestations in various areas of life, with particular emphasis on international politics. On this basis, readers are offered practical tools for academic and school education. While preparing individual parts of this book, the authors consulted numerous monographic studies, research reports, expert opinions, other studies, and media reports on disinformation in international relations, its causes, goals, methods and means, and used the results of this research to form practical recommendations on how to counteract disinformation.

The volume contains 11 texts covering a broad spectrum of the problem. Its first part, devoted to the theory and practice of disinformation, opens with a chapter by **Robert Kupiecki**, "Disinformation and international relations: sources, aims, actors, methods", which reviews disinformation from the perspective of international security studies. It also provides basic knowledge about the origins, definitions, internal structure, and the main state manifestations of disinformation. The second text by **Tomasz Chłoń** and **Krzysztof Kozłowski** is entitled "Selected case studies of disinformation: Russia and China" and is an attempt to systematically analyse the goals and manifestations of

these two countries' activities in the infosphere. Not only are they a large part of the disinformation phenomenon today, but they also serve as a specific model of technically advanced methods of operation. The subsequent chapter, by **Agnieszka Legucka**, "Targeting Poland: history as a tool of Russian disinformation" tackles the problem of the *weaponisation* of the past in Russian information operations. They are instrumentalised by Moscow as both tools of its foreign policy and domestic legitimisation.

Wojciech Lorenz, in his essay "Strategic propaganda and disinformation: the evolution of Russia's campaign to undermine NATO", takes a broad look at the propaganda and information warfare means Russia has utilised to break NATO cohesion. This alliance, since 1949 has been considered by the authorities in Moscow, first as the Soviet Union and now by the Russian Federation, as the main geopolitical enemy. **Jędrzej Czerep**, with his piece "Illusion of attractiveness—Russian pursuit of a success story in Africa "brings a case of a complex, multi-layered exercise by Russia to win hearts and minds, in this particular case, in the Central African Republic and Mali. Next, **Jan Misiuna** authors the short essay "Disinformation and elections: case study of US presidential elections", in which he examines the impact of Russian disinformation on electoral processes and presents as case studies the 2016 and 2020 U.S. presidential elections. This part of the book is completed by **Marcin Przychodniak**'s chapter on "Chinese disinformation: ideology, structures, efficiency". The author shows the specificity of China's disinformation activities and their developmental nature based on adapted Russian patterns.

While the first part of the book offers a broad perspective on the scope of disinformation, its roots, objectives, tools, and perpetrators, the second part takes on the much more challenging issue of combating this phenomenon on the individual, state, and international community levels. The primary focus of this part of the book is education, aiming to lead to "responsible use

of information". It is focused on developing readers' practical skills to recognise and combat disinformation. In "Countering disinformation", **Tomasz Chłoń**, who until 2020 was the Director of the NATO Office in Moscow, takes up the issue. In addition to reviewing best practices of various countries in this field, he also brings a considerable dose of knowledge about non-governmental initiatives and places where good standards in this field are created. This "big picture" attempt is then substantiated by the following texts. The chapter "Detecting and countering disinformation—proposed syllabus for a university course" by **Filip Bryjka** contains a 30-class-hour course programme (including bibliography) that can be used for courses in the political sciences, business, strategic studies, or journalism. The added value of the syllabus lays also in the fact that its individual modules can be adapted in form and content to the specific educational needs. Bryjka's "Notes on detecting and countering disinformation. Educational materials for university syllabus" serve as a detailed companion to the content of the most important parts of the proposed syllabus.

"Protect yourself against disinformation" by **Justyna Podemska** and **Piotr Podemski** contains a detailed proposal of plans for three lessons at the primary/secondary school level prepared by experienced teachers. The aim is to show how to shape students' basic skills in the responsible consumption of information based on the Knowledge–Attitudes–Practice (KAP) model. The authors' intention is to make lessons on this topic interesting for students through extensive use of multimedia and encouraging participation in class.

All contributors to this volume are experienced academicians, or think-tank researchers and practitioners. Each of their texts is fully referenced to document the course of work and present readers with a selection of verified publications. For those interested in the scientific study of disinformation, the aforementioned literature may serve as a starting point or help in further research.

This project could not have begun without the support of the North Atlantic Treaty Organisation and its scientific grant *Counter-Disinformation Platform—Building Social Resilience. Research and Education*. However, it would not take the form of this book without the Polish Institute of International Affairs, to whom the editors and authors express their gratitude.

Robert Kupiecki, Agnieszka Legucka

ROBERT KUPIECKI
Faculty of Political Science and International Studies
University of Warsaw
ORCID: 0000-0003-3419-6948

Disinformation and International Relations: Sources, Aims, Actors, Methods

In order to live and thrive in a society, people need information, i.e., data, that is true or based on the understanding of the impact of distortions on the general correctness.[1] Information is part of the human ecosystem, no less essential than water, air, and food for it helps determine in a similar way one's survival and quality of life. Information is necessary to understand and relate to the surrounding world. The significance of accurate information increases with its functioning in important social contexts: those requiring knowledge, interpretation of important events, or in making key decisions. This general statement applies to all human

[1] To verify whether information is true, one can deploy intellectual standards based on experience, verified data, procedures, reliability of sources, and a scientific approach. For the latter approach, see: L. McIntyre, *Post-Truth*, MIT Press, Cambridge 2018.

individuals and organisations, including societies, nations, and states, and their mutual relations based on the exchange of information.

The Concept of Disinformation

Securing information sources and the ability to verify and protect data is an elementary component of the security of every entity, regardless of the level of analysis (individual-state-international system) or its functional dimensions (e.g. politics, economy, military, environmental issues, social). The truthfulness of the information obtained, as a reliable reflection of the facts, is a condition for making rational decisions. Based on the correct processing of the input data, information allows an individual or group to choose an action that creates the premises for the optimal achievement of the set goals without harming others or at their expense.

This process can be disturbed in many ways, for example, due to ignorance, or rejection of knowledge, or independent of the decision-maker confronted with intentional and systematic deception. This may be the result of deliberate attempts at disinformation or unintentional disinformation (in the sense of unknowingly introducing false information into circulation, partly untrue, or unverified as to its truthfulness), or misuse of information (e.g. to stigmatise certain social groups, hate speech).[2] Irrespective of its manifestation, each of these information manipulations is a threat and can be the result of external inspiration and hostile influences. A special case, however, is deliberate disinformation aimed at:

[2] Terminological issues related to the notions of "disinformation-misinformation-malinformation" are discussed by A. Lanoszka, "Disinformation in international politics", *European Journal of International Security*, April 2019, pp. 3–4, DOI: 10.1017 /eis.209.6.

- falsifying knowledge required for the guaranteed accuracy of some course of action;
- making access to verified facts difficult;
- transforming social awareness;
- causing fear or uncertainty; or,
- manipulating (mixing truth and falsehood) fact-based premises for decisions made by the victim of disinformation.

The gaining of control, or even partial, by a foreign state of the way information is processed by the society of another state or its content[3] implies the ability to influence the latter's decision-making systems. Those who can influence the decisions of nations increase their own power and international political effectiveness. They also do it at a lower cost compared to long-term economic pressure, political coercion, or armed conflict.

In interstate relations, influencing others by means of disinformation based on fabricated data (essentially false, although with details that combine untruth and truth) has been

[3] The problem was also extensively analysed, see: K. Shu et al. (eds.), *Disinformation, misinformation, and fake news in social media. Emerging research challenges and opportunities*, Springer Nature, 2020, DOI: 10.1007/978-3-030-42699-6_1, J. Auerbach, R. Castronovo (eds.), *The Oxford handbook of propaganda studies*, Oxford University Press, Oxford 2013, T.R. Levine (ed.), *Encyclopedia of deception*, SAGE, London 2014. On the other hand, manuals for such actions (and counter-actions) are available, see: *Journalism, fake news, disinformation. Handbook for journalism education and training,* United Nations Educational, Scientific and Cultural Organisation, Paris 2018, R. Kick (ed.), *The Disinformation guide to media distortion, historical whitewashes and cultural myths*, Disinformation Network, New York, 2001, H.K. Melton. R. Wallace, *The official CIA manual of trickery and deception*, Harper, New York 2010, D. Smith, *Banned mind control techniques unleashed. Learn the dark secrets of hypnosis, manipulation, deception, persuasion, brainwashing and human psychology*, 2014, I.M. Pacepa, R.J. Rychlak, *Disinformation. Former spy chief reveals secret strategies for undermining freedom, attacking religion and promoting terrorism*, WND Books, Washington DC 2013, P. Houston, M. Floyd, S. Carnicero, *Spy the Lie. Former CIA officers teach you how to detect deception*, St. Martin's Press, New York 2012.

a component of strategic communication of states or a political tool in times of war and peace from the earliest times. The goal has always been to gain an advantage over the opponent, to disrupt their situational awareness, and thus to make it difficult to overcome the *decision fog*—the inherent uncertainty of a decision concerning a more or less distant future. For example, doctored information was used to mislead enemy armies during war.[4] A classic example of this is the story of the deception during the Battle of Troy—the Trojan Horse—which was preceded by an information operation about the withdrawal of the Greeks besieging the city, prompting the Trojans to lose vigilance. In times of peace, appropriate control of information (true, partially false, or false) can project an image of power to convince the opponent that aggression is not profitable. The effectiveness of the deterrence policy is based on a psychological mechanism of political manipulation. This is achieved by extensive application of propaganda (supported by intelligence organisations) and public diplomacy, gradually enriched with knowledge from social sciences and human sciences, as well as modern mass communication technologies.

The methods of contemporary marketing and advertising based on the repetition of content and images, subliminal persuasion using a combination of real and prepared data, and individualisation of the message (for example, online advertisements personalised on the basis of machine analysis of users' internet behaviour) are just a contemporary "training ground" for more complex and socially harmful information operations. The state-owned disinformation

[4] Sun Tzu, the Chinese general and author of classic strategic thought for 25 centuries, often points to the importance of misleading the enemy, see: *The Art of War. Complete Texts and Commentaries* (T. Cleary, transl.), Shambhala Publications, Boston/London 2003. Following his lead, other classics of strategic thought, from the Greeks and Romans through Niccolò Machiavelli to the strategists of the nuclear era and contemporary theoretical approaches to strategic disinformation, point to how information is used.

dispatchers also draw conclusions from marketing and advertising, observing the techniques and methods and their effectiveness in changing customer preferences. The worlds of politics and global trade, although differing in the effects of the actions induced, can be compared on the level of the approach to information, or its instrumentalisation in order to achieve specific benefits.[5]

The deliberate use of false information to mislead a recipient is therefore hardly new in politics or in business, at least in terms of the general characteristics of disinformation activities and the intentions of their operators. However, the nature and significance of this problem in modern times has become more relevant, spurred on by the development and globalisation of media and the rapid technological development in digital communication tools. Permitted by this technological revolution and endowed with "weapons of massive manipulation", the temptation to conduct information operations grows rapidly. Online platforms have fundamentally changed the reach and nature of disinformation, as well as the speed with which it spreads. These platforms also provide financial incentives to specific groups of users (e.g., those with the highest reach and "click-through" rates), favouring the dissemination of unverified information and making it difficult to identify the actual producers. The platforms also have significantly facilitated the conduct of disinformation operations (e.g., by state services) by making it possible to efficiently and effectively use fabricated texts, photos, graphics, and audio recordings. Their purpose may include (or often in combination with several of these goals) disseminating false descriptions of events, authenticating untruths, undermining knowledge-based opinions, discrediting democratic institutions, or confusing recipients.

[5] See: *Zjawisko dezinformacji w dobie rewolucji cyfrowej. Państwo, społeczeństwo, polityka, bisnes*, NASK Państwowy Instytut Badawczy, Warszawa 2019, www.cyberpolicy.nask.pl/raport-zjawisko-dezinformacji-w-dobie-rewolucji-cyfrowej-panstwo-spoleczenstwo-polityka-bisnes (accessed 21.11.2022).

The long-term impacts of this type of manipulation can lead to changed attitudes and different individual and group decisions. In the United States, a fierce debate lasts to this day over the extent of Russian information operations during the 2016 presidential elections and their impact on Donald Trump's victory. Equally controversial and interesting for analysts was the long campaign—supported from abroad—that favoured the UK leaving the European Union (Brexit). Planned and deliberate disinformation is therefore a special case, and its derivative threats are increasingly important. The aim is to permanently influence the behaviour of large groups of people and to manipulate their attitudes, while the tools used for this purpose are based on the systemic use of false information in order to destroy cultural or common-sense foundations for the functioning of societies: destroying trust in authorities, scientific knowledge, and public institutions, or influencing the democratic processes of foreign countries.

The Sources and Conceptual Framework of Disinformation

Definitions of disinformation indicate that it is an intentionally developed type of message based on falsehood and "whose purpose is to trigger an expected reaction in the recipient: a view, decision, action or lack thereof, in accordance with the assumption of the sender".[6] The problem is, however, so complex that many governments and international organisations define disinformation in their own way, as the basis for more or less

[6] There are many ways of defining disinformation in the scientific literature, which, for example, more clearly emphasise the manipulator's benefit (measured by the effectiveness of the influence on the side of the manipulated), the purposefulness of its actions, the structural falsehood of the message, or the intentional harmfulness of the intention, see: R. Kupiecki, F. Bryjka. T. Chłoń, *Dezinformacja międzynarodowa. Pojęcie, rozpoznanie, przewciwdziałanie*, Wydawnictwo Naukowe Scholar, Warszawa 2022, pp. 64–82.

advanced strategies to combat this contemporary political scourge. For example, the North Atlantic Treaty Organisation (NATO) defines disinformation as the "deliberate creation and dissemination of false and/or manipulated information with the intent to deceive and/or mislead. Disinformation seeks to deepen divisions within and between allies and to undermine people's confidence in elected governments".[7] The definition used by the European Union is in a similar vein, but also indicates a financial motivation of those trading in disinformation.[8] In 2018, the EU also created its own "Code of Conduct on Combating Disinformation", aimed at reducing the scope of disinformation.[9] It is not a legally-binding regulation, but an incentive for technology companies to self-regulate in order to limit the possibility of the use of social networks and the internet in general to spread disinformation and fake news.

These definitions, incorporating the impact of disinformation on state security and international economic relations, are of great importance for recognising the phenomenon itself and understanding its possible implications. However, there

[7] NATO's approach to countering disinformation, www.nato.int/cps/en/natohq/177273.htm#case (accessed 23.11.2022). Since 2014, Riga has a Centre of Excellence for Strategic Communication, dealing with, among others, research and analysis of the phenomenon of disinformation (NATO StratCom COE). These issues are also dealt with by the European Centre of Excellence for Counteracting Hybrid Threats (the so-called Hybrid COE based in Helsinki) cooperating with NATO.

[8] "Disinformation, i.e., verifiably false or misleading information that is created, presented and disseminated for economic gain or to intentionally deceive the public, distorts public debate, undermines citizens' trust in institutions and media, and even destabilises democratic processes such as elections." *Questions and answers—The EU steps up action against disinformation*, www.ec.europa.eu/commission/presscorner/detail/en/MEMO_18_6648 (accessed 23.11.2022).

[9] *EU Code of Practice on Disinformation*. For a summary and the full text, see: www.ec.europa.eu/digital-single-market/en/news/code-practice-disinformation (accessed 5.12.2022).

is a dispute among experts on the subject as to whether disinformation activities act like a "parasite" on existing social divisions or whether they have real power to create division.[10] The Council of Europe (CoE) and the Organisation for Security and Co-operation in Europe (OSCE) also draw attention to another dimension of the phenomenon, that relating to civil liberties and media freedom.[11]

The very term "disinformation" comes from the Soviet Union and was created in the interwar period by its intelligence services. Ion Pacepa, the former intelligence chief of communist Romania who fled to the West in 1978, wrote that "Joseph Stalin invented this secret 'science' by giving it a French-sounding name and pretending that it was a dirty Western practice".[12] Thus, from the very beginning, this political method was marked by a falsehood intentionally masking its origin. Interestingly, the term appeared in the dictionaries of Western languages only more than a half a century later. Before then, its semantic place was exhausted by the notions of "communist lies", or more broadly, "propaganda". In Russia, disinformation has been raised to the rank of a weapon used for the implementation of political strategies, as well as closely related to new concepts of blurring the boundaries of a conflict between clear times of war and peace in terms of offensive activities in the information domain (i.e., the "Gerasimov doctrine"). Russia was responsible for the

[10] See: A. Lanoszka, "Disinformation in international politics", *European Journal of International Security*, April 2019, pp. 1–22, DOI: 10.1017/eis.209.6., André W.M. Gerrits, "Disinformation in international relations. How important is it?," *Security and Human Rights*, 2018, no 29, pp. 3–23.

[11] For more, see: A. W.M. Gerrits, "Disinformation...," *op. cit.*, pp. 16-18.

[12] I.M. Pacepa, J.S. Rychlak, *Disinformation, Former spy chief reveals secret strategies for undermining freedom, attacking religion and promoting terrorism*, WND Books, Washington DC 2013, p. 34.

significant development of disinformation methods and providing them with a broad theoretical foundation based on notions of "active measures"[13] and "information warfare".[14]

The Russian term *maskirovka* is a more modern incarnation. It is a concept of deliberately concealing one's own intentions and assigning specific meanings to messages, as well as other instruments for gaining "influence, control of behaviour/reflexes" of the opposing party (Russian: *refleksivnoje upravlenie,* or *refleksivnyj kontrol*).[15] Therefore, it is not about a one-time action, but about exerting continuous, long-term, and complex influence on an opponent (by using, among others, prepared sequences of information). These methods complement the traditional instruments of foreign policy, serving specific programming and the controlled triggering of expected behaviours. The entire process uses narratives replicated through various technical information platforms with the clearly defined purpose of eliciting the intended reactions

[13] They refer, among others, to the techniques of manipulating media and public opinion in foreign countries by using fabricated information and more complex narratives, based on mixing true and false content, or simple falsehood and disinformation. They can be disseminated using open information platforms or people recruited for this type of operation. For more on these kinds of Soviet activities during the Cold War, see: *Soviet active measures in the west and the developing world*, www.psywar.org/content/sovietActiveMeeasures (accessed 7.12.2022).

[14] Understood as conducting information operations supporting military activities, or their independent application to achieve political goals.

[15] For more, see: T.L. Thomas, "Russia's reflexive control theory and the military", *Journal of Slavic Military Studies*, 2004, no. 2, pp. 237–256, DOI:10.1080/13518040 490450529., Ch. Paul, M. Matthews, *The Russian 'Firehouse of Falsehood' propaganda model. Why it might work and options to counter it*, RAND Corporation 2017, www.rand.org/pubs/perspectives/PE198.html (accessed 18.11.2022), M. Wojnowski, "Zarządzanie refleksyjne jako paradygmat rosyjskich operacji informacyjno-psychologicznych w XXI w.", *Przegląd Bezpieczeństwa Wewnętrznego*, 2015, no 12, pp. 11–36.

(or minimising the cases of undesired behaviour) on the part of the recipients.[16] It is based on the recognised mechanism of the tendency of human minds to accept as true information relating to common elementary knowledge and emotions repeated over and over again by many sources, regardless of facts or evidence to the contrary. Therefore, a narrative based on falsehood when confronted with the truth does not lose its persuasive power.

Thus, this way of influencing another person, groups of people, or the foreign state is a constant component of the reality in which various entities compete with each other for some specific good (e.g., international position, security, control over specific resources, military victory). In this context, a lie can function:

- as a stand-alone policy tool (relating to a specific case or person),
- as interrelated narrative sequences (concerning the course, assessment or interpretation of more complex phenomena, sequences of events, or social processes),
- or as a component of complex operations where information (information operations) plays an important role, paving the way for other policy tools.

The term "disinformation" has many synonyms, such as "propaganda", "social engineering", "persuasion", i.e., techniques of social manipulation. They mean the systematic promotion of messages with the characteristics of information prepared in a biased manner in order to evoke specific behaviours or attitudes.[17] Their common elements are:

[16] C. Kasapoglu, *Russia's renewed military thinking. non-linear warfare and reflexive control*, NATO Defence College, Research Paper 121, Rome 2015, www.ndc.nato.int/news/news.php?icode=877 (accessed 9.12.2020).

[17] M. J. Mazarr et al., *Hostile Social Manipulation. Present Realities and Emerging Trends*, RAND Corporation, 2019, www.rand.org/pubs/research_reports/RR2713.html (accessed 30.11.2022).

- the use of social tools that allow for manipulative influences persuading decision-makers to act in a specific way,
- the voluntary character of the behaviours caused by disinformation,
- awareness of deliberate harm caused to the object of the disinformation,
- awareness on the part of the purveyor of disinformation that the induced effects (decisions) are not necessarily in the best interest of the decision-maker but favour the interests of the source of the manipulation.[18]

An individual (a person who takes some action, e.g., the act of voting in democratic elections), a state body, or a social group that exerts pressure on constitutionally empowered state authorities can be considered decision-makers. Therefore, disinformation, depending on its purpose, the importance of the goals it supports and the complexity of the mechanisms serving it, can be divided into:

1) immediate and simple (tactical) for the simplest situations, such as causing a specific behaviour change (e.g., a one-time decision),
2) complex (operational), when it functions over longer or repetitive time sequences, relating to multi-threaded issues that are not a single decision-making situation (e.g., undermining trust in democratically elected authorities, authorities in some field of knowledge, scientific findings, etc.),
3) strategic, where it serves to achieve long-term goals, concerning the most important (vital) issues, precisely defined by the disposer of disinformation activities, e.g., causing a permanent change in the way of thinking or evaluating phenomena.

[18] Ł. Afeltowicz, K. Pietrowicz, *Maszyny społeczne. Współczesna inżynieria społeczna i innowacje socjotechniczne*, Wydawnictwo PWN, Warszawa 2013.

With the help of disinformation, states can offensively influence the communication and decision-making processes of foreign actors by indicating the direction of desired changes, legitimising their own goals, and consolidating their own community, while reducing the costs of such activities (in relation to the costs of other methods). They can also defend their international decisions and behaviours or hide or falsify their actual intentions by using intentionally crafted and consistently repeated content, building a friendly environment and audience for them. Finally, they can implement a hybrid strategy that integrates many internal and external, offensive, and defensive goals simultaneously.

Disinformation as a Never-Ending Story

Disinformation also can have an infinite number and form of carriers, from spoken word such as a joke or a common rumour repeated many times (freely changing the content during "circulation"); political speech; a television interview with a debate between "pseudo-authorities"; through various forms of images (manipulated films, advertising, photos, or graphic representations), sounds (music influencing the subconscious mind, relevant texts of popular songs), to the written word in the form of a press article, other message, or a text shared on social media.

Types of Disinformation

Satire and parody—function to discredit the object of disinformation with or without the intention to harm, but with the potential to fool the recipient.
Misleading content—specific use of information for a pre-intended representation of a fact or person.
Imposter content—fake content that pretends to be the original source.

Fabricated content—fully falsified information intended to deceive the recipient and cause damage.
False connection—when the title of a text or image is not reflected in the content or meaning.
False context—When true content is conveyed in a false context.
Manipulated content— when the original content is distorted in order to deceive the recipient.[19]
Myth—a renewing message containing empirically unconfirmed complex information.[20]

As we can see from this list, the content of disinformation is often intertwined integrally with its carrier and may have a seemingly innocent form. Any form of disseminating manipulated information can also create a story with a life of its own. Its pedigree and destiny can only be guessed until we acquire a larger fragment of the complex story it is part of.[21] Experts point to a relationship between three, separable, but not separate factors:

– the story/narrative itself (i.e., the way certain events are presented),

[19] The first seven types of disinformation were quoted after: C. Wardle, H. Derakhshan, *Information Disorder. Toward an interdisciplinary framework for research and policymaking*, Council of Europe, Strasbourg, October 2017, p. 17, www.firstdraftnews.org/latest/coe-report (accessed 1.12.2022).

[20] R. Kupiecki, "Mit założycielski" polityki zagranicznej Rosji", *Sprawy Międzynarodowe*, 2019, no 4, pp. 77–105, DOI: 10.35757/SM.2019.72.4.03. Myths created by states can be used in numerous narratives in foreign policy, manipulated in terms of the truthfulness of facts and the way they are presented. They can change over time and are subject to modifications and updates, depending on the needs of their administrator, as well as the changing situation.

[21] M. Bal, *Narratology. Introduction to the theory of narrative*, University of Toronto Press, Toronto 2009, T.E. Ricks, "Narratives are about 'meaning,' not 'truth'," *Foreign Policy*, 12 March 2015, www. foreignpolicy.com/2015/12/03/narratives-are-about-meaning-not-truth (accessed 16.9.2022).

- its specific message (a story enclosed in text or some other record),
- the plot (organising the description and interpretation of events in terms of context, time, place, or morally defined roles in a simple pattern of good and evil).

The relationships between the message, plot, and narrative can create an infinite number of versions of representations (plot modifications) depending on the needs, the audience to which they are directed, and the possibilities of the medium used for this purpose. The message itself is only a time- and place-specific concretisation of the narrative, which, being essentially a superior structure, functions independently of its carriers and records.[22] Such a message plays a strictly auxiliary role in relation to the key goals of policy and has for it only the value of being useful for a specific action or result it can produce. It is possible (and even necessary) to change it, maintaining consistency not in its content, but only to the overarching goal it serves. In foreign policy that uses such tools, they are deployed to achieve an aggregated effect from the various messages within a coherent strategic narrative. The aim is to have a specific informational impact on the international debate or a situation in a foreign country, in accordance with the needs of the party conducting the given disinformation activities.

Disinformation—The Vulnerability of Democratic Societies

The dynamics and complexity of these phenomena, multiplied by the power of modern digital technologies, make it extremely difficult to recognise and fight disinformation in an organised manner, as well as to isolate and remove false content from public

[22] J. H. Kołodziej, "Narratologia w badaniach komunikacji politycznej. Metodologiczne przymiarki," *Polityka i Społeczeństwo*, 2017, no 1, p. 26, DOI: 10.15584/polispol.2017.1.2.

circulation. The impact of a given message depends on many factors, including:

- the nature of the environment in which it operates (e.g., an open society with a democratic nature of public debate),
- determination of the administrator regarding its use in the country and abroad,
- social affirmation of the content and the emotional involvement of its recipients,
- the intensity of repetition of the desired content by sources considered reliable,
- reference to the general state of consciousness being common knowledge,
- inconsistency in the counter-narrative of the defending side.

For example, the democratic structure of public debate that characterises Western societies and political systems means that those who govern and those who are governed essentially draw on the same sources of information. Both parties also accept as a natural thing the permanent presence of messages other than their own in the information space. Thus, false information may not only be tolerated there, but due to the political culture, it may be relatively easily to gain the status of equal positions in the public debate. This places the beneficiaries of offensive disinformation narratives in a privileged position to influence the state of consciousness and decision-making processes in Western societies.

A different example in this respect is Russia (also China, which is imitating it), as it is one of the states that most aggressively uses disinformation operations in its foreign policy against Western countries nowadays. Russia strongly aspires to protect—and is quite effective in controlling—information dissemination within its territory (although, unlike in the Soviet era, it is no longer a monopolist state). It does so through legal solutions that penalise hostile information activities, the ownership structures

of media (limiting the participation of Western entities), state propaganda in media, and control of the internet[23] and educational programmes in schools.[24] This limits the flow of external content and keeps Russian public opinion within the influence of government political narratives developed in the spirit of a specific and controlled exposition of national interests.

Building on the obviousness of Russians' perception of their own difference from the Western world, little space is left here for external content, justifying "patriotic intensification" and the need to mobilise around the goals set by the state authorities.[25] The Russian side shows not only initiative but also an advantage in terms of the intensity of the measures used. Finally, it has the support of the state apparatus, its secret services, business, and agents of influence. All this increases the potential effectiveness of the applied measures, regardless of the adopted standard of success, such as having a beneficial influence on decision-making processes or "only" gaining penetration of the prepared information into the consciousness of Western societies, undermining their confidence in their own sources of information, authorities, and institutions, which as a result increases their susceptibility to the Russian (state) point of view. This is sometimes achieved by reaching selected people and communities directly, or by using traditional media, expert debates, or social media.

[23] A. Legucka, "The Future of Russia's Sovereign Internet," *PISM Bulletin*, no 67 (1763), 29 March 2021, www.pism.pl/publications/The_Future_of_Russias_Sovereign_Internet (accessed 20.9.2022).

[24] K. Giles, *Handbook of Russian information warfare*, NATO Defence College, "Fellowship Monograph" 9, Rome 2016, pp. 27-30, www.researchgate.net/publication/313423985_Handbook_of_Russian_Information_Warfare (accessed 1.12. 2022).

[25] See: M. van Herpen, *Putin's propaganda machine. Soft power and Russian foreign policy*, Rowman & Littlefield Publishers, London 2015; R. Diresta, S. Grossman, *Potemkin pages and personas: assessing GRU online operations 2014-2019*, Stanford University, Stanford 2019.

"Safety and Security" of the User and Information Producer

Whenever we receive information that causes us to worry or arouses other intense emotions, it is worth waiting and calming down, sourcing this information in other media, looking for the original source. Don't get carried away and don't share such provoking information on social media or in messages to loved ones. It's also good to get out of your information bubble, talk to people with different views and reach for verified, recognised sources. Knowing that someone may by trying to misinform you on purpose for gain is crucial to awareness. I know from my experience as a reporter that a good test—not only in the case of contact with fake news—is to ask yourself the question, "Am I really right? Where else can I check it?"[26]

Combatting Disinformation

Effectively combating disinformation is problematic for democracies—even before touching upon the issues of detection and response—because of their political and legal systems. This is because they not only encourage pluralism of media and the dissemination of information but they also actively defend these practices. In addition, they enjoy broad social consent, strengthened by decades of immersion in a culture of freedom, tolerance, and free choice. Disinformation actors take advantage of the cover provided by open societies and the inconsistency in the actions of media operators.

The same environment forces information verifiers and institutions specialising in combating disinformation to engage

[26] B. Biel, B. Grysiak, "Musimy odkłamywać fake newsy," *Rzeczpospolita*, 15 November 2020.

in seemingly endless, rarely conclusive discussions about the boundaries between the right to opinion (freedom of speech) and deliberate disinformation, the ability to distinguish the transmitter of disinformation from its source, or the intentions accompanying activities in the disinformation space. Legitimate action for security or to protect civil liberties while combating disinformation must be separated from restrictions on media freedom or overt censorship, although the line is not always perceptible.

Even if such protections are disregarded, there are technical questions about how to successfully detect disinformation, gather evidence of it, identify the perpetrator, and remedy the damage. Each of these phases of the counter-disinformation process creates a new problem, which right from the start often means a late reaction to the perpetrator's action and risks the rapid spread of false information. There is also the question of who—state authorities and services, media using technological internet traffic filters, social organisations, activists—has the ability and right to counter disinformation, to what extent, and in what areas (e.g., education)? And, are all these entities capable of the task and should they cooperate with each other?

Apart from the need for states and societies to realise the inevitability of coexisting with information anomalies, the effectiveness of combating them should be based on two factors:

- prevention, particularly through social media education, to develop the capability to generate critical attitudes in recipients of information from an early age, build habits of checking credibility, and enhance skills in this area, and thus instil far-reaching resistance to threats arising from such anomalies,
- response strategies and procedures aimed at removing disinformation from the infosphere and correcting adulterated content. The technology that supports disinformation actors can in this case also serve to combat their activities (blocking

and filtering specific content, machine recognition of disinformation, etc.).[27]

How to combat disinformation more effectively[28]
Technology companies:
– Create international advisory mechanisms based on cooperation and the exchange of good practices. – Create standards for machine content creation.
– Eliminate financial incentives that favour disinformation (linking "click-through" content to profit). – Improve internet misinformation detection-and-elimination tools. – Develop fact-checking and information-producer verification tools.
Governments:
– Cooperate in the field of detection and mapping of disinformation threats. – Regulate internet content management (transparency, financing, technology). – Support public media, research, and education. – Support the technological education of societies and develop an awareness of threats in cyberspace.

[27] R. Kupiecki, T. Chłoń, "Sztuczna inteligencja: miecz i tarcza (dez) informacji," *ITWiz*, 2021, no 3(33), www.researchgate.net/publication/351884003_Robert_Kupiecki_Tomasz_Chlon_Sztuczna_inteligencja_miecz_i_tarcza_dezinformacji_ITWiz_2021_nr_3_33 (accessed 15.10.2022).

[28] Selected recommendations of the report prepared under the auspices of the Council of Europe, for more, see: C. Wardle, H. Derakhshan, *Information Disorder. Toward an interdisciplinary framework for research and policymaking*, Council of Europe, Strasbourg, October 2017, pp. 80–85, www.firstdraftnews.org/latest/coe-report (accessed 1.12.2022).

Media:
– Cooperate and implement common standards of information space management. – Implement ethical standards of media work. – Unmask and remove fraudulent content and its producers. – Improve the quality of information and message titles . – Educate recipients of information.
Civil Society:
– Develop public education and research on information threats and new media. – Develop new standards of general and vocational education corresponding to the pace of social development. Fairly mediate between producers and users of information.

Some Conclusions about Disinformation

The pervasiveness of disinformation (and hostile social influence techniques) is a global threat to individuals, states, their economies, and political systems. Democratisation in the area of access to information, based on technological advances and new media (social media), not only has multiplied social interactions but also geometrically increased the amount of information introduced into global circulation, and with it the temptation of information operations based on disinformation.[29]

[29] The rapid expansion of social media changed the balance of power in the information sphere. Traditional media has lost its importance and is slowly moving its activities to the web. Currently, information can be published by anyone—a professional journalist, "publicist, or citizen whistle-blower convinced of his mission", blogger or influencer using social media. Internet users are not only recipients of messages, but they can have an unlimited and

In this context, there is even talk of a "global information pandemic" ("infodemic"), "global information pollution", or information disorder, having a fundamentally different nature than the cases of disinformation known from history. In the modern world, "contaminated information" ceases to be an anomaly and becomes a common phenomenon. It coexists with reliable knowledge based on verified and true information. It even creates its own "bubbles" gathering recipients who are convinced, for example, about the harmfulness of universal vaccination, the flatness of the globe, the existence of global conspiracies, secret groups governing global politics, etc. Such self-replicating "(dis) information bubbles" may have a local or global dimension, depending on the topic.

The ongoing technological revolution resulting in an increase in the computing power of individual computers and system-level solutions enhanced by various applications of degrees of Artificial intelligence (AI) will create new possibilities in the future for both disinformation activities and methods of combating them. AI, which "feeds" on large datasets, will challenge the protection of information and data-processing systems, privacy, and security of data that people unknowingly direct to networks and trusted institutions every day. However, a particular threat concerns an object given human identity, including image, voice, location, intention, output, and created reputation (falsification), which can be used in the broader sense in a campaign of deliberate disinformation. Techniques of this kind, such as "deepfake", carry criminal risk if used to commit a crime, as well as political risk, where the target could be a leader of a state whose identity is fabricated to, for example, seem to utter words that delegitimise their leadership or raise a threat to peace. In this respect, AI gives

direct influence on their creation and spread, e.g., by sharing or commenting on the content of their choice.

possibilities to surpass the currently available entertainment applications to allow a user (or disinformation actor) to recreate anyone, anywhere, and in any manner.[30]

[30] R. Kupiecki, "Sztuczna inteligencja a bezpieczeństwo międzynarodowe w przyszłości," [in:] R. Kuźniar, A. Bieńczyk-Missala, P. Grzebyk, R. Kupiecki, M. Madej, K. Pronińska, A. Szeptycki, P. Śledź, M. Tabor, A. Wojciuk, *Bezpieczeństwo międzynarodowe*, Wyd. Naukowe Scholar, Warszawa 2020, pp. 472–497.

TOMASZ CHŁOŃ
Ambassador (ret.)

KRZYSZTOF KOZŁOWSKI
Institute of International Studies, Warsaw School of Economics
ORCID: 0000-0003-2886-8277

Selected Case Studies of Systemic Disinformation: Russia and China

Time will tell if recent years go down in the history of disinformation in international relations as a turning point and to what extent the experience with the COVID-19 pandemic perpetuated China's behaviour as an actor that had been increasingly using disinformation against other states. One thing is clear now, though: the crises related to the pandemic have led to a rather unprecedented correlation between Russia's and China's communication strategies, providing an impulse to strengthen propaganda and media cooperation between them. In the case of this particular partnership, Russia secured an ally in its opportunist disinformation offensive, while China gained a defender against allegations that it intentionally initiated the pandemic. This

partnership has also proven to be durable and visible throughout the course of Russia's war against Ukraine.

Nevertheless, despite the specific similarities in the goals and methods of disinformation on the part of these two countries and despite the combination of their efforts and activities, observers, analysts, and communication practitioners in the West must consider the quite significant differences regarding the actions of the two countries. This applies to both their current and long-term goals and the methods they use.

Russia is behind the absolute majority of disinformation and media influence operations in the world. China has relatively recently started to duplicate the patterns of aggressive disinformation along the lines of the Russian practices. In an assessment of China's efforts, it can be said that the country is still learning this style of communication. Russia is more assertive towards the West and assumes that fear is a reliable method of gaining respect on its part. China is more reactive, and therefore creating international recognition in its vision is less about causing fear and more about building admiration for and recognition of its achievements.

Both countries strive to transform the existing international order in a way that strengthens their role at the expense of the current global leaders and the principles on which the international order is based. Russia seems to accept the prospect of chaos accompanying the possible—albeit very unlikely—collapse of Western communities, while China prefers a gradual change.

This difference is enhanced by the asymmetry of resources and, consequently, Russia's preference for the use of corruption vis-à-vis foreign countries—for Russia, it is primarily political, and on the Chinese part, economic. At the same time, China is closed for information purposes, and its authorities are striving to fully control the communication space. Russia, on the other hand, despite ever stricter control of its own infosphere, nevertheless still fights to control the minds of its own people.

Beijing's clear ambition is to rewrite the history of the 2020 pandemic to ignore its origins in China, which has a much more long-term significance. Its disinformation activity is aimed not only at rebuilding the tarnished international image of the country, but most of all the related "soft power" as an instrument for the realisation of political and economic interests.

Russian Smoke Screen: Conceal Your Actions and Confuse Your Opponents

Russia is regarded as an infamous perpetrator of the vast majority of identified and described activities of systemic disinformation targeting other countries. Is it because of its "wounded soul" and lack of acceptance of the fall of its empire? How does a disappointed partner (in Russia's own story, failed by the West) look for compensation from a failed relationship?[1] Or finally maybe just because it can act "like a village bully, she wants to show the world that she is able to do whatever she wants"?[2]

The Causes of Disinformation

In fact, there are many reasons and causes for disinformation, as well as a sufficiently long tradition of similar activities, described in numerous studies.[3] In the opinion of this writer,

[1] About the myth of "Russia's betrayal by the West", see: R. Kupiecki, "The Founding Myth of Russian Foreign Policy", [in:] A. Legucka, R. Kupiecki (eds.), *Disinformation, Narratives and Memory Politics in Russia and Belarus*, Routledge, London 2022, pp. 43–58.

[2] This is what Andrei Illarionov, in the past a close advisor to Putin, thinks in an interview with Jessikka Aro, see: J. Aro, *Trolle Putina*, Wydawnictwo SQN, Kraków 2020, p. 16.

[3] See: M. Domańska, "The myth of the Great Patriotic War as a tool of the Kremlin's great power policy," *OSW Commentary*, www.osw.waw.pl/en/publikacje/osw-commentary/2019-12-31/myth-great-patriotic-war-a-tool-kremlins-great-power-policy (accessed 6.12.2022).

one of the contemporary reasons for disinformation is also the conflation by a small group of Russia's current rulers of their own interests, including the gigantic business benefits unimaginable for an ordinary Russian, with national interests. This and other motivations have unfortunately led to a complete loss of scruples and restraint in this group to the point of falsifying reality for the purposes of material gain and politics. It creates a toxic smokescreen around the perception and understanding of one's surroundings that confuses and blinds both these elites and the majority of their country's citizens, and sometimes, unfortunately, also the public in other countries.

Several lessons about the intentions of this group in its international relations include the events in Estonia in 2007 concerning the relocation of a monument of a Soviet soldier (the so-called Bronze Soldier) from the centre of the capital to a Tallinn cemetery, and above all the war in Georgia in 2008. However, as it turned out, these lessons were insufficient for the West.

Disinformation, or more broadly manipulating information, in a holistic hybrid dimension, which, along with cybernetic elements, include special operations, even those up to the threshold of direct military actions, and political corruption, is often and in fact incorrectly (e.g., M. Galeotti) referred to as the "Gerasimov doctrine".[4] In fact, the Russian chief of the General Staff, in a short speech published in a niche periodical,[5] characterised the actions of not Russia, but, in his opinion, the West, which through "colour" revolutions aimed to gain new footholds for itself without firing a single shot. It was enough for the West to

[4] Galeotti himself admitted that he was too rushed in applying the name, www.inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war (accessed 12.12.2022).

[5] The general did not, of course, go to the trouble of analysing their real causes, www.vpk-news.ru/sites/default/files/pdf/VPK_08_476.pdf (accessed 12.12.2022).

control human emotions and, consequently, actions. According to Gerasimov, Russia should respond to the West with the same. One can, therefore, imagine the chief of the General Staff of the Armed Forces of the Russian Federation in a command office poring over a map of the globe with the largest territorial state in its centre, and another commander from an era 25 centuries removed, prominently juxtaposed proclaiming that the greatest achievement is defeating the enemy without engaging in battle.

Thus, disinformation and wider hybrid activities have now been raised by Russia to the level of war waged by other methods, especially because, given the asymmetric economic potentials, it is much cheaper.

Disinformation: Goals, Methods, and Means

Russia is developing and constantly adapting its arsenal of what it calls "active" (in fact hybrid) activities, the genesis of which is outlined by Robert Kupiecki in the first part of this book. In their set, the leading role in the practical manipulation of information and its dissemination was entrusted to the press concern Rossiya Segodnya,[6] with its foreign direct or indirect subsidiaries RT (formerly Russia Today) and Sputnik.[7] It has been provided with a budget larger than the budget of the Polish Ministry of Foreign Affairs and has been legally established as a state-owned enterprise of strategic importance. Crypto-centres have been created for illegal operations on the internet, with the infamous Internet

[6] J. Godzimirski, M. Østevik, "How to understand and deal with Russian strategic communication measures?", *Policy Brief*, 1/2018, [NUPI] www.nupi.no/en/news/how-to-understand-and-deal-with-russian-strategic-communication-in-europe (accessed 20.12.2022).

[7] M. L. Richter, "What We Know about RT (Russia Today)," *European Values*, Prague, 10 September 2017, www.europeanvalues.net/wp-content/uploads/2017/09/What-We-Know-about-RT-Russia-Today-1.pdf (accessed 17.12.2022).

Research Agency (IRA)[8] at the helm, and pseudo-independent press agencies and media, including foreign ones under their influence or control. Examples include the Baltnews portals, operating in the Baltic States under the ineptly concealed control of Rossiya Segodnya[9], or the Federal News Agency associated with IRA. Sputnik has more than 30 language versions, and their range indicates geographic, or rather geopolitical priorities. Traditional, online, and social media connected in this way make it possible to control the flow of (dis)information, as well as to introduce it more or less effectively into local mass media. As a result, this relationship has given Russian-controlled disinformation influence in social and political processes, such as election campaigns abroad, which was demonstrated by the U.S. presidential elections in 2016 or in France in 2017, respectively, as well as subsequent elections in number of other countries.

In addition to state media, supported by other state authorities and services, or media controlled by the state in various ways, most often by political and financial ties, other professional groups also are involved in the implementation of disinformation activities. This applies, for example, to some scientific circles, networks of social organisations financed or otherwise supported by the state, businesses subordinated to the Kremlin, and the Orthodox Church.

The intentions of Russia towards the local "victims" of its propaganda and disinformation are clearly diversified, but they have one main goal: to rebuild the existing international order in

[8] J.C. Wong, "Russian agency created fake left-wing news outlet with fictional editors, Facebook says," *The Guardian*, www.theguardian.com/technology/2020/sep/01/facebook-russia-internet-research-agency-fake-news (accessed 6.12.2022).

[9] "Russia propaganda campaign revealed in Baltic state," The National, www.thenationalnews.com/world/europe/russia-propaganda-campaign-revealed-in-baltic-state-1.765040 (accessed 4.12.2022).

a revision of its post-Cold War foundations and the revanchist-driven push to restore Russia to the role of a global super-decision maker and arbiter deciding the fate of other countries in an elite concert of the greatest powers. Most strategic communication operations around the world serving this purpose have certain common features in terms of intention, namely:

- causing a sense of threat, fear, and chaos, if not conflict, in the internal relations of states and their international relations;[10]
- undermining trust in democratically elected governments and their policies;
- creating doubts in matters of key importance to national, social, and economic security;
- undermining faith in oneself, one's own potential, credibility towards allies, international organisations, especially NATO or the European Union;
- dividing and polarising society;
- discrediting groups and people critical of Russia;
- creating and promoting pro-Kremlin circles; and,
- influencing the sovereign decisions of states to suit the best possible interests of Russia.

A responsible, thinking citizen and voter in these countries is undesirable from the Russian elite's point of view—instead, the voter is a soldier on a modern battlefield who must be defeated if not recruited to your side. In its disinformation actions and operations of influence, Russia refers primarily to feelings and

[10] Sputnik regularly warns of World War III. Russian media, which are engaging both the local and international public, fill their time with news on military manoeuvres, exercises, and tests of new models of weapons while the state authorities attempt to cover the true situation with statements on the unmatched military capability of the Russian Federation. At the same time, according to the World Bank in 2019, Russia's share of the global GDP was just 1.42% and decreasing, with a simultaneous increase in social problems.

emotions, exploiting them against the background of nationalisms and all other negative "-isms", including chauvinism, racism, and radicalism (the list is much longer). For this, it uses the fertile soil of religion, xenophobia, migration, economic inequalities, and social controversies such as vaccinate mandates or the right to possess firearms. By the way, most of these phenomena can be easily identified in Russia's own historical experiences. In this paradigm, rationality is the enemy while emotionality and ignorance are allies.

According to *The New York Times*, a manipulated or deceptive administrator or performer of such operations must obey the following seven "commandments": seek divisions, create a lie, wrap them in the appearance of facts, hide your actions, find a useful idiot, deny everything, and play the game in the long term.[11]

Seven Commandments of Disinformation	
Seek divisions in society	Find a useful idiot
Create a Big Lie	Deny everything
Make the Big Lie look like truth	Think long-term
Hide your actions	

Own work based on an article in The New York Times. [12]

Concealment or denial is often accompanied by mockery, but in the zeal to discredit imaginary enemies, humour—a potentially phenomenal instrument for this—most often turns into its own caricature. How else to assess the post by the spokeswoman for the Russian Ministry of Foreign Affairs, Maria Zakharova, on a social

[11] "Seven commandments of fake news," EUvsDisinfo, www.euvsdisinfo.eu/seven-commandments-of-fake-news-new-york-times-exposes-kremlins-methods (accessed 11.12.2022).

[12] *Ibidem*.

networking site in response to a Polish official: "Be afraid of God, Stanisław. As many lies and dirt as Polish politicians poured towards Russia, it would be enough to pollinate the orchards of Paradise", she wrote on Facebook.[13]

Kremlin propaganda diversifies its messages and the methods of conveying them depending on the targeted groups and situations.[14] Younger generations are usually targeted abroad and all kinds of opportunities and emerging crises are used to deepen social divisions and escalate conflicts. This is the case with COVID-19 pandemic, in which, for example, the North Atlantic Alliance was portrayed in Russia's messaging as an organisation that was not only useless but even harmful to the societies of its member states as having allegedly exposed them to an increase in infections due to military exercises. The NATO Defense College assessed these

[13] "Bój się Boga!" Rosja znowu atakuje Polskę", www.o2.pl/informacje/boj-sie-boga-rosja-znowu-atakuje-polske-6575931656727520a (accessed 10.12.2022).

[14] Internal disinformation is not the main subject of these considerations, but it is worth noting that the Kremlin, with almost full control of the information space, criticises the West constantly to millions of Russians, most of whom still learn about the world from state-controlled television channels. In its messaging, democratic states, i.e., the West, are presented as degenerate, anarchist, ruled by a corrupt and unscrupulous establishment, torn by internal conflicts, aggressive towards Russia. The effectiveness of Russian propaganda is evidenced by the fact that only 3% of Russians believe that the Skripals were poisoned by the Russians. As many as 28% think it was the British who attacked them. Rbc.ru, "Только 3% россиян связали отравление Скрипалей с российскими спецслужбами," 25 October 2018, www.rbc.ru/politics/25/10/2018/5bd088539a794762be18d9af?from=main (accessed 10.12.2022). Moreover, according to Denis Volkov, a sociologist with the Levada Center (one of the last independent sociological research centres in Russia), many ordinary Russians are eager to spread official propaganda because they simply want to participate in a conflict with the West. D. Volkov, Carnegie.ru, "Отравили – ну и что? Верят ли в России, что Москва ни во что не вмешивалась", www.carnegie.ru/commentary/77678?fbclid=IwAR1LZgM-muuTHO_7WTOZcMKK9eEAmlsSP-vzttGZ09u_QFiaNMddpdX-Eso (accessed 10.12.2022).

Russian actions as not without negative effects on the image of the Alliance, especially in the European countries most affected by the virus in the first phase of the pandemic, such as Italy.[15]

Although researchers and commentators differ in their assessments of the effectiveness of pro-Kremlin propaganda abroad, its effects can be decisive in situations where the results may be determined by a small group of voters voting for one side or another, or due to the absence of people discouraged from participating in the elections.

Selected States as Objects of Disinformation

Let us take a closer look at the examples of Russian disinformation targeting Poland and, briefly, some other countries close to it either geographically or as allies.

Poland

Since 2014, due to the deep degradation of relations with the West after Russia's aggression against Ukraine and the illegal annexation of Crimea, Poland has become one of the main targets of Russian information manipulation. These actions have assumed unprecedented scale and form, especially in the dimension of historical politics. In fact, we are dealing with a special operation in which Poland is presented by Russia as not one of the victims of World War II but as almost an accomplice in its start, and this defamatory campaign is led by the head of state.

Its causes and goals are presented by Maria Domańska from the Centre for Eastern Studies in Warsaw, pointing to the context of Russian efforts to weaken Euro-Atlantic communities and its

[15] A. Monaghan, "Russian Grand Strategy and the COVID crisis," *NDC Policy Brief*, December 2020, no 22, www.ndc.nato.int/research/research.php?icode=6 (accessed 20.12.2022).

individual members.[16] Someone will ask what is the connection between history and the present here? What does something as shameful as the ongoing rehabilitation of Stalinism and the retouching of Stalin's and Hitler's cooperation in Russia have to do with today's NATO and the European Union? Why stigmatise in parallel the pre-war governments of other countries as alleged allies of Nazi Germany? Are these assertions not limited only to the matters of internal propaganda and social consolidation around certain historical facts and myths?

Well, not only. In this "world of performances" built on Russian lies, the claim of "Poland as Hitler's ally" can justify Moscow's present security concerns and weaken an important member of the community of states that Russia is deliberately portraying as a modern enemy. In Moscow's narrative, since Poles betrayed others in the past (e.g., Czechoslovakia in 1938), what is the guarantee that they will not do it again sometime. No matter how outrageous or abstract it may sound in Poland, such observations may evoke some resonance abroad. And in this Russian historical narrative, it is important to create the context for current operational activities. This also applies to disinformation measures which, using dedicated social networks, prepared fake news or manipulated reports, or even forged documents, will add a contemporary point of continuation to these "historical sins".

For example, the news bulletin below by Radio Sławenia ("Aktualności Pilne 05.11.7528r. w Radio Sławenia", "Urgent news November 5, 7528. in Radio Sławenia")[17], contains the absurd theme of "Poland's superpower ambitions" and "claims" to the historic Polish territories of present-day Belarus:

[16] M. Domańska, "The myth of the Great Patriotic War ..., *op. cit*.

[17] "Aktualności Pilne 05.11.7528 r. w Radio Sławenia," https://youtu.be/RO_XjTQBaso (accessed 6.12.2022).

This programme could seem like a silly joke or satire, but it is not, because of the media reach of the broadcaster. Considering its embarrassing intellectual quality, it is a wonder how the author even managed to promote himself among his hundreds of thousands of internet followers.

Less satirical, however, are media headlines that "members of parliament believe that a permanent U.S. base in Poland will mean the loss of some sovereignty" (a reference to one independent MP), or a (fake) "interview" with a Polish general criticising the presence of U.S. military in Poland, or systematic attempts to discredit the deployment of NATO battalion battlegroups and allied military exercises in Poland.

The pro-Kremlin media and trolls naturally aim more broadly and target other spheres of key importance to state security, such as the energy sector, reaching the mainstream of Polish media with their message, and the Polish authorities and the Embassy of the Republic of Poland in Moscow cannot complain about the lack of work in counteracting disinformation.

Against this background, discussion may arise about the conviction that in the case of Poland, Russia should recognise that attempts to undermine Poles' Euro-Atlantic aspirations and their allied credibility are doomed to failure. It is impossible

to undermine the very high support among Poles for Poland's membership of NATO and the EU and to lie about the tragic experiences of Poland during World War II, millions of victims, and the military contribution of Poles to the final defeat of Nazi Germany. It turns out, however, that Russia not only will not stop these efforts but also intensifies them, which is puzzling because just like in other countries also in Poland it finds opinion-forming, so-called useful idiots for this purpose.

The Polish example then shows clearly that Russia is engaged in a "long-term" game of undermining an understanding crucial for the functioning of states and societies, specifically the sense of identity and political stability, security, and credibility. Thanks to journalistic investigations, new light has been shed on Russia's Belarusian-backed activities in Poland that combine information manipulation with hybrid attacks, including cyber-intrusions and political corruption. In particular, this is evidenced by the wiretapping affair that targeted politicians of the ruling coalition of the Civic Platform and the Polish People's Party in 2014,[18] as well as the illegal extraction of email from the Head of the Prime Minister's Office Michał Dworczyk's, which were strategically released to the public throughout 2021 and 2022[19].

Estonia, Lithuania, and Latvia

As with Poland, Russia is seeking to discredit other democratically elected governments using all available means. In

[18] A. Krzysztoszek, "Tapes that caused 2014 Polish government crisis were allegedly sold to Russia," *Euroactiv*, www.euractiv.com/section/all/short_news/tapes-that-caused-2014-polish-government-crisis-were-allegedly-sold-to-russia (accessed 22.10.2022).

[19] W. Czuchnowski, "Polish Authorities Ignored Early Warnings of Cyber Attacks on Government Officials," *Gazeta Wyborcza*, https://wyborcza.pl/7,173236,27247035,polish-authorities-ignored-early-reports-of-cyber-attacks-on.html (accessed 22.10.2022).

the case of Estonia, Lithuania, and Latvia, Russia incorporates an ethnic element into the "cluster" of historical and Euro-Atlantic narratives. In extreme pronouncements, it denies the permanence of the statehood of what it calls the "troika" and does not admit to over a half-century of Soviet occupation, trying to convince the world that the Baltic states voluntarily became part of the USSR. Russia presents the Baltic states as weak structures where governments, instead of focusing on social care in the standard of living, use limited resources to defend themselves against an imaginary enemy (Russia).

Estonia and Latvia, which are inhabited by a large group of ethnic Russians (about 25% of the total population), are attacked for allegedly discriminating against the Russian minority in the local labour market and education system. This message is focused on key spheres of life for people in which the authorities are supposedly trying to harm Russians.

Lithuania is accused not only of having an inefficient government leading to the depopulation of the country, but, as in the case of the other Baltic states, of surrendering to "occupation by NATO".[20] Additional accusations include supporting terror in Belarus or surrendering sovereignty under pressure from Finland and Sweden over, for example, the Ostrowiec nuclear power plant in Belarus, and even of declaring a hybrid war on Russia.

[20] The Baltic states (and Poland) are in the crosshairs due to the presence of NATO battalion groups. However, media disseminating content directed against these countries on the national market often do so also for purely commercial purposes as this content, unfortunately, sells well. See: Atlantic Council's Digital Forensic Lab, "Propaganda for profit targets the Baltic states on YouTube. Fringe YouTube channels monetise pro-Kremlin narratives about the Baltic states," (via *Medium*), www.medium.com/dfrlab/propaganda-for-profit-targets-the-baltic-states-on-youtube-b8bf78c32d78 (accessed 7.12.2022).

Ukraine

If according to Moscow the Baltic states have weak and inept governments, and even doubtful state credibility, Ukraine is directly presented as an artificial creation that should not be a state at all because the Russians and Ukrainians are one nation. Russian disinformation operators emphasise that Ukraine is used by the West and betrayed their East Slavic brother through an "illegal coup" (Maidan). As a result of this alleged coup, neo-fascists and nationalists came to power, which harm Russians living in Ukraine and violate their social, economic, and cultural rights, in addition to their rudimentary needs. Under the post-Maidan government, Ukraine is portrayed as having become a vassal of the West, especially of the United States, which were allowed to, among other claims, set up biological weapons laboratories on its territory and given permission to use Ukrainian citizens in secret American experiments to test the vaccines against the coronavirus.[21] The information war and limited conflict in the Donbas eventually culminated in the full-scale Russian invasion of Ukraine in February 2022, which has been combined with Goebbels-style propaganda towards foreign audiences and for domestic purposes.

Finland and Sweden

In the eyes of the Kremlin, Finland and Sweden are guilty of rapprochement and maintaining a far-reaching civilian and military cooperation with NATO, which finally led to their applications for NATO membership following Russia's invasion of

[21] Ukraine is a case that deserves a separate and more detailed discussion due to the scale of its experience with disinformation. Naturally, it has extensive expertise in the field of defence against it. Together with NATO, as part of one of the partner programmes, Ukraine has created a so-called hybrid platform that is, among others, a place for exchanging experiences and practical cooperation.

Ukraine. Therefore, according to the Russian line, they deserve an exemplary stigma applied with the use of specific preventive (dis) information pointing to the potential political and economic costs of strengthening their pro-NATO orientation. This preventive information targets the mainstream Nordic parties, exploiting sensitive issues not only relating strictly to defence policy but also to migration, sovereignty (hence these sources' support for anti-EU sentiments) or ethnic issues (discrimination against Russians in Finland). This is accompanied by hybrid activities *par excellence*, including the acquisition of real estate in the Finnish archipelago and the construction of paramilitary infrastructure on it.[22]

Finland is also a peculiar case of an aggressive Russian historical narrative that creates a certain dissonance with fairly correct before its application to join NATO interstate relations against the background of Russia's general relations with the West. An example of a kind of patriotic policy carried out in this way and, at the same time, of educating young Russian generations is the opening in 2020 in Karelia, on the border with Finland, of a "Finnish concentration camp" museum, reconstructing the conditions in which Finns imprisoned Russian prisoners during World War II. The target of this project are the students who come to this place on group visits from all over Russia as part of "history" lessons. Today, no one is surprised why schoolchildren in Russia are not included in the obligatory programme of visits to Soviet gulags, nor what experiences form their educational basis for patriotism.[23]

[22] A. Higgins, "Finnish soldiers find 'secret Russian military bases' after raiding mysterious island," *The Independent*, www.independent.co.uk/news/world/europe/finland-russia-military-bases-sakkiluoto-putin-dmitry-medvedev-police-a8612161.html (accessed 5.12.2022).

[23] "Russia Builds Replica WWII Prison Camp for Kids," *The Moscow Times*, www.themoscowtimes.com/2020/11/13/russia-builds-replica-wwii-prison-camp-for-kids-a72035 (accessed 11.12.2022).

Sweden is also an interesting case of adaptation of Russian media activity abroad. Sputnik went out of business there when the Russian decision-makers, who usually have a generally high tolerance of costs, deemed it ineffective. Instead, they bought six local Swedish internet portals.[24]

Slovakia, Czechia, Hungary

In the context of disinformation, the Visegrad Four (V4) does not exist as a coherent object of Russia's actions. First, none of the other countries is under attack like Poland. The second difference consists of the cyclical, sometimes "surgical", dosing of propaganda towards selected recipients. Certain political forces in the V4 become the subject of disinformation in response to unfavourable political processes or actions considered by Russia as hostile.

After the elections in Slovakia in 2020, a coalition that was more critical of Russian foreign and security policy than its predecessors took over. At the same time, the president, Zuzana Čaputová, a liberal politician, exercises her mandate by often referring to the democratic values on which the European Union and the North Atlantic Alliance are based. Consequently, Slovakia has for some time been the target of increased criticism from Moscow and disinformation activities related to the COVID-19 pandemic. It must be admitted, however, that Russia is able, in a less aggressive way and through its genuine presence in the Slovak mainstream media space, to count on a considerable level of sympathy among Slovaks, still rooted in the Pan-Slavic tradition.

In the case of Czechia, diplomatic scandals involving Russia and the decision of the Prague authorities to move a monument to a Soviet general, Russia reacted with a wave of harsh media

[24] J. Rudolph, T. Morley, "Covert Foreign Money: Financial Loopholes Exploited by Authoritarians to Fund Political Interference in Democracies," Alliance for Securing Democracy, German Marshal Fund of the United States, www.securingdemocracy.gmfus.org/covert-foreign-money (accessed 15.12.2022).

criticism, accusations, and provocations. However, tensions with Czechia have been fairly consistently eased through, among others, the participation of former and present representatives of the highest authorities, especially presidents Vaclav Klaus and Milos Zeman.

In Hungary, on the other hand, Russia is trying to maximise its political and economic influence by using the mainstream media there, where they are more open to presenting Russian narratives than the mass media in Czechia and Slovakia.[25]

The Netherlands

Ever since Malaysia Airlines Flight 17 (MH17) was shot down in 2014, Russia has continually tested the patience of public opinion in the Netherlands and internationally as it defends itself against charges of perpetration. It seems that today these activities have hurt Russia more than helped it, particularly since Dutch investigators and prosecutors presented conclusive evidence against it in court. Questioning the evidence causes widespread frustration, anger, and outrage. Russian policymakers must realise that this tactic of negation is double-edged; nevertheless, it exemplifies the ironclad rule of Russia's hybrid action—admit nothing.

However, Russia is playing a long-term game with the Dutch because of their membership, activity and diplomacy in the European Union and NATO, as well as the tendency of the Dutch to conduct open and critical debate, also towards friendly countries. Given the Netherlands' tradition of examining things in depth, including against their potential economic consequences, these debates can lead to unpredictable results. This was the case with the EU-Ukraine Association Agreement vetoed by The Hague, in effect as

[25] D. Bartha, "Countering Disinformation at Home. Tools to combat state-controlled amplifiers," *Visegrad Insight*, www.visegradinsight.eu/disinformation-home-hungary (accessed 13.12.2022).

a referendum around which Russia carried out prolonged and active lobbying.

Other Countries

The discussion in the United Kingdom and elsewhere on the role played by the Kremlin in Brexit, namely taking advantage of the euroscepticism of the British people, fuelled for years by media, including some owned by Russian oligarchs, will not be over soon. In any case, the UK, even outside the EU, remains one of the most important objects of pro-Kremlin disinformation due to its influence and importance in international relations. The British state became convinced of this after Russian secret services poisoned the former Russian spy Sergei Skripal on its territory. It also observed it in the context of the COVID-19 vaccine research conducted on a competitive basis and having remarkable social, economic, and political importance.

As perceived by the Kremlin, and in its vision to which it wants to convince not only itself but also the international community, the United States is responsible for almost "all evil" in the world, including international crises and even Russian domestic troubles. In the Russian view, the U.S. does not treat Russia as an equal partner, imposes sanctions on it, and *forces* other countries and organisations to take similar steps. Meanwhile, in the same vision, the Americans themselves are torn apart by political and social conflicts and quite systemic crises.

A report prepared in 2018 for the U.S. Senate emphasised that campaigns containing such disinformation are directed at the younger generations of Americans, and that they are "encouraging" propagandists to also reach for topics of pop culture, local events, and happenings, especially social demonstrations or protests.[26]

[26] See, e.g., the Lakhta Project, conducted by the Internet Research Agency (RIA) owned by Yevgeny Prigozhin, an oligarch linked to the Kremlin (who is

Russia naturally denies that media are subordinated to its services, including portals and groups on social forums created in the United States, which eagerly prey on social divisions in the country, and exploit and even inspire conflicts there. Nevertheless, anyone with elementary knowledge about the operation of U.S. institutions and the judiciary is aware that the evidence about Russian interference in U.S. interests and democratic processes presented by the prosecution must be sound.

The list of countries affected by the Russian virus of disinformation and influence operations is naturally much longer. There are reports based on thorough official and journalistic investigations and allegations of Russian interference in the election processes and political life in France and Germany, including through disinformation. In the case of Germany, political trolling observed there recently is a consequence of the country's primarily humanitarian decision to save the life of Russian opposition politician Alexei Navalny, poisoned by Russia's services. Obviously, extremist parties such as Alternative for Germany (AfD) or the National Front in France are supported and used by Russia, also in media. Similar actions support the separatist Five Star Movement in Italy and the secessionist movements in Catalonia, seeking to separate from Spain.

In the Balkans, Russia uses its strong political and media influence, especially in Serbia, but also supports or corrupts local media and even creates groups of individual collaborators (students and young people) to carry out paid social media trolling. This

also credited with funding Russian paramilitary organisations). RIA has at least 1,000 accounts focused on wreaking havoc and escalating emotions on topics such as gun control, mass shootings, gay rights, and women's marches. It had a budget of $35 million ahead of the 2018 U.S. mid-term elections. See: The US Department of Justice, "Russian Project Lakhta Member Charged with Wire Fraud Conspiracy," www.justice.gov/opa/pr/russian-project-lakhta-member-charged-wire-fraud-conspiracy (accessed 9.12.2022).

serves to slow down or even derail the integration of the countries in the region with NATO and the European Union. It also enables the implementation of hybrid operations, including cyber actions against opponents from outside the region.[27] Russia resorted to extreme steps to overthrow the government and remove the Montenegrin prime minister ahead of the referendum on joining NATO. Russia tried to prevent an agreement between Athens and Skopje on the name of the Macedonian state that paved the way for it to join the North Atlantic Alliance and gave new impetus to integration with the European Union.

An "Infopandemic" and What Next

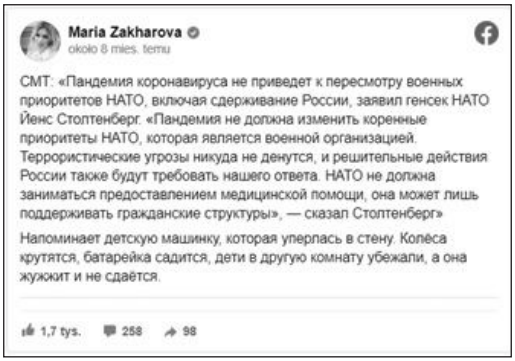
Russia's perverse *carpe diem* of seizing any opportunity has manifested itself in all its nefarious glory as a permanent presence in the COVID-19 pandemic. Italians and Serbs, having received support from Russia in equipment and medical teams, became targets of intrusive indoctrination on the allegedly utter uselessness of organisations like NATO and the EU in the fight against the pandemic.

The aggressive propaganda exploiting the SARS-CoV-2 crisis ultimately has caused Russia more harm than good, but this has not discouraged the creators of this strategy from continuing their efforts with stubbornness worthy of a better cause. The list of their "results" is regularly compiled by EUvsDisinfo, one of the best anti-disinformation teams and websites devoted to tracking the subject in the world.[28] NATO has proved that statements by

[27] I. Stanley-Becker, "Pro-Trump youth group enlists teens in secretive campaign likened to a 'troll farm,' prompting rebuke by Facebook and Twitter," *The Washington Post*, www.washingtonpost.com/politics/turning-point-teens-disinformation-trump/2020/09/15/c84091ae-f20a-11ea-b796-2dd09962649c_story.html (accessed 15.12.2022).

[28] EUvsDisinfo, "EEAS Special Report Update Short Assessment of Narratives and Disinformation around COVID-19 Pandemic (Update May -

the spokeswoman for the Russian Ministry of Foreign Affairs, who likened the organisation to a broken and redundant "toy", are not amusing but pathetic and ineffective.[29]



Given the recent perspective and against the background of countering Russian disinformation by the West and its Euro-Atlantic organisations, it seems reasonable to assess that the latter are emerging relatively unscathed from the ongoing "infopandemic". They strategically demonstrate and communicate the systemic (medical, civil, and military) potential of fighting the pandemic based on the economic and technological advantage of their members over Russia, thus effectively disavowing the Kremlin's actions.

This does not mean that the world has rendered Russia less prone to use disinformation as a non-static (which should be stressed) instrument of international competition. The world has been facing a new reality of information warfare accompanying

November)," www.euvsdisinfo.eu/eeas-special-report-update-short-assessment-of-narratives-and-disinformation-around-the-covid-19-pandemic-update-may-november (accessed 5.12.2022).

[29] "NATO's approach to countering disinformation: a focus on COVID-19," NATO website, www.nato.int/cps/en/natohq/177273.htm (accessed 20.12.2022).

Russia's full-scale and criminal war against the Ukrainian people. Therefore, the transatlantic community must constantly adapt the measures used to torpedo such practices. It will be necessary to intensify practical activities in three areas: media education, unmasking the perpetrators, and implementing regulations, including new laws.

China—the Virtual Chinese Wall, or the Case of the PRC's (Dis)information Policy During the COVID-19 Pandemic

What we see depends on what we are looking at, as well as what we have learned to perceive. In the case of Chinese information policy, it must be recognised that what we are looking at may be something completely different from what Chinese citizens see behind the virtual Chinese wall.[30] An analysis of Chinese information and disinformation policy, which constitutes a kind of war for minds in the narrative of the pandemic, allows us to draw some general conclusions.

First of all, the fundamental goal of Chinese policy is to control information within China itself. While the attention of many observers may be attracted to, for example, Chinese activity on social networks available in Western countries, it is often forgotten

[30] The aim of this part of the study is to outline the main challenges related to disinformation practiced by Chinese public institutions, as well as other entities directly or indirectly representing their political line. Due to the size of the study, most of the conclusions will be based on the analysis of China's information policy related to COVID-19 in 2020, excluding disinformation campaigns regarding, for example, Hong Kong, Tibet, Xinjiang or Taiwan. While the latter provide extensive background material on Chinese disinformation, discussing them would require an introduction to the geopolitical specificity of each of them. In turn, the usefulness of basing the argument on the example of China's information policy regarding COVID-19 is supported by the clear Chinese ambition to rewrite the history of the 2020 pandemic to ignore its origins in the PRC and emphasise subsequent real and perceived successes and assistance to countries particularly affected by the spread of the coronavirus.

that external entities are practically prohibited from activity behind the Chinese virtual wall. This in practice means very significant restrictions on reaching Chinese audiences with content different from the messages dominating their information environment, which are mainly propaganda-conditioned and controlled by the Communist Party of China (CPC).

The effectiveness of the PRC's information policy seems to be correlated with the effectiveness of China's cooperation with the governments of countries whose societies are exposed to Chinese information efforts. However, the official positive image of relations often does not correspond to the realities of interactions in the people-to-people dimension. The effectiveness of China's information policy, however, varies markedly depending on the degree of previous historical exposure of a given society to Chinese information efforts. This is clearly seen in Taiwan, South Korea, and Vietnam's distrust of the first reassuring signals from the PRC regarding COVID-19, following their experiences with similar messages from the SARS epidemic.

The PRC relatively recently began to duplicate patterns of aggressive disinformation similar to the Russian pattern, and judging by their efforts, it can be said that they are just learning this style of communication. However, given the escalation of these activities, they should not be underestimated, especially in the long run.

The Middle Kingdom and the Global Village

Over 50% of the population in China has access to the internet. Unlike Western countries, in China the internet is subject to public control and censorship (as is the entire Chinese media landscape), and popular Western social networking sites are unavailable without a VPN service. As early as 1998, the Chinese authorities implemented the Golden Shield Project, often referred

to as the Great Firewall of China, officially to increase public safety. Under Chinese law, however, it means blocking all content that is inconsistent with the official ideology and political line of the CPC.

The most important consequence of closing the Chinese virtual space to Western social media is the domination of domestic alternatives (often copying Western solutions). Having access to a wide portfolio of services as part of WeChat (approx. 1 billion users), QQ (over 800 million users), or Qzone (over 500 million users), including all functions available on media such as Facebook, Instagram, or Twitter, extended to online payments and VoD services, the Chinese are not even interested in Western social media. This has consequences not only in terms of business communication (in the sense of different channels of communication with the client) or personal communication (maintaining contact with friends from China often requires using Chinese software) but also in the field of information policy.

Reaching a Chinese recipient with a political message that is contradictory or even different from the version promoted and accepted by the state authorities is possible only to a limited extent and in fact is tantamount to breaking Chinese law. This means that in the event of competing versions or interpretations of events inside and outside China, an entity wishing to reach the Chinese audience with its own narrative will be exposed to an unfavourable asymmetry. While the Chinese state will be able to enjoy free access to the internet, e.g., in Western countries, the message from outside to recipients in China may not reach them at all. Thus, the Chinese government is figuratively and literally unrivalled in competition for Chinese public opinion. It can be concluded that in the conditions of a global internet village, the PRC has become a privileged island with access to the world's ocean of opportunities but governed by its own rules within its borders.

Patterns of Chinese information activities with the example of COVID-19

The COVID-19 pandemic allows us to trace the mechanisms of China's information (and disinformation) policy, directed both inside and outside the country.

The initial reaction of mainland Chinese authorities to the detection of the first cases in December 2019 and January 2020 was the introduction of strict censorship. Wuhan administrative authorities, for example, prevented doctors from revealing the threat.[31] Information control has gone so far as to delay the introduction of procedures to prevent the virus from spreading to the rest of China. The situation was worsened by the fact that the first cases in Wuhan fell in the weeks before the Chinese New Year. This is the busiest period during the year in terms of the number of trips around the country as people travel to celebrate the holiday with their families. With the virus spreading beyond Wuhan, the first infections abroad were only a matter of time. However, this did not lead to less censorship of information on this subject. In the official chronology of events, Chinese authorities consistently ignore the above facts, focusing instead on the course of the pandemic outside the PRC.

A general pattern of information dissemination management in Chinese communications directed outside China can be observed.[32] As to formal channels, the Chinese authorities, most often the Ministry of Foreign Affairs, generate messages about the pandemic. These are then repeated in social media by the Chinese

[31] J. Jakóbowski, M. Bogusz, "China's responses to the global COVID-19 pandemic," *OSW Analyses*, www.osw.waw.pl/en/publikacje/analyses/ 2020-03-31/chinas-responses-to-global-covid-19-pandemic (accessed 13.12.2022).

[32] M. Przychodniak, "China's Public Diplomacy on Social Media," *Bulletin PISM*, no 183(1429), 20 December 2019, www.pism.pl/publications/Chinas_Public_Diplomacy_on_Social_Media (accessed 13.12.2022).

diplomatic missions and in English-language party media such as the *People's Daily*. To help authenticate the message and reach a broader group of recipients, diplomatic representatives also try to use local press titles to publish statements from China (for example, *Rzeczpospolita* in Poland).

The message in formal channels is then picked up by social media accounts. Accounts, not users, because some of them are false or automated (bots) with profiles tuned to the local media environment. In August 2019, Twitter closed about 1,000 fake profiles, Facebook closed three groups of users, each with about 15,000 subscribers, and Google has blocked 210 similar channels on YouTube. The number of users associated with them was estimated at several hundred thousand people. A year later, there was an upward trend in this regard.[33]

These communication procedures were accompanied by "face mask" policy: medical supplies were given to countries affected by the pandemic, offered both commercially and free of charge.[34] The policy is particularly positively perceived in developing countries or those particularly acutely hit by the pandemic. Countries that have recently been cooperating with China on a larger scale seem to be more susceptible to Chinese information efforts (even in Europe there has been a relative improvement in the image of China, e.g., in Serbia and Italy).[35]

[33] "Twitter deletes 170000 accounts linked to China influence campaign," *The Guardian*, www.theguardian.com/technology/2020/jun/12/twitter-deletes-170000-accounts-linked-to-china-influence-campaign (accessed 13.12.2022).

[34] J. Jakóbowski, "Chinese medical equipment supplies to Europe," *OSW Analyses*, www.osw.waw.pl/en/publikacje/analyses/2020-03-20/chinese-medical-equipment-supplies-to-europe (accessed 13.12.2022).

[35] V. Zeneli, F. Santoro, "China's Disinformation Campaign in Italy," *The Diplomat*, www.thediplomat.com/2020/06/chinas-disinformation-campaign-in-italy (accessed 13.12.2022).

As a consequence, China conceals the neglect of its own services during the first wave of the spread of the virus and emphasises its own commitment to addressing the challenges of successive waves of infections outside the PRC. This allows it not only to promote a positive image of China and its effectiveness in the fight against the virus but also provides premises for beliefs that actions taken by other countries are ineffective.[36]

Development of China's Information and Disinformation Policy

Although Chinese disinformation activities abroad are increasingly portrayed as being equally aggressive as analogous actions by the Russian Federation, they still seem to be less advanced.[37] This is exemplified by the quite inept dissemination by the Chinese embassy in April 2020 of information about the abandonment of patients in French nursing homes by local medical personnel.[38] In Poland, in turn, allegations of inept disinformation by China were raised in disputes between the Chinese embassy and the U.S. embassy, in which the former was

[36] M. Schrader, "Analysing China's Coronavirus Propaganda Messaging in Europe," *Alliance for Securing Democracy*, https://securingdemocracy.gmfus.org/analyzing-chinas-coronavirus-propaganda-messaging-in-europe (accessed 13.12.2020); J. Kurlantzick, "China thinks the pandemic will make it the world's new leader. It won't," *The Washington Post*, www.washingtonpost.com/outlook/china-uses-the-pandemic-to-claim-global-leadership/2020/05/21/9b045692-9ab4-11ea-ac72-3841fcc9b35f_story.html (accessed 13.12.2022).

[37] T. Uren, E. Thomas, J. Wallis, "Tweeting through the Great Firewall," Australian Strategic Policy Institute, www.aspi.org.au/report/tweeting-through-great-firewall (accessed 13.12.2022).

[38] J. Irish, "Outraged French lawmakers demand answers on 'fake' Chinese embassy accusations," *Reuters*, www.reuters.com/article/health-coronavirus-france-china/outraged-french-lawmakers-demand-answers-on-fake-chinese-embassy-accusations-idUKL5N2C370M (accessed 13.12.2022).

accused of using fake accounts to promote negative comments and an online dictionary to simulate the activity of Polish internet users.[39]

What may be a lack of practice or the occasional mishaps of Chinese diplomats on social media should, however, be placed in a broader context. Chinese diplomacy has started using Western social media relatively recently (the Chinese ambassador to the U.S. Cui Tiankai was the first to use Twitter in June 2019).[40] Although Western social media were used by representatives of major Chinese press offices more than a decade earlier, their role in Chinese public diplomacy began to grow only in recent years. An analysis of the content published on these communication channels leads to the conclusion that in the years leading up to the pandemic, the Chinese authorities were content to just present to non-Chinese audiences their own actions and to promote a positive image of the PRC abroad.[41] The years 2019 and 2020 brought significant changes in this regard in the form of an increasingly assertive and often even aggressive policy, based on criticism of Western solutions, active accusations of prejudice against China, and finally resorting to political manipulation. What is more, those actions are conducted in an increasingly organised manner. In June 2019, the Chinese Ministry of Foreign Affairs entrusted the Chinese *Global Times* with the task of monitoring social networks

[39] P. Uznańska, "Wojna o narrację o COVID-19: jak Polska stała się miejscem potyczek amerykańsko-chińskich?," Europejskie Centrum Projektów Pozarządowych, www.ecpp.org.pl/wojna-o-narracje-o-covid-19-jak-polska-stala-sie-miejscem-potyczek-amerykansko-chinskich (accessed 13.12.2020).

[40] M. Przychodniak, "China's Public Diplomacy..., *op. cit*.

[41] It should be emphasised once again that the exceptions are the narratives about the Chinese periphery: Taiwan, Hong Kong, Xinjiang, and Tibet. In line with the assumptions presented in the introduction in the text, they are not analysed, mainly due to the unique geopolitical conditions specific to each of the indicated cases.

for information on the PRC.[42] Information activities are also supported by fake accounts from China.

It should be noted, however, that until relatively recently, Chinese information policy was generally associated with public diplomacy. It was only in 2020 that the European Union openly named the PRC as a state spreading disinformation premeditatedly on an equal footing with Russia.[43] While the reports of the European Commission did not emphasise this aspect of mutual relations, the speech by Vice-President of the European Commission Věra Jourova given on 10 June 2020, sparked a wave of confirmatory accusations against the PRC of disseminating false data on the spread of the coronavirus in Europe.[44]

Conclusions

The use of disinformation as a way to conduct politics is nothing new, especially for a regime like China. This is where the monumental work *The Art of War* originates from, in which Sun Tzu devotes an entire last chapter to the role of disinformation in the creation of competitive advantages against rivals.

The main threat posed by Chinese disinformation is its anti-democratic overtone. The actions of the PRC, although not always effective in reaching Western recipients in the current phase, threaten the quality of the information society, especially in the area of discourse on democratic values. In the longer term, they may contribute to the erosion of democratic institutions in

[42] M. Przychodniak, "China's Public Diplomacy..., *op. cit*.

[43] "EU says China behind 'huge wave' of Covid-19 disinformation," *The Guardian*, www.theguardian.com/world/2020/jun/10/eu-says-china-behind-huge-wave-covid-19-disinformation-campaign (accessed 13.12.2022).

[44] N. Bentzen, T. Smith, "The evolving consequences of the coronavirus 'infodemic'", European Parliament, www.europarl.europa.eu/RegData/etudes/BRIE/2020/652083/EPRS_BRI(2020)652083_EN.pdf (accessed 13.12.2022).

individual Western countries, as well as weaken the dynamics of cooperation based on democratic values, which are presented as ineffective in comparison with autocratic patterns of anti-crisis measures. In the context of Chinese double standards of information circulation inside and outside its own borders, this challenge requires a joint response from states and organisations committed to democratic values.

Interestingly, however, neither information policy, nor public diplomacy, nor the "face mask" policy met with a positive reception in the immediate vicinity of China, which two decades ago was particularly affected by SARS. South Korea, Taiwan, Singapore, or even Vietnam, ideologically close to the PRC, ignored the reassuring signals coming from the Middle Kingdom and immediately blocked the flow of people from mainland China. This may lead to the conclusion that the prolonged exposure to Chinese information measures in the face of everyday relations with the Middle Kingdom does not bring the intended effects. Therefore, a question can be raised whether building a virtual wall in the context of the COVID-19 pandemic in the end weakens Chinese public diplomacy as such. This is best expressed by the growing interest of Western institutions in Chinese disinformation, which is reflected, for example, in the increasingly assertive stance of the EU in this regard. However, the PRC has shown many times that it can learn from mistakes. It would be a mistake for the recipients of Chinese actions to assume that this time it will be different.

AGNIESZKA LEGUCKA
Polish Institute of International Affairs
Academy of Finance and Business at Vistula University
ORCID: 0000-0002-9438-2606

Targeting Poland: History as a Tool of Russian Disinformation

History in the Service of Russian Disinformation

Disinformation is a term used to denote information that is intentionally false, manipulated, or misleading.[1] Its aim is to influence the actions of the recipients by creating uncertainty or hostility, polarising societies, and disrupting democratic processes. Russian disinformation covers many topics, including history. It is often confused with terms such as "propaganda", which imposes its own version of history, or "memory wars", which focus

[1] R. Kupiecki, "Dezinformacja w stosunkach międzynarodowych – geneza, cele, aktorzy, metody. Zarys problemu," [in:] R. Kupiecki, T. Chłoń, F. Bryjka, K. Kozłowski, J. Misiuna, J. Podemska, P. Podemski, *Platforma Przeciwdziałania Dezinformacji – budowanie odporności społecznej badania i edukacja*, Dom Wydawniczy Elipsa, Warsaw 2021, pp. 15–32.

on criticising alternative views of history to replace them with the one acceptable to Moscow. Sometimes, it is incorrectly compared with "memory diplomacy", which is a "form of public diplomacy in which states or political groups try to improve relations and reputations by exporting commemorative practices and historical narratives and allying their own historical narratives with those of another country".[2] Due to its deceptive intent, disinformation is notably distinct from different interpretations of historical events that result from practices like "memory diplomacy". This point has been emphasised by Adam D. Rotfeld and Anatolii W. Torkunov, co-chairs of the Polish-Russian Group for Difficult Issues, who were tasked with drawing up a list of historical events that divide Poles and Russians. They wrote that: "Historical facts are indisputable. However, their interpretation may vary. Different nations have different assessments of the same events (...) The current state of Polish-Russian relations carries the burden of history. Our memory of historical events significantly contributes to how we look at the world and how we perceive ourselves in the world around us. It is important to ensure that memory is not subject to manipulation and deliberate falsification of the past, that it resists attempts to obliterate the traces of what was shameful and deserves to be condemned (...)".[3]

This chapter takes-up the role interpretation of history plays in Russia's state politics and its deliberate manipulation of the past as well as its use of false opinions and distortions of historical events. It will analyse the disinformation historical campaigns carried out

[2] J. McGlynn, "Moscow Is Using Memory Diplomacy to Export Its Narrative to the World," *Foreign Policy*, 25 June 2021, https://foreignpolicy.com/2021/06/25/russia-puting-ww2-soviet-ussr-memory-diplomacy-history-narrative (accessed 12.08.2021).

[3] A. D. Rotfeld, A. V. Torkunov (eds.), *White Spots. Black Spots. Difficult Matters in Polish-Russian Relations 1918–2008*, University of Pittsburgh Press, Pittsburgh 2015, pp. 6, 7.

against Poland and assess their effectiveness through the lens of Russia's goals. It will also examine the characteristics of Russia's foreign policy goals and how Russian authorities use historical narratives to fulfil them. Then, it will examine Russia's toolbox for conducting historical disinformation campaigns. In addition to necessary references to the past, the analysis will focus on the period after 2014 when the Russian authorities strengthened their foreign policy tools using historical policy, propaganda, and disinformation.

Between the beginning of the 16th century and the middle of the 20th century, Poles and Russians fought against each other in almost 20 different conflicts, which together lasted about 70 years. Russia's victories made it an empire for the next several hundred years. At the turn of the 17th and 18th centuries, Poland transformed into a Russian protectorate and lost its independence at the end of the 18th century. At the beginning of the 19th century, over 80% of its territory was under Russian rule. However, Poles did not accept the pan-Slavic idea of Russian-Polish brotherhood. Poland regained full independence for a short time (1918-1939), but soon returned to its position as a protectorate of Russia during World War II. It regained its sovereignty only in 1993 when "the last Russian soldier left its territory".[4] For centuries, the image of the enemy has been a way of building the identity of both Russians and Poles. As Andrzej de Lazari and Oleg Ryabov noted, "if there was no Poland, it would have to be invented".[5] Since Poland regained its independence in the 1990s, Russia has objected to the idea of Poland shaping the European discourse on Russia. From the Russian perspective, Polish control of the rhetoric has

[4] A. Balcer, "Vis-à-vis postimperium: Polska polityka wobec Rosji," *Nowa Europa Wschodnia*, 19 July 2021, https://new.org.pl/#1591,balcer_rosja_polska_relacje_usa_historia_polityka (accessed 12.08.2022).

[5] A. de Lazari , O. Riabow, *Polacy i Rosjanie we wzajemnej karykaturze,* Polski Instytut Spraw Międzynarodowych, Warszawa 2008, p. 11.

resulted in tougher Western policies. In the past, Poles viewed Russia through an orientalist lens, thus depriving "barbaric" Russia of the character of a civilised political entity. Today, among the societies of Central Europe, Russia is perceived as a threat to the greatest extent by Poles (68%), followed by Czechs (43%), Hungarians (25%) and Bulgarians (3%).[6] On the other hand, for Russia, recognising Poland as part of the West has had both positive and negative consequences. For some Russian thinkers, this recognition allowed Russia to strive to "catch up and overtake" Poland, while for others, Poles were perceived as part of the "rotten West", which does not respect Russian values and traditions.[7]

The Goals of Russian Disinformation

Keir Giles rightly points to the fact that almost each period of Russian history has been "referred to in some venue or another as setting a precedent for what is happening today".[8] History, along with its false and misleading variations, explains Russia's confrontational foreign politics toward the West. Furthermore, "the way history is managed has real implications for post-Soviet Russia and its neighbours", including Poland. Russia's history-based disinformation serves four main goals.

First, it aims to strengthen Russia's international position, which results from the need to pursue Russian superpower interests and recognise the special role of the Russian Federation in shaping international security. Using international media for

[6] D. Milo, "The image of Russia in Central & Eastern Europe and the Western Balkans," Globsec, 23 March 2021, p. 17. https://euagenda.eu/publications/the-image-of-russia-in-central-eastern-europe-and-the-western-balkans (accessed 10.07.2021).

[7] A. de Lazari, O. Riabow, *Polacy...*, *op. cit*., pp. 11, 12.

[8] K. Giles, *Moscow Rules: What Drivers Russia to Confront the West?*, Brookings Institution Press, Chatham House, 2019, pp. 117–120.

disinformation purposes is not only a soft power mechanism; it also helps to undermine Russia's adversary—the United States and its allies. When Putin praises the post-Yalta Conference settlement, "he is extolling a world that stands in contrast to the unipolar U.S.-led system that came after 1991" and indicating his desire to settle a multilateral order based on the most important powers in the world. This specific interpretation of Russia's history and selective memory of World War II is used as a tool to "remind the world of Russia's inherited right to the great-power status earned by the Soviet Union in 1945".[9] One of the tasks of disinformation is to support the implementation of the state's foreign policy goals. The Russian authorities have decided to utilise a "time-worn method by reviving the traditional international identity of Russia as a great power". Memory politics have played a crucial role in the process of Russian de-Westernisation. While Yeltsin conducted a policy of returning to Europe, Putin revived Stalin's rhetoric of the "besieged fortress" along with the anti-Western rhetoric of the Cold War. This strategy has resulted in an "old-new" foreign policy of rivalry with the United States and the European Union.

The *second goal* of Russia's history-based disinformation is to build a parallel between the past and the present in order to justify (in legal and moral terms) its foreign policy and military activity. History and its defence are related to the national security of the Russian Federation. The Military Doctrine published in December 2014 denotes information activities aimed at undermining historical traditions as the "main internal military risk".[10] According to the National Security Strategy published in July 2021, protection of "historical truth" "aims to mobilise the Russian nation, even

[9] J. McGlynn, "Moscow is using...," *op. cit.*

[10] *The Military Doctrine of The Russian Federation, Approved by the President of the Russian Federation on December 25, 2014* [in:] R. Kupiecki, M. Menkiszak (eds.), *Documents Talk. NATO-Russia Relations after the Cold War*, PISM 2020, pp. 500–503.

the Russian identity itself, against western bogeymen at home and abroad". This motivation has led to the militarisation of Russian thinking about the past and been used to justify Russia's military operations in the world today. This mentality has been used to compare Ukrainians to fascists and frame Russia as the protector of Christians. By creating this narrative, Russia is able to garner citizens' support for armed activity in Ukraine and Syria and to implement the Kremlin's geopolitical ambitions. For example, in 2014, eastern Ukrainian "self-defence" units gathered, bedecked in St. George's ribbons and buoyed by Russian propaganda, to defend Soviet war memorials from the "Banderivtsy" (wartime Nazi collaborators). "The ribbon became a symbol of two wars but also evidence of how the Kremlin uses the memory of World War II, at home and abroad, as a Trojan horse to smuggle in other, more contentious, geopolitical stances".[11]

Third, the manipulation of history is used to help consolidate society around Putin, who is portrayed as the one who upholds respect for Russian values and the past as a "gatekeeper" to national memory. References to history provide an important message: Russia, as a "besieged fortress", needs a strong commander, and anyone questioning this commander's leadership is a threat to the country. According to Jane McGlynn, the "Russian government has co-opted and instrumentalised the powerful memory of Soviet heroism and victimhood to legitimise its rule". This historical narrative is used to perpetuate the claim that an authoritarian system is an optimal governing model for Russia, in which the society accepts the rule that defends respect for the leaders' past.

The *fourth goal* of Russia is to weaken the European Union and NATO. Poland is a particular target of Russian disinformation campaigns, and Russia aims to reduce Poland's influence on the eastern policy of these organisations. The primary reason for this

[11] J. McGlynn, "Moscow is using...," *op. cit.*

is the contradictory interests of Poland and Russia in the common eastern neighbourhood, in which Poland strives to stabilise these countries, introduce democratic reforms, support civil societies, and increase the transparency of doing business. Russia, however, views the strengthening of Eastern European states' sovereignty as counter to its interests. The pro-Kremlin media and the Russian authorities aim to marginalise the Polish voice in the European debate on Western-Russian relations, arguing that historical Polish-Russian animosities have led to Polish Russophobia and that Poles are incapable of making constructive proposals in relations to their eastern neighbour. This is conducive to breaking up and weakening the cohesion of western institutions. In order to achieve this goal, Russia has invested heavily in a "weaponised" information programme that uses a variety of means to sow doubt and division.

Warsaw presents a serious challenge to the Russian narrative of events during World War II and its historical identity. Poland's historical account provides proof of the cooperation between Nazi Germany and the USSR. Russian authorities have attempted to minimise discussion of the Molotov-Ribbentrop Pact and the Soviet-German cooperation during the intra-war period. Russian authorities prefer to show only the victory in the Great Patriotic War, which is treated as the founding myth of Putin's regime. To strengthen the legitimacy of Putin's authoritarian rule, the Kremlin has introduced legislative measures that aim to limit different interpretations of historical events. Amendments to the constitution of 2020 introduced the obligation to "defend the historical truth" and a prohibition on "diminishing the achievements of the nation in defence of the homeland".[12] Furthermore, the amended penal code introduced a penalty for

[12] "Новый текст Конституции РФ с поправками 2020," Государственная Дума, http://duma.gov.ru/news/48953 (accessed 10.08.2021).

disseminating deliberately false information about veterans of the Great Patriotic War or insulting them (maximum penalty of 5 and 3 years, respectively).[13] In July 2021, the law was amended, introducing a ban on the public identification of the actions of the leadership of the USSR and the Third Reich in an effort to halt the equating of Nazism and Stalinism.[14] These amendments correspond to the restrictive historical policy of the Russian authorities and the limitation of historical research, which aims to prevent, among others, deception of the past in dialogue with Poland. From the Russian perspective, Poland undermines the liberating role of the Red Army and its participation in the end of World War II. By blaming Poland for being jointly responsible for its outbreak, the Russian authorities justify the actions of the USSR in Central and Eastern Europe. They aim to "remove the aggressor's odium from the USSR, which in September 1939, under the Ribbentrop-Molotov Pact, took the eastern territories of the Second Polish Republic, and in 1940, annexed Lithuania, Latvia and Estonia".[15]

[13] Yury Dmitriev, a civil rights activist and historian in Karelia who has worked to locate the execution sites of Stalin's Great Terror, was in July 2020 convicted of the sexual assault of his daughter It was meant to serve as a cautionary tale for the research community not to deal with compromising moments from the USSR/Russian past. M. Domańska, J. Rogoża (cooperation), "Rosja: dalsze zaostrzanie ustawodawstwa dotyczącego polityki pamięci," *Analizy OSW*, 19 May 2021, www.osw.waw.pl/en/node/28856 (accessed 10.07.2022).

[14] "О внесении изменения в Федеральный закон 'Об увековечении Победы советского народа в Великой Отечественной войне 1941– 1945 годов'", *Duma.gov*, 1 July 2021, https://sozd.duma.gov.ru/bill/1166218-7 (accessed 10.07.2022).

[15] A. Dyner, "World War II in Russia's Foreign Policy," *PISM Bulletin*, no. 12(1442), 28 January 2020, www.pism.pl/publications/World_War_II_in_Russias_Foreign_Policy (accessed 10.07.2022).

Russia's Toolbox

Russian disinformation aims to confuse various audiences about Russia's past and present. Generally, narrative laundering is successful when propaganda narratives cannot be traced back to Russia. Hidden channels and indirect disinformation campaigns have been utilised to influence perceptions of major events like the U.S. presidential election in 2016 and the COVID-19 pandemic Unlike these types of covert campaigns, history as a tool of Russian disinformation is disseminated in a more official manner. State authorities, including Putin, have published several articles and repeatedly voiced their opinions about past events. Putin's rationale for utilising this method of disinformation is to build the image of a leader inside Russia who defends the past and projects a strong image of Russia to the world. The Russian authorities and the pro-Kremlin media, in part due to their hierarchical management style, have successfully created a false but coherent message in which the Russian historical narrative prevails. At the same time, the Russian authorities have for many years restricted the possibilities of free discussion, including on the internet (RuNet).

In an effort to spread disinformation abroad, Russian media organisations, like state-owned Sputnik and RT, now operate in several foreign languages. RT, which was rebranded from Russia Today in 2009, has also revised its content to feature less Russia coverage and more deliverable provocations and conspiracy theories under the slogan "Question More".[16] The Internet Research Agency (IRA), a "troll factory" owned by Putin associate Yevgeny Prigozhin, is also an important tool of Russian disinformation policy. It has operated since 2013 with a monthly budget of one

[16] A. Shekhovtsov, *Russia and the Western Far Right: Tango Noir*, Routledge, London 2017, pp. 134-135.

million euros and is divided across foreign sections to conduct discussions in various European languages. Its aim is to induce extreme emotions and anger people on the internet; most often, these trolls question Western values and instigate historical debates based on stereotypes and false accusations. In recent years, this aspect of Russia's disinformation toolbox has adapted to new conditions. Russia's notorious IRA has faced increasing resistance from Western governments, civil society, and, most notably, social media platforms. The IRA has refined its manipulation efforts via the website RIA FAN (Federal News Agency). It publishes its "news" through Kremlin-friendly Telegram accounts that have a combined following of over 160,000 users.[17] Another novel source of Russian disinformation is TheSoul Publishing, a media enterprise that has the third-largest reach on YouTube (number of views and subscribers) after Disney and Warner Media. This company, which releases massive amounts of content, also offers pro-Russian views through platforms like fake movies that discuss the history of World War II.

Among the disinformation platforms that focus on history is the news portal Regnum.ru, which is visited daily by over one million people and gets more than 31 million hits monthly.[18] This site has repeatedly published false information about past events and their interpretations. In one article, it suggested that if Poland had lost the war with the Bolsheviks of 1919-1921, it would have

[17] L. Mejia, C. Watts, "The Illusion of a Russian Media Empire: How Anonymous Bloggers and Obfuscated Identities Power the Troll Factory's Successor," *GMF*, 19 July 2021, https://securingdemocracy.gmfus.org/the-illusion-of-a-russian-media-empire-how-anonymous-bloggers-and-obfuscated-identities-power-the-troll-factorys-successor (accessed 22.07.2022).

[18] "Статистика посещаемости," *Regnum.ru*, https://pr-cy.ru/site-statistics/?domain=regnum.ru (accessed 10.01.2021).

become part of the USSR; within this scenario, it concluded that "Poles could have prevented the Second World War".[19]

Operations against Poland and Historical Disinformation: the Most Popular Narratives

Russian accusations against Poland, sometimes supported by Belarusian propaganda, are regularly disseminated. However, the content and frequency of these accusations have seen periodical "intensification" related to:

- the political situation in Russia, Ukraine, and Belarus as well as the dynamics of political events in Poland (elections, protests, etc.);
- historical anniversaries like International Holocaust Remembrance Day on 27 January; the anniversary of the 1921 Treaty of Riga on 18 March; the end of World War II on 8 and 9 May; the anniversary of Operation Barbarossa on 24 June; the anniversary of the 1939 Ribbentrop-Molotov pact on 23 August; and the outbreak of World War II as well as the USSR's aggression against Poland on 1 and 17 September, respectively;
- the announcement of EU sanctions or decisions against Russia like the adoption of the European Parliament resolution in September of 2019 that condemned both Nazism and communism;[20]
- NATO-led military exercises (particularly on the Alliance's Eastern Flank).

[19] С. Стремидловский, "Почему проигрыш в польско-советской войне стал бы благом для Польши," *Regnum.ru*, 16 March 2021, https://regnum.ru/news/polit/3216160.html (accessed 10.08.2022).

[20] *Resolution on the importance of European remembrance for the future of Europe*, 2019/2819(RSP), European Parliament, 19 December 2019, www.europarl.europa.eu/doceo/document/TA-9-2019-0021_EN.html (accessed 10.08.2021); "Путин трижды за неделю осудил резолюцию Европарламента. Что важно знать," 24 December 2019, *RBK.RU*, www.rbc.ru/politics/24/12/2019/5e02044b9a7947ed72a460bc (accessed 10.08.2022).

The three most popular historical narratives used against Poland in the promotion of pro-Russian sentiment are as follows:

1) Poland was responsible for the outbreak of World War II, a notion that aims to detract from accusations against the USSR and its aggression against Poland on 17 September 1939. The disinformation campaign based on the narrative of alleged cooperation of the government of the Second Polish Republic with Hitler began with a speech by Putin in December 2019, although similar accusations had appeared earlier in the Russian press. The main theme of the Russian leader's "historical lectures" centred on the thesis that Poland, together with Germany, was responsible for the outbreak of the Second World War.[21] In these lectures, Putin alleged that Poland collaborated with the Third Reich in its aggression against the Soviet Union.[22] In an article for *The National Interest*, the Russian leader stated that blame for starting the war lies "entirely on the conscience of the then Polish government, which prevented the conclusion of the Anglo-Franco-Soviet military alliance and counted on the help of Western partners".[23] The Russian media has also argued that during WWII, the Polish government in exile tried to establish contacts with Nazi Germany in order to fight the USSR together. It was noted that on 26 January 1934, the German Minister of Foreign Affairs Konstantin von Neurath and the Polish Ambassador Józef Lipski signed the "declaration

[21] В. Путин, "В документах Второй мировой все написано. Читайте," *RG.ru*, 19 December 2019, https://rg.ru/2019/12/19/vladimir-putin-v-dokumentah-vtoroj-mirovoj-vse-napisano-chitajte.html (accessed 12.08.2022).

[22] A.D. Rotfeld, "Rosja: strategiczne dylematy," *Sprawy Międzynarodowe*, 2019, vol. 72, no 4, pp. 22-23, DOI: 10.35757/SM.2019.72.4.01.

[23] V. Putin, "The Real Lessons of the 75th Anniversary of World War II," *The National Interest*, 18 June 2020, https://nationalinterest.org/feature/vladimir-putin-real-lessons-75th-anniversary-world-war-ii-162982 (accessed 3.01.2023).

of non-use of force between Germany and Poland" (Non-aggression Treaty between Germany and Poland) in Berlin. The "Piłsudski-Hitler Pact",[24] as it is called by Putin, is used rhetorically to emphasise the fact that Poland was the first country in Europe to conclude a treaty with Nazi Germany.[25] On the website Regnum.ru, one article asserted that Poland was not a victim of World War II, but one of the main culprits of this conflict. Poland has been accused of, among other things, participation in the partition of Czechoslovakia and the 1942 deportation of the Polish army by General Anders to Iran during the Battle of Stalingrad.[26]

2) Poland was Hitler's ally in actions against Jews, which means that Poles are complicit in the Holocaust. The commemorations of the 75th anniversary of the liberation of Nazi German death camps by the Red Army in January 2020 served as a pretext for Russia to impose its own vision of history on the world. A wave of negative comments swept through Russian media (Gazieta.Ru, Lenta.Ru, RIA Nowosti, SPUTNIK, and others) in connection with Putin's alleged failure to gain an invite to the ceremony at Auschwitz-Birkenau. Putin took part in the "World Holocaust Forum", a ceremony organised in Jerusalem a few days before the commemorations in Poland. The forum, which was

[24] Putin presented such accusations at a meeting with leaders of the Commonwealth of Independent States (CIS) on 20 December 2019. He wanted to gain their support for the Russian view of history. "Ставка Польше чем жизнь," *Kommersant*, 23 December 2019, www.kommersant.ru/doc/4205137 (accessed 12.08.2022).

[25] "Историк раскрыл, как эмигрантские власти Польши искали дружбы с Гитлером," *RIA.ru*, 6 May 2021, https://ria.ru/20210506/voyna-1731252802.html (accessed 12.08.2022).

[26] "Почему Польша не может быть «главной жертвой Второй мировой войны»?", *Regnum.ru*, 22 July 2021, https://regnum.ru/news/society/3302071.html (accessed 12.08.2022).

organised by Moshe Kantor, a Russian Jew associated with the Kremlin, featured Putin as the main speaker; during his speech, Putin proposed that a summit of the permanent members of the UN Security Council should be convened to discuss the current challenges to peace and security. After the visit to Israel, numerous quotes from Putin's speeches appeared in Russian media. One quote that appeared in *Rosijskaja Gazeta* stated that, "[in] Israel as well as in Russia, they are concerned and outraged by the attempt to revise the results of World War II, and do not allow the world to forget what is caused by national egoism, divisions, compliance with chauvinism, anti-Semitism and Russophobia".[27]

3) Russian disinformation contends that Poland actively participated in the murder of Jews during the Nazi occupation. For example, the Russian media often mentions the pogrom of Jews in Kielce on 4 July 1946 and emphasises that the murders of Holocaust survivors were perpetrated by the inhabitants of Kielce and not by the German Nazis. The pro-Kremlin media combines historical moments with current events in an effort to influence Poland's relations with Israel and the United States. In an *RIA Novosti* article entitled "Poland does not want to pay for its sins", the author accused the Polish Sejm (the lower house of parliament) of passing a law that prohibited the descendants of Polish Holocaust victims from applying for the return of property (the actual law did not exclusively apply to Jews).[28] The article continued that the United States, "which Warsaw

[27] W. Baluk, "Polska na celowniku Putina. Narracja rosyjskiej propagandy w sprawie wybuchu II wojny światowej," *Biuletyn. "Monitoring propagandy i dezinformacji*," 2020, no 1, pp. 15-18.

[28] "Польша отказывается платить за свои грехи," 30 June 2021, https://planet-today.ru/novosti/politika/item/135262-polsha-otkazyvaetsya-platit-za-svoi-prestupleniya (accessed 1.07.2022).

has faithfully served in recent years", had an unfavourable opinion of this document.[29] Furthermore, *Sputnik Polska* frequently writes about Polish anti-Semitism and has suggested that "it can be called a part of the cultural code, something that has been sucked out with mother's milk. Polish anti-Semitism has in fact become historical and differs little from Polish Russophobia, Ukrainophobia or Germanophobia."[30] A common theme has emerged among pro-Russian publications regarding Polish anti-Semitism that features the thesis that, "Poland should learn from Russia's example".[31]

4) Poland is destroying the cemeteries of Russian/Soviet soldiers, which aims to show a lack of gratitude for the USSR's role in liberating Central European countries from fascism. The Russian disinformation campaign regarding the destruction of memorials has intensified since Poland's adoption of an act on 1 April 2016[32] that prohibits the propagation of communist symbols in public spaces, but which did not address the issue of monuments. It only ordered the removal of street names associated with the communist period. Meanwhile, the Russian authorities reacted sharply to the Polish announcement that monuments of gratitude to Soviet soldiers would be liquidated. The Russian Ministry of Foreign Affairs responded with criticism of the plans to

[29] *Ibidem*.

[30] "Żyd w Polsce może czuć się dziś bezpieczniej niż w jakimkolwiek z zachodnioeuropejskich państw," *Sputnik News*, https://pl.sputniknews.com/20210704/zyd-w-polsce-moze-czuc-sie-dzis-bezpieczniej-nis-w-jakimkolwiek-z-zachodnioeuropejskich-panstw-15390076.html (accessed 10.01.2023).

[31] *Ibidem*.

[32] *Ustawa o zakazie propagowania komunizmu lub innego ustroju totalitarnego przez nazwy budowli, obiektów i urządzeń użyteczności publicznej*, Dz.U. 2016, poz. 744.

demolish the monuments and announced what it called a justified reaction.[33] The response that followed from the Polish MFA referenced the 1994 agreement between Poland and the Russian Federation on the graves and memorials of victims of wars and repression; it argued that the agreement specified that only cemeteries and war graves could not be removed, and that it did not apply to symbolic monuments that do not enclose the remains of soldiers and only provide a testimony to past Soviet domination.[34] This Polish attempt at clarification did not prevent the Russian authorities and the pro-Kremlin media from falsifying information, asserting unequivocally that monuments to Soviet soldiers and cemeteries are systematically being destroyed in Poland.[35] Media have repeatedly reported that the number of monuments to Soviet soldiers in Poland has decreased fivefold (from about 500 to around 100).[36]

[33] "Zakharova sravnila snos pamyatnikov v Pol'she s deystviyami IG v Pal'mire," *RIA Novosti*, 31 March 2016, https://ria.ru (accessed 7.01.2023).

[34] *Oświadczenie MSZ w związku z wypowiedzią rzecznik Ministerstwa Spraw Zagranicznych Rosji*, MSZ, 1 kwietnia 2017 r., www.msz.gov.pl; por. *Umowa między Rządem Rzeczypospolitej Polskiej a Rządem Federacji Rosyjskiej o grobach i miejscach pamięci ofiar wojen i represji, sporządzona w Krakowie dnia 22 lutego 1994 r.*, Dz.U. 2012, poz. 543.

[35] "Слуцкий призвал извлечь уроки из ситуации с уничтожением захоронений советских воинов в Польше," *DumaTV*, 9 May 2021, https://dumatv.ru/news/slutskii-prisval-isvlech-uroki-is-situatsii-s-unichtozheniem-zahoronenii-sovetskih-voinov-v-polshe (accessed 8.01.2023).

[36] "За 20 лет число памятников советским воинам-краноармейцам в Польше сократилось в пять раз," https://evo-rus.com/avto/exluzive/za-poslednie-20-let-kolichestvo-pamyatnikov-sovetskim-voinam-v-polshe-sokratilos-v-pyat-raz.html; "В Польше пересчитали советские памятники," https://pobedarf.ru/2021/05/08/v-polshe-pereschitali-sovetskie-pamyatniki/; "Число памятников советским воинам в Польше сократилось в пять раз, ИА Красная Весна," https://rossaprimavera.ru/news/13da068f (accessed 8.01.2023).

The Effectiveness of Russian Distortions of History

The effectiveness of disinformation campaigns has largely depended on the target group against which the Russian information operations were carried out, with varied results in Polish-speaking audiences, Western countries, Russia, and the Russian-speaking post-Soviet space (mainly Ukraine and Belarus).[37] The goal of increasing Russia's position in international relations and building an international perception based on the imperial past of Russia, has not been fulfilled. Few in the West believe Russian narratives about the outbreak of World War II because there is ample evidence to refute this claim. Putin has failed to transfer responsibility for the outbreak of WWII from the Molotov-Ribbentrop Pact to the Munich Agreement and the partition of Czechoslovakia, as evidenced by the resolution of the European Parliament in September 2019 that condemned the cooperation of totalitarian regimes of communism and Nazism.

Thus far, Putin has not been able to convene his proposed meeting of the "Big Five" (permanent members of the UN Security Council), which he sees as an ideal way to establish a concert of powers that could address international affairs. Russia seeks to promote the Soviet version of its history and suppress history in Ukraine, Belarus, and the Baltic states in an effort to promote its "special" role and interests in the post-Soviet space. In other words, Russia's Soviet history provides a rationale for "protecting" its sphere of influence in Eastern Europe and the South Caucasus. This effort to export its own version of history in the post-Soviet space has achieved a degree of success. A moderate example of a successful memory export from Russian Victory Day celebrations is the Immortal Regiment procession, which is now present in

[37] A. Lelonek, "Propaganda i dezinformacja Federacji Rosyjskiej w Polsce," *Biuletyn „Monitoring propagandy i dezinformacji*, 2020, no. 1, p. 11.

115 countries.[38] It is also evident that the Russian narrative has gained support in some post-Soviet states, such as Belarus.

Putin's historical narratives are largely successful with the Russian public and members of the Commonwealth of Independent States. It could be surmised that even the architects of the narrative did not believe it would gain much traction outside of the area of the former Soviet Union. The aforementioned second and third goals of Putin's historical disinformation campaigns, which relate to justification of his foreign policy and the consolidation of society, are welcomed by many Russians. In recent years, the regime has invested a great deal of attention to the rhetoric of civilisational differences between Russia and the West (including Poland).[39] In 1989, 60% of respondents regarded the Western way of life as exemplary; under Putin's regime, however, 67% of respondents characterised a Western type of society as "incompatible with the way of life in Russia".[40] According to the Levada Center, the number of those who believe that Russia is a European country has decreased by almost half in recent years: from 52% in 2008 to 29% in 2021.[41]

In the internal aspect the Russian disinformation is successful as the Kremlin has managed to achieve its goals. Opinion polls showed great support for Putin's military operation in Ukraine and his president support increased significantly after March 2022 (it was over 80%).[42] In November 2022 prop up for the Russian

[38] J. McGlynn, "Moscow is using...," *op. cit.*

[39] N. Robinson, *Contemporary Russian politics*, Polity Press, Cambridge 2018, p. 240.

[40] O. Kushir, *Ukraine and Russian Neo-imperialism. The Divergent Break*, The Rowman & Littlefield Publishing Group, Inc., London 2018, p. 19.

[41] "Russia and Europe," Press Release/Publications, *Levada Center*, 22 March 2021, www.levada.ru/en/2021/03/22/russia-and-europe (accessed 1.07.2022).

[42] K. Chawryło, "Weapons of mass deception. Russian television propaganda in wartime," *OSW Commentary*, www.osw.waw.pl/en/publikacje/

Armed Forces in Ukraine remained high (over 40%), so Russians supported militarisation of Russian foreign policy.[43]

Russia's disinformation campaigns aim to discredit Poland within the international arena and isolate Warsaw from the transatlantic community. On occasion, European leaders have echoed Russian narratives that Poles are Russophobic;[44] however, the European Union and NATO have taken active measures to tighten their policy toward Russia. Despite these efforts, Russia's goal of weakening cohesion and stirring discord among NATO and EU member states has been partially successful.[45] There is evidence that Russian disinformation undermines social trust in democratic institutions. In every European Union country, at least half of respondents say that they encounter fake news at least once a week. In Poland, the pro-Russian voices are usually more silent and marginal, but this does not mean that Poles are fully resilient against disinformation.[46] According to Eurobarometer surveys,

osw-commentary/2022-05-06/weapons-mass-deception-russian-television-propaganda-wartime (accessed 18.02.2023).

[43] „Conflict with Ukraine" Presse Release, *Levada Center*, 12 November 2022, www.levada.ru/en/2022/12/12/conflict-with-ukraine-november-2022.

[44] D.M. Herszenhorn, "Summit exposes stark clash of EU views on Russia," *Politico*, 25 June 2021, www.politico.eu/article/emmanuel-macron-russia-vladimir-putin-european-union (accessed 1.09.2022).

[45] N. MacFarquhar, "A Powerful Russian Weapon: The Spread of False Stories," *The New York Times*, 28 August 2016, https://www.nytimes.com/2016/08/29/world/europe/russia-sweden-disinformation.html (accessed 15.07.2021).

[46] The exception is Mateusz Piskorski, a pro-Russian political figure who does not have widespread support. In 2015, he founded the pro-Russian leftist party called Zmiana (Change). His comments were widely spread in Sputnik and RT as a "geopolitical expert". In May 2016, Piskorski was arrested by the authorities on charges of espionage for Russia and China, and he was imprisoned. At the same time, his European Centre for Geopolitical Analysis (ECAG) was largely using money from Russia. P. Krekó, L. Györi, "A House Undivided," *Visegrad Insight*, 2017, no 2(1), p. 12.

75% of Poles observe some disinformation in their daily life. Within the European Union, only Spain (78%), Hungary (77%), and Croatia (76%) have higher exposure to disinformation.[47]

At the bilateral level, relations between Poles and Russians are largely perceived to be problematic due to historical issues, various traumas from the past, and differing views of past events. Research carried out in 2020 by the Centre for Polish-Russian Dialogue shows that Poles consider historical problems to be the basis of the most important mutual disputes (74%) between Poland and Russia.[48] Russians emphasise the "unfriendly, hostile attitude of Poles" (24%) as well as "historical events, partitions, World War II, Katyn" (16%), and "a different view of history, denial of the role of Russia" (14%) as the top bilateral issues.[49]

It is worth noting that disinformation regarding "memorials" has been an effective rhetorical tactic for Russia. Almost 90% of Russians have heard about the removal of Red Army monuments, and Poland can count on 10% to 12% of Russians to understand its arguments about memorials. This issue is consistently used by the Russian authorities to fuel negative social emotions. As a result, it is unsurprising that interviewed Russians often use the terms

[47] "Flash Eurobarometer 464 (Fake News and Disinformation Online)," *GESIS Data Archive, Cologne. ZA6934 Data file Version 1.0.0,* European Commission, Brussels (2018), https://doi.org/10.4232/1.13019.

[48] "Wojna informacyjna i propaganda historyczna. Raport z badania opinii publicznej dla Centrum Polsko-Rosyjskiego Dialogu i Porozumienia," Centrum Polsko-Rosyjskiego Dialogu i Porozumienia, Warszawa 2020, http://cprdip.pl/assets/media/Wydawnictwa/Raporty/Wojna_informacyjna_i_propaganda_historyczna_raport_z_badan_2020.pdf (accessed 10.07.2021), p. 8.

[49] "Obraz Polski w Rosji przez pryzmat sporów historycznych," Centrum Polsko-Rosyjskiego Dialogu i Porozumienia, Warszawa 2020, http://cprdip.pl/wydawnictwo,raporty,668,obraz_polski_w_rosji.html (accessed 10.07.2021), p. 12.

"ungrateful, treacherous, Russophobic, and lying" to describe their Polish counterparts.[50]

Conclusions

Russia's historical disinformation towards Poland is part of Russia's new confrontation policy against the West. Poland is perceived by the Russian authorities as an American proxy that represents different interests in the post-Soviet space. Moreover, Warsaw is seen as a rival because of its historical narratives, which contradict the interests of Putin's authoritarian regime. As a result, the Russian authorities have gone to great lengths to discredit Poland within the transatlantic community and limit its influence on NATO's eastern policy. Despite its efforts, the effectiveness of historical disinformation outside of Russia is limited. Russia has not gained a significant level of Western support for its historical message, and all of its disinformation campaigns against Poland have experienced mixed results in different regions. At the domestic level, Russian disinformation has been highly effective in garnering support for Russia's foreign policy. It is evident that Russians are ready to defend the imperial policy of the USSR or Tsarist Russia. Under this logic, Russian authorities do not need to impose a vastly different vision of history; instead, through the use of swollen stereotypes and prejudices (including those directed at Poles), they can target the emotions of their audience, which is an essential element of disinformation.

[50] *Ibidem*, p. 6.

WOJCIECH LORENZ
Polish Institute of International Affairs
ORCID: 0000-0001-8459-6603

Strategic Propaganda and Disinformation: the Evolution of Russia's Campaign to Undermine NATO

The main goals of Russian propaganda and disinformation against NATO have not changed much since the Alliance was formed more than 70 years ago.[1] The Kremlin's ultimate goal has been a European security system that lacks an effective Western alliance that could weaken Russia's ability to influence the policies

[1] Propaganda can be defined as purposeful dissemination of information and ideas in a biased way for political purposes. Disinformation is a narrower term and usually refers to dissemination of deliberately false information. Both terms are sometimes used interchangeably by political practitioners and it would be difficult and impractical to establish a clear-cut boundary between them. The author uses both terms to indicate a broad dimension of information operations carried out by the USSR and Russia. See: N. Bentzen, "Understanding propaganda and disinformation," European Parliamentary Research Service, November 2015, www.europarl.europa.eu/RegData/etudes/ATAG/2015/571332/EPRS_ATA(2015)571332_EN.pdf (accessed 7.10.2022).

of other states and maintain its "sphere of influence". To achieve its goals, Russia uses propaganda to weaken the cohesion of the Alliance and its ability to defend its members from political pressure and military threats. With time, new methods of propaganda and disinformation and new narratives have been mastered to maximise their political efficiency. Propaganda and disinformation are regarded by Russia as important peace and wartime instruments that can help undermine NATO as an effective political and military alliance. Messaging based on manipulation to stir emotions for political effect are applied as a classic strategy, which should facilitate the achievement of goals (ends) with the available tools (means) and the use of the most effective methods (ways). Since resources are always limited and Russia's influence is based mainly on military power, propaganda and disinformation becomes an indispensable, yet economical instrument (both a tool and a method) for enhancing influence at an acceptable cost.

Soviet Goals

Since the 1917 Bolshevik Revolution, the point of reference for the formulation of Russia's foreign policy goals was the capitalist and democratic West, perceived as a political and military threat to a newly formed communist power.[2] Guided by Marxist-Leninist ideology, the leaders of the USSR ruled out the possibility of the coexistence of capitalism and socialism and assumed the inevitability of war provoked by the capitalist world. The communist power sought to obtain a favourable correlation of forces with the West, necessary for political rivalry and for winning

[2] For an analysis of Soviet threat perception and interests, see: W. Lorenz, *Odstraszanie. Strategia i polityka*, Polski Instytut Spraw Międzynarodowych, Warszawa 2021, pp. 94-115.

a possible military conflict.[3] Marx and his followers perceived the United States as the leader of the capitalist world and an arch-rival, which, due to its potential, was an obstacle to the spread of socialism on a global scale.[4] Therefore, the goal of the Soviet Union was to achieve greater potential than the United States, extend the socialist system to as many countries as possible, and defeat capitalism in an ideological rivalry or by taking advantage of a military conflict.

After the end of the World War II, the USSR's policy in Europe was based on the assumption that, as in the past, Germany and other capitalist powers might attack the Soviet Union. The doctrine of ideological expansion and the sense of threat from the West offered a rationale for asserting political control over the immediate neighbourhood ("sphere of influence") and forming a security perimeter ("buffer zone") beyond its own borders. The strategic interests of the USSR included subjugating the satellite states of Central and Eastern Europe, weakening Germany by maintaining its division, or assuring neutrality and forcing the U.S. withdrawal from Europe.

The U.S. decision to support Europe through the Marshall Plan (1948) and then to provide security guarantees to European allies through the creation of NATO (1949) seriously undermined the Soviet ability to promote its strategic goals Europe-wide. After the creation of NATO, the main goals of the USSR remained to drive the U.S. out of Europe, block or delay the remilitarisation of Germany and maintain its division, fuel divisions among NATO members undermining Alliance's ability to act, and discourage political and economic integration of western Europe, which could

[3] J. Lider, *Correlation of Forces. An Analysis of Marxist-Leninist Concepts*, St. Martin's Press, New York, 1986.

[4] See: Ch. Andrew, O. Gordievsky, *Instructions from the Centre. Top Secret Files on KGB Operations 1975–1985,* Hodder & Stoughton 1991, p. 10.

also strengthen NATO. Although in the 1950s the USSR departed from the dogma of the inevitability of war between the socialist and capitalist world, this did not change the general goal to win the ideological struggle with the West. Since NATO was perceived as a pillar of the West and extension of U.S. power, Moscow has not resigned from attempts to weaken it with aggressive propaganda and disinformation.

The Cold War—Methods and Instruments

For the communist regime, which took power in Russia through a bloody revolution, propaganda and disinformation were important instruments of political influence and were used on a large scale towards its own society and to support foreign policy goals.[5] In a sense, a "doctored truth" lay at the foundation of the movement calling itself "bolsheviks" (the majority), which in reality enjoyed at the time a minority status among revolutionary political factions in Russia. Propaganda activities, and fake news fabricated for domestic purposes were to awaken the class consciousness of the proletariat, consolidate support for the regime, threaten and force society to make sacrifices related to rapid modernisation of the state and preparation for a possible war.

To ensure political control over Central and Eastern Europe, regarded as within its sphere of influence and a military buffer zone, the Soviet Union presented itself as a liberator of satellite states and the defender of a new status quo based on the changed borders. Soviet propaganda developed the myth of the "Great Patriotic War", which presented the USSR as a main victim of Nazi Germany and the country that suffered more than any

[5] D. Brandenberger, *Propaganda State in Crisis: Soviet Ideology, Indoctrination, and Terror under Stalin, 1927–1941*, Yale University Press, 2012, F.C. Barghoorn. *Soviet Foreign Propaganda*, Princeton University Press, 1964.

other. It either tried to remove from history books examples of its aggressive policy of invasion (e.g., of Finland and Poland in 1939) or occupation (e.g., of the Baltic States since 1940), or argued that it was nothing more than justified self-defence.

As a foreign policy tool, propaganda and disinformation were used throughout the whole Cold War era to convince international public opinion of the superiority of communism over capitalism. Soviet narratives argued that capitalism is responsible for most of the problems of the modern world, while communism carries out its historic mission of leading people out of inequality, exploitation and war, and can bring peace, brotherhood and happiness to all mankind.[6] The USSR accused the West of carrying out propaganda activities referred to as psychological warfare against the "socialist camp", but at the same time it undertook aggressive information operations against the western world, treating it as an element of an ideological struggle. Especially at the beginning of the Cold War the Soviets tried to force the withdrawal of U.S. forces from Europe using the slogan "Europe for Europeans" and called for the creation of a European security system without U.S. participation. Since NATO military credibility depended on the willingness of European allies to host U.S. troops and coordinate actions, propaganda activities were used to divide the Alliance politically, paralyse its ability to implement collective defence policy, and strengthen the relative position of the USSR.[7] Increased propaganda activities were directed towards countries

[6] That was clearly in stark contrast with the situation in the Soviet Union, where millions perished because of massive repressions, deportations, forced labour, or famine.

[7] Ch.A. Sorrels, "Soviet Propaganda Against NATO," U.S. Arms Control and Disarmament Agency, October 1983; http://insidethecoldwar.org/sites/default/files/documents/Soviet%20Propaganda%20Campaign%20Against%20NATO_0.pdf (accessed 10.08.2022), R. Kupiecki, *Siła i solidarność. Strategia NATO 1949–1989,* PISM, Warszawa 2012, pp. 268–272.

that were perceived as the weakest links of the Alliance. Such was the case with, for example, Norway and Denmark, which were prepared to take into account the Soviet threat perception and did not agree to the deployment of NATO infrastructure, troops, and nuclear weapons on their territory.[8] To prevent remilitarisation of Germany and its integration with the Western security system, fear of a threat from Germany was carefully cultivated by the USSR. The Soviet narrative also emphasised that the creation of NATO is a manifestation of the imperialist policy of the capitalist powers, which is to lead to the restoration of fascism and German militarism.

By exaggerating its technological and military capabilities the USSR tried to convince Western public opinion and decision-makers that it had the military advantage and, by creating a sense of threat in NATO countries (the one you cannot beat), intimidate societies and influence their policies. One of the most important aims of propaganda was to fuel fears of a nuclear conflict. Since NATO was a military alliance that based its strategy on the threat of nuclear weapons, it became an easy target for propaganda attacks. The USSR presented itself as a peace-loving state and accused the U.S. and NATO of aggressive intentions and of carrying out preparations for war. Communist propaganda emphasised that the very existence of NATO and its military policy significantly increased the risk of conflict, which could easily escalate to nuclear war and annihilation of mankind.

With time, the USSR recognised that the withdrawal of the United States from Europe was unlikely, and greater effort was directed towards severing the transatlantic link by fuelling anti-Americanism and undermining the credibility of American

[8] "Soviet Reactions to Scandinavian Adherence to the Atlantic Pact," Intelligence Memorandum no 149, CIA, 29 March 1949, www.cia.gov/reading room/docs/CIA-RDP78-01617A000400140001-8.pdf (accessed 10.08.2022)

security guarantees in the eyes of European allies. The Soviet Union presented the U.S. as an aggressive state seeking to deploy troops and weapons of mass destruction on the territory of European allies against their interests. One example of such actions includes a forged letter by a supposed Danish general, K. Jorgenson, who informs a Copenhagen area residents that their homes will be requisitioned by U.S. troops participating in NATO exercises in 1983.[9] The Soviets also tried to fuel fears of European countries that, in case of a war in Europe, the U.S. would not use strategic weapons against the USSR and would try to limit the war to European territory.

To reinforce the propaganda message, the Soviet Union increased tensions by raising the readiness of its military and organising large-scale exercises and troop movements. The attempts to scare Western societies with the prospect of war were supplemented with "peace" initiatives that were usually difficult for the Alliance to accept.[10] At one point, the USSR even expressed readiness to join NATO, creating a dilemma for the allies how to reject the proposal.[11] Moscow also regularly called for disarmament but mainly to impose limitations on democratic states and achieve

[9] "Active Measures: A Report on the Substance and process of Anti-U.S Disinformation and Propaganda Campaigns," United States Department of State, August 1986, http://insidethecoldwar.org:60080/8db6e0057c6ee2bb765ddf9fc595559eb7726f7d/522aeaa1-3146-e428-143c-9222c614ae6a/tap2_2y4GE0_dec/Soviet%20Active%20Measures%20Substance%20and%20Process%20of%20Anti-US%20Disinformation%20August%201986.pdf (accessed 10.10.2022).

[10] See: *The United States Permanent Representative on the North Atlantic Council (Hughes) to the Department of State, Foreign Relations of the United States, 8 April 1954*, https://history.state.gov/historicaldocuments/frus1952-54v05p1/d257 (accessed 12.08.2022).

[11] G. Roberts, *Molotov's Proposal that the USSR Join NATO, March 1954*, Cold War International History Project, Wilson Centre, www.wilsoncenter.org/publication/molotovs-proposal-the-ussr-join-nato-march-1954 (accessed 12.08.2022).

superiority over the West. The Kremlin came out with arms-reduction initiatives but did not agree to the introduction of verification mechanisms, without which such agreements would not make sense. When the negotiations stalled, it blamed the U.S. and NATO, claiming that they were interested only in keeping their military superiority over the armies of the USSR and its satellites.

The USSR also used propaganda to influence elections in NATO states. In 1984, the Kremlin tried to stop Ronald Reagan from being re-elected, coming up with the slogan "Reagan means war". Trying to discredit Reagan and complicate Spain's accession to NATO, Soviet agents also forged a letter from President Reagan that suggested that he was exerting pressure on the King of Spain Juan Carlos to "deal with the opponents of his country's membership in the Alliance".

One of the most spectacular examples of Soviet propaganda was a campaign against the development of a neutron bomb at the turn of the 1970s and 1980s. In response to the intense increase in Soviet military power (including the deployment of SS-20 missiles), NATO was ready to support the U.S. production and deployment of this new type of nuclear weapon. Due to the reduced explosive power and enhanced radiation it could be more effective in killing enemy troops while limiting the scale of material destruction. Its greater usefulness could increase the risk that it could be used on the battlefield, strengthening deterrence. The USSR launched an aggressive propaganda campaign against the "weapons of the imperialists" saying they care more about material goods than human life. The narrative was supported with massive demonstrations of peace and anti-nuclear movements across the NATO states.

The USSR approached propaganda and disinformation in a systematic and scientific manner. In order to increase the ability to influence the policies of other countries, the theory of "reflexive

control" has been developed.[12] The Soviet Union also tried to maximise its influence through so-called active measures, which covered a wide span of clandestine practices, including propaganda and disinformation operations, political influence efforts, and activities of foreign communist parties or other organisations supporting Soviet goals.[13] Since the regime had a monopoly on the distribution of information and the state structures were highly centralised, information activities were usually well-coordinated. The message was approved at a high political level, presented during official speeches of the leaders (public or secret) and then directed by appropriate institutions to specific audiences in NATO countries. All the means of communication available at that time were used to disseminate the message: press, television, radio, leaflets, and posters. The KGB played a significant role as it was responsible for the application of "active measures" and had its own agents placed not only in diplomatic missions around the world but also posing as correspondents of Soviet media, which offered them better access to influential people.[14] The KGB maintained close links with the International Department of the Central Committee of the Soviet Communist Party (CPSU), which was responsible for information activities directed especially at socialist parties, trade unions, and peace organisations in other countries. The USSR is said to have been able to influence hundreds of foreign organisations.[15]

[12] T.L. Thomas, "Russia's Reflexive Control Theory and the Military," *Journal of Slavic Military Studies*, 2004, no 17, pp. 237–256.

[13] D. Kux, "*Soviet Active Measures and Disinformation: Overviews and Assessment*," *The U.S. Army War College Quarterly: Parameters*, 1985, no 1, https://press.armywarcollege.edu/cgi/viewcontent.cgi?article=1388&context=parameters (accessed 1.10.2022).

[14] Ch. Andrew, O. Gordievsky, *Instructions from the Centre…*, *op. cit.*, p. 3.

[15] J. Darczewska, P. Żochowski, "Active measures. Russia's key export," , Point of View, no 64, www.osw.waw.pl/en/publikacje/point-view/2017-05-30/active-measures-russias-key-export (accessed 2.10.2022).

Natural Soviet "allies" in exploiting information for political influence were the foreign peace and anti-nuclear movements, which exerted political pressure on Western governments, obstructing investment in military potential without similar effect in the USSR. Some activists, artists, academics, and journalists were agents of influence who consciously supported Soviet goals. One of these numerous such agents was Danish citizen Arne Herlov Petersen, who maintained contacts with the KGB and disseminated Soviet propaganda proposals, including for a nuclear-free zone in Northern Europe. Those who were supporting Soviet goals inadvertently were sometimes dubbed "useful idiots".[16]

Soviet leaders used important international conferences and diplomatic negotiations to stage propaganda attacks, increasing the chances that these messages would find their way to a foreign audience. Since Soviet-controlled media had limited influence on the western audience and the USSR was a country that was not easily accessible to foreigners, the privilege of entry and direct contact with the leaders was offered to those who gave a chance to publicise Soviet propaganda abroad: sympathetic journalists, representatives of trade unions, or political parties sharing the goals of the CPSU. The rare privilege of interviewing the Soviet leader guaranteed that the message would be on the frontpage of foreign newspapers.

Effectiveness of Soviet Information Operations

The effectiveness of the Soviet propaganda and disinformation against NATO is difficult to measure. It seems that the results were ambiguous at best. Aggressive attempts to strengthen control over the new sphere of influence in Central and Eastern Europe after World War II even proved counterproductive. The USSR provoked

[16] J. Hackett, *The Third World War. Untold Story*, Sidgwick & Jackson, London 1985, p. 31.

the United States to adopt a strategy of containment and provide substantial economic and military aid to the states of Western Europe. Russia has failed to achieve its main goal of pushing the U.S. out of Europe. The exaggeration of military capabilities additionally prompted the U.S. to develop its military potential and stimulated an arms race that the Soviet economy was unable to cope with. Soviet disinformation often proved too cumbersome to have positive results. The KGB did not manage to convince a single Western journalist to pick up the slogan "Reagan means war". Spanish media also quickly recognised that the letter supposedly written by Reagan to the King of Spain was a KGB operation. The same goes for the forged letter of the Danish "general".

However, it cannot be excluded that attempts to influence the internal politics of NATO states and to undermine NATO's cohesion were to some extent effective. Denmark and Norway, consistently refused to host NATO troops, infrastructure, or nuclear weapons on their territory throughout the Cold War. Soviet political and military pressure, supported with propaganda and disinformation, deepened the divisions and tensions within NATO to such an extent that the Allies decided to complement defence and deterrence with the policy of détente. On the one hand, such policy lowered political tensions and helped to some extent neutralise hostile Soviet narratives about NATO aggressiveness and preparation for war. But on the other hand, it was perceived by the Soviet leadership as exceptionally beneficial, as it allowed for a relative strengthening of the position of the communist superpower vis-à-vis the West.[17]

One of the biggest propaganda successes was the anti-neutron bomb campaign, which was accompanied by massive protests from anti-war movements and made the U.S. abandon its plan to

[17] G.S. Barrass, *The Great Cold War. A Journey Through the Hall of Mirrors*, Stanford University Press, 2009, p. 288.

deploy such weapons in Europe.[18] The success, however, proved to be short-lived. The Soviet success strengthened NATO's resolve to implement a "double-zero" policy. The Allies agreed to deploy Pershing II ballistic missiles and ground-launched cruise missiles in Europe, which increased the risk that during a conflict Soviet territory could be attacked. At the same time, they offered to scrap the plans in return for a complete withdrawal of these types of weapons from Europe. The USSR launched an aggressive campaign against the so-called "Euromissiles", trying to stop the NATO deployment and offering a moratorium on further deployment of this type of missiles.[19] With this propaganda stunt, the Kremlin tried to enforce a change in NATO's policy, while maintaining its own military advantage. Despite significant pressure from peace movements, NATO stuck to its policy. Faced with the new NATO weapons, the Kremlin agreed to sign the Intermediate Nuclear Forces (INF) treaty, banning the deployment of missiles with ranges between 500 and 5,500 km in Europe. This concession reflected the accelerating erosion of the Soviet state, which collapsed a couple of years later.

The End of the Cold War—In Search of a New Narrative

After the reunification of Germany in 1990, the collapse of the USSR in 1991, and a short period of political and economic reforms, Russia's elites started to adjust their strategic goals to the new post-Cold War realities. Russia was substantially weakened

[18] S.D. Symms, E.D. Snow Jr., "*Soviet Propaganda and the Neutron Bomb Decision*," *Political Communication*, 1981, pp. 257-268.

[19] T. Agres, "Soviets Seek to Discredit Alliance with Accusation of Counterbuildup," *Washington Times*, 25 November 1983, CIA Archives, www.cia.gov/readingroom/docs/CIA-RDP90-00806R000100130002-4.pdf (accessed 13.08.2021), "Soviet Propaganda on U.S. forces in Europe," FBIS Analysis Group, 4 January 1983, CIA Archives, www.cia.gov/readingroom/docs/CIA-RDP09-00997R000100480001-6.pdf (accessed 13.08.2022).

and its goals included regaining the position of a regional and global power, strengthening the multipolar system (which meant undermining the dominant position of the U.S.), and blocking or delaying the expansion of the Alliance.[20] Unable to completely stop NATO's enlargement, Russia tried to influence the transformation of the Alliance into a collective security organisation, but one which would not offer credible security guarantees to its members, especially the new ones.[21] Such goals implied that Russia, as in the past, wanted to maintain a buffer zone on the territory of the former satellite states and increase its chances of reintegration of the former Soviet republics. While NATO has imposed numerous restrictions on the deployment of troops and infrastructure in the new member states, Russia's goals towards NATO have not changed.

Attempts to achieve the strategic goals were supported by propaganda directed at the U.S. and NATO. One of the main narratives in Russian disinformation campaigns has been the myth of a broken promise not to enlarge NATO, allegedly made during the talks on the reunification of Germany.[22] NATO was presented as an obstacle to a stable international security system. Although NATO imposed some self-limitations on the deployment of troops to new member states and attempted to build partnership with

[20] See, e.g.: M. Gorbachev, *Gorbachev. On My Country and the World,* Columbia University Press, New York 1999, p. 203, "*The Basic Provisions of the Military Doctrine of the Russian Federation*, adopted by edict No. 1833 of the president of the Russian Federation, dated 2 November 1993, https://fas.org/nuke/guide/russia/doctrine/russia-mil-doc.html (accessed 14.08.2021), *National Security Concept of the Russian Federation*, approved by Presidential Decree No. 24 of 10 January 2000, www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/589768 (accessed 14.08.2022).

[21] R.D. Asmus, *Opening NATO's Door. How the Alliance Remade Itself for a New Era*, Columbia University Press, New York 2002, pp. 105-106.

[22] *Ibidem*, p. 142; R. Kupiecki, "Mit założycielski polityki zagranicznej Rosji," *Sprawy Międzynarodowe*, vol. 72, no 4, pp. 77–105.

Russia, Kremlin argued that the policy of enlargement (the "open-door policy") created new division lines in Europe and further increased the risk of confrontation.

After Putin came to power in 1999, the propaganda efforts against NATO became increasingly hostile. To stir anti-NATO sentiments, the Kremlin presented NATO as an aggressive alliance that was encircling Russia and preparing for war.[23] In 2007, during a conference in Munich, Putin launched a passionate attack against the West, criticising NATO expansion, U.S. military presence in the new member states, development of a missile-defence system in Europe, interventions without UN approval, and interference in the internal affairs of other countries.[24] At the 2008 NATO summit in Bucharest, he warned that the inclusion of Ukraine and Georgia in the Membership Action Plan (a NATO programme that facilitates the necessary reforms before accession) would pose a direct threat to Russia.[25]

Trying to block NATO enlargement, Russia attacked Georgia in 2008, effectively using propaganda to accuse the Georgian president of provoking the conflict and weakening NATO's response. In 2014, it annexed Crimea and fuelled a conflict in the eastern part of Ukraine. Russia again resorted to propaganda and disinformation, presenting its own aggressive actions as justified self-defence. It claimed that annexation of Crimea was a legitimate action because NATO tried to draw Ukraine into the Alliance, wanted to create military bases in Crimea, and encouraged a popular uprising in

[23] "NATO-Russia Relations: the facts," NATO, 5 October 2021, www.nato.int/cps/en/natohq/topics_111767.htm#Myths (accessed 5.10.20221.)

[24] *Speech and the Following Discussion at the Munich Conference on Security Policy*, President of Russia, 10 February 2007, http://en.kremlin.ru/events/president/transcripts/24034 (accessed 14.08.2022).

[25] R. Kupiecki, M. Menkiszak (eds.), *Documents Talk. NATO-Russia Relations After the Cold War*, Polski Instytut Spraw Międzynarodowych, Warszawa 2020, pp. 384–391.

Ukraine to oust a legitimately elected president. As in the past, the Russian propaganda was often directed at individual NATO states that were perceived as the weak links of the Alliance. After the annexation of Crimea, Putin directly addressed Germany, referring to Russian consent to the reunification and to the myth of the broken promise not to enlarge NATO.

To block NATO enlargement in the Balkans, in 2016, Russia attempted to overthrow the government in Montenegro ahead of the referendum on NATO membership. It also tried to undermine a possible agreement between Greece and the government in Skopje, which was necessary to unblock the prospects of NATO membership for the Macedonian state. Such actions were supported with propaganda and disinformation about NATO. The narratives included the accusations that NATO was weak, divided, hegemonic, aggressive, and its policy of enlargement (open-door policy) increased the risk of war.

The attempts to block NATO expansion were supplemented with the proposal of building a new "stable" security system, which would help Russia strengthen its position at the expense of the security of smaller neighbours.[26] In 2008, the then-president, Dmitri Medvedev, presented the concept of a new European security treaty that would give Russia the possibility to block sovereign decisions of other states under the pretext of a threat to Russia's security interests.[27] In 2014, after Russia's annexation of Crimea, Putin directly referred to the 1945 Yalta

[26] The first such attempt was made in 1993 by President Boris Yeltsin, who in a letter to U.S. President Bill Clinton suggested the creation of a security system based on guarantees offered by major powers to former Soviet satellite states. As the proposal was not revealed by Russia, it should not be perceived as propaganda. R. Kupiecki, M. Menkiszak (eds.), *Documents Talk..., op. cit.*, pp. 129–131.

[27] Y. Fedorov, "Medvedev's Initiative: A Trap for Europe?," *Research Paper*, 2009, no 2, Association for International Affairs, www.amo.cz/wp-content/uploads/2015/12/amocz-RP-2009-2.pdf (accessed 14.08.2022).

agreement, which divided Europe into spheres of influence, as a positive solution that brought stability to Europe.[28] Just like during the Cold War, Russia tried to promote its strategic goals by influencing a threat perception among NATO populations. Russia started to deploy new military capabilities and intensified manoeuvres near the Alliance's borders.[29] It openly threatened some NATO states with nuclear weapons and tried to highlight its military and technological superiority over the Alliance.[30] When in response to Russia's aggressive behaviour NATO deployed small, multinational military units to Poland and the Baltic States, the Kremlin resorted to the narrative that the presence of these troops breaks international agreements and threatens Russia. NATO's defensive actions were further exploited as a pretext and justification for the mobilisation of Russian forces, which was clearly done to intimidate neighbours.[31] By blaming NATO for the increased risk of conflict, the Kremlin tried to divide the Alliance, paralyse its ability to strengthen its defences and maintain a military advantage over NATO. When the U.S. decided to withdraw from the INF treaty in response to continued Russian violations of the agreement, Kremlin used Leonid Brezhnev's tactics and proposed a moratorium on the deployment of banned

[28] *Meeting of the Valdai International Discussion Club 2015*, President of Russia, 22 October 2015, http://en.kremlin.ru/events/president/news/50548 (accessed 14.08.2022).

[29] A. Wilk, "The Zapad-2017 exercises: the information war (for now)," *OSW Commentary*, 4 September 2017, www.osw.waw.pl/en/publikacje/osw-commentary/2017-09-04/zapad-2017-exercises-information-war-now (accessed 20.08.2022).

[30] "Russia threatens to aim nuclear missiles at Denmark ships if it joins NATO shield," *Reuters*, 22 March 2015, https://www.reuters.com/article/us-denmark-russia-idUSKBN0MI0ML20150322 (accessed 14.08.2022).

[31] "Russia says buildup at Ukraine border is a response to NATO 'threats'," *Euronews*, 13 April 2021, *Euronews.*, www.euronews.com/2021/04/12/g7-calls-on-russia-to-cease-provocations-on-ukraine-border (accessed 13.10.2022).

missiles, which would have limited the Alliance's possibilities to respond in kind, consolidating Russia's military superiority in these types of weapons. During the COVID-19 pandemic, Russia was well-prepared to exploit new opportunities to undermine NATO cohesion. When the Italian government's request for help fell on the deaf ears of its allies, the Russian army quickly delivered medical supplies to Italy. Even though it was insignificant in practical terms, the Kremlin made every effort to make it highly visible, labelling the operation "From Russia with love". Russia also claimed that NATO failed to support the Allies during the pandemic, that the virus was produced by the CIA, and that COVID-19 is spread by NATO troops.[32]

Although Russia uses some old tactics, it has skilfully adapted its propaganda tools to the new strategic and technological realities related to the development of the internet, social media, and satellite television. Since 2000, Russia's strategic documents have underlined the threats in the information domain.[33] The Kremlin again accused the West of using information warfare and presented this as a pretext to take counteraction. After a short period of media independence, the Russian authorities took control of major TV stations in the country and strengthened their control over news agencies. In 2005, the Kremlin-controlled state media established the English-language Russia Today satellite television station, which was later renamed RT to hide its associations with the Russian government. The Sputnik information service was created, which has, among others, internet portals in nine language versions. The efficiency of these information operations was additionally increased by "troll factories", companies

[32] "Russia's Top Five Myths about NATO and Covid-19," NATO Factsheet, April 2020, www.nato.int/nato_static_fl2014/assets/pdf/2020/4/pdf/2004-Factsheet-Russia-Myths-COVID-19_en.pdf (accessed 13.10.2022).

[33] *National Security Concept* (2000), *op. cit.*

employing hundreds of people and using thousands of automated social media accounts ("bots"), responsible for promoting specific content on the internet. This offered Russia unprecedented ability to influence political debates and even the results of elections in NATO member states.[34]

The Effectiveness of Russian Propaganda and Disinformation

The effectiveness of Russian propaganda in the post-Cold War era is again difficult to measure. Among the most spectacular proof that propaganda and disinformation are much more effective than during the Cold War was Russia's ability to influence the results of the 2016 U.S. elections. It probably also helped delay NATO enlargement in the 1990s. Although declassified documents and reports by Soviet leader Mikhail Gorbachev himself clearly indicate that the promise not to enlarge NATO was not made, the narrative had some visible effect. Influential experts and scientists were willing to support the Russian point of view and present NATO enlargement as an unnecessary provocation and a justification for its aggressive policy, although they did not offer a credible alternative to the post-Cold War security system.

But the long term results of propaganda and disinformation are less obvious. Despite Russia's pressure, the Alliance has admitted 14 new countries since the end of the Cold War, growing to 30 members in total. NATO also continued the open-door policy that allowed any country from the Euro-Atlantic area to join the Alliance, provided that certain conditions are met. Even though

[34] *Report of the Select Committee on Intelligence United States Senate on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election, Volume 2: Russia's Use of the Social Media with Additional Views*, 116th Congress, https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf (accessed 13.10.2022).

the membership of Georgia and Ukraine seems unlikely in the foreseeable future, the open-door policy indicates that NATO does not accept a security system based on spheres of influence, as promoted by Russia. Since Russia's illegal annexation of Crimea, NATO also has continued its policy of strengthening defence and deterrence. Nevertheless, Russian propaganda may be effective in influencing the Allies' calculations regarding the risk of provoking Russia. This in turn makes it more difficult for democratic states to build the consensus necessary for the development of military potential and collective-defence mechanisms, including the deployment of troops and infrastructure on the territory of eastern NATO member states. How much Russian information operations will affect the policies of individual states and further adaptation of the Alliance to changing strategic and security realities remains an open question.

JAN MISIUNA
Institute of International Studies
Warsaw School of Economics
ORCID 0000-0002-3663-2697

Disinformation and Elections: A Case Study of U.S. Presidential Campaigns

This text discusses disinformation activities undertaken in connection with the presidential elections in the United States in 2016 and 2020. Its purpose is to show forms of disinformation, its evolution, and the importance of the attitudes of state and corporate authorities in counteracting it. The informative and illustrative value of this example remains significant.[1] We have rich sources of knowledge about the election campaigns resulting from investigations conducted by, among others committees of the U.S.

[1] See, e.g.: K. H. Jamieson, *Cyberwar. How Russian Hackers and Trolls Helped Elect a President: What We don't, Can't and Do Know*, Oxford University Press, New York 2018, Y. Benkler, R. Faris, H. Roberts, *Network Propaganda: Manipulation, Disinformation, and Radicalisation in American Politics*, Oxford University Press, New York 2018.

House of Representatives,[2] the Senate,[3] and the Special Counsel,[4] which were undertaken following a joint U.S. intelligence report.[5]

It is difficult to overestimate the importance of the election process for the legitimacy of the entire political system in a democratic state. For this reason, all disinformation activities aimed at the electoral system are in fact attacks aimed at the essence of the system itself, lead to its destabilisation, and in the extreme case, to its delegitimisation. The open nature of the election campaign in the United States,[6] conducive to public debate, is also responsible for difficulties in defending against disinformation activities aimed at the election process. Thus, what constitutes the strength of democracy as a political system is also the cause of its weakness when disinformation is introduced into the system. In recent years, the U.S. presidential elections have been the target of organised, planned disinformation campaigns conducted by both extra-systemic and intra-systemic entities. However, the intensity of these actions, the conditions in which they were carried out, their effectiveness, and the dominant entities changed.

[2] U.S. House of Representatives, Permanent Select Committee on Intelligence, *Russia Investigation Transcripts and Documents*, https://intelligence.house.gov/russiainvestigation (accessed 12.01.2022).

[3] *Report of the Select Committee on Intelligence United States Senate on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election*, Vol. I-V, Washington D.C. 2019-2020.

[4] R. S. Mueller, III, *Report On The Investigation Into Russian Interference In The 2016 Presidential Election*, Vol. I–II, U.S. Department of Justice, Washington, D.C., 2019.

[5] Intelligence Community Assessment, *Assessing Russian Activities and Intentions in Recent US Elections*, ICA 2017-01D, 6 January 2017, www.dni.gov/files/documents/ICA_2017_01.pdf (accessed 12.01.2022).

[6] The open nature of the election campaign in the USA manifests itself in the multiplicity of broadcasters of electoral messages and the relatively low threshold that an organisation or group must overcome to join this group.

Disinformation in the 2016 Presidential Campaign

The 2016 presidential election campaign is an example of effective disinformation activities undertaken primarily by external entities. In the reports prepared by investigative committees, the Special Counsel and academic researchers, there is unanimity that a key role in introducing untrue information into the public debate and social media was played by entities commissioned by, or part of, Russian intelligence organisations. The aim of the measures taken was to defeat the Democratic Party candidate for the office of the U.S. president, Hillary R. Clinton, who was considered a worse alternative from the perspective of the interests of the Russian Federation compared to the Republican Party candidate, Donald J. Trump. A kind of "consolation prize" in the event of the Democratic Party's candidate winning would have been the undermining of the credibility of the election process itself. The scale of the Russian operations undertaken in connection with the 2016 presidential elections in the U.S. was so large that, according to Kathleen Hall Jamieson, they at least partially met the criteria of cyberwarfare.[7] Their effectiveness was high due to the Russians playing the strengths of the American political system against itself, such as the protections of freedom of press and speech, lax regulation of media and political communication, as well as the marketing potential of social media.[8]

As a result of the high political polarisation of the American society, the effectiveness of disinformation activities has increased. A kind of feedback loop took place here: polarisation fostered the effectiveness of disinformation, and effective disinformation enhanced polarisation. Among the factors increasing the

[7] Cyberwar is understood by her as "actions taken by one country to penetrate computers and networks in another country to inflict damage or disruption", see K. H. Jamieson, *op. cit.*, p. 7.

[8] *Ibidem*, p. 11.

effectiveness of disinformation against the U.S. presidential election in 2016, it is worth mentioning the very method of conducting the elections, which, thanks to the Electoral College, with electors chosen in almost all states based on the state-wide majority system, enables—seemingly contradictory—minimising the importance of the will of the majority of the entire electorate.[9]

It should be emphasised that the 2016 election campaign was obviously not the first one in which foreign entities tried to influence the outcome of U.S. elections.[10] However, the technological shift that has taken place in election campaigns and information distribution in the United States in the 21st century, especially since Barack Obama's first presidential campaign in 2008, have opened up new opportunities for determined actors who are not afraid to risk and take advantage of emerging opportunities.[11] What is also of great importance, the new opportunities to influence the course of election campaigns and the election results did not require making large financial investments. This made it possible not only to carry out wide-ranging activities, but also to differentiate them according to the audience, which in turn could increase the effectiveness of the entire disinformation campaign.

[9] In the 2016 elections, the Democratic Party candidate obtained almost 3 million more votes than the Republican Party candidate, which, however, did not give her the majority of votes in the Electoral College. Se: Federal Election Commission, *Federal Elections 2016: Election Results for the U.S. President, the U.S. Senate and the U.S. House of Representatives*, Washington, D.C., December 2017, www.fec.gov/resources/cms-content/documents/federalelections2016.pdf (accessed 12.01.2022), p. 5.

[10] C. Walton, "'Active measures': a history of Russian interference in US elections," *Prospect*, 23 December 2016, www.prospectmagazine.co.uk/science-and-technology/active-measures-a-history-of-russian-interference-in-us-elections (accessed 12.01.2022).

[11] On the importance of opportunism in the foreign policy of the Russian Federation during the reign of Vladimir Putin, see F. Hill, C. G. Gaddy, *Mr. Putin: Operative in the Kremlin*, Brookings Institution Press, Washington, D.C. 2015.

Russia's disinformation activities during the 2016 presidential election campaign can be divided into those aimed directly at ordinary voters and those aimed at opinion leaders, mainly journalists. In both cases, the goal was to bring about a behaviour change, but the nature of the change was different. While in the first case it was only about election behaviour—voting for one of the candidates, not necessarily Trump, or causing election absenteeism—the second goal was to change the content of current affairs and news programs, i.e., distract journalists (and through them, voters) from information that presented Trump in a negative light and instead focus on issues difficult for Clinton, thus causing a change in electoral behaviour. The best example of such action is the coverage of the scandal related to the recording of Trump's comments regarding women (the Access Hollywood tapes) by the publication on WikiLeaks of content stolen from Democratic Party servers.[12]

Although the primacy in conducting disinformation campaigns during the election campaign before the U.S. presidential election in 2016 is attributed to organisations acting on behalf of Russian intelligence services, this does not mean that other entities remained passive. A special case of deliberate disinformation activities were those undertaken by Trump's election committee, which were designed to lead to electoral absenteeism among Democratic Party voters. While the employees of Trump's election committee defined their actions as voter suppression,[13] understood as discouragement to participate in elections, and not according to the classic definition of limiting the possibility of exercising the

[12] K. H. Jamieson, *op. cit.*; Part Two and Part Three, pp. 67-189.

[13] J. Green, S. Issenberg, "Inside the Trump Bunker, With Days to Go," *Bloomberg Businessweek*, 27 October 2016, www.bloomberg.com/news/articles/2016-10-27/inside-the-trump-bunker-with-12-days-to-go (accessed 12.01.2022).

right to vote,[14] and placed them in the area of a negative election campaign, their *modus operandi* clearly puts these activities within the disinformation framework. Perhaps this is the point where it is worth asking when and where exactly ordinary political marketing activities and disinformation converge. Although it is not too difficult a task to develop criteria that make it possible to distinguish relatively precisely between them, even in quite complex cases, it is beyond the scope of this text.

Disinformation in the 2020 Presidential Campaign

The scale and extent of disinformation during the presidential election campaign in 2016 constituted a point of reference for assessing the threat to the electoral process in the United States before the election campaign leading up to the 2018 elections to Congress and also before the 2020 presidential election campaign. However, both the 2018 and 2020 election campaigns were not simple repetitions of the one from 2016: they differed not only in terms of the scale and scope but also the nature of the disinformation activities carried out. While during the previous presidential election campaign, the foreign entity that undoubtedly played the most important role was the Russian Federation and organisations acting on its behalf, during the 2020 election campaign, the number of countries that decided to engage in disinformation activities aimed at the American election process rose. Moreover, each of them had slightly different goals that they wanted to achieve. Neither American intelligence agencies nor research centres have yet submitted full reports on the disinformation actions during

[14] See J. Misiuna, "Ograniczenie możliwości korzystania z czynnego prawa wyborczego (voter suppression) a wybory w USA w 2016 r.," [in:] A. Bielecki, D. Szarfrański, T. Gąsior (eds.), *Problemy prawa polskiego i obcego w ujęciu historycznym, praktycznym i teoretycznym. Część ósma*, Wydawnictwo C.H. Beck, Warszawa 2017, pp. 113–122.

the 2020 election campaign, but available studies indicate that, in addition to Russia, China and Iran also tried to play an important role in influencing the outcome of U.S. elections. In the September 2020 opinion of the National Counterintelligence and Security Center, the difference between the goals that the countries engaged in actions against the U.S. wanted to achieve was as follows: "China works to discredit U.S. President Donald Trump, Russia is aiming to undermine Democratic presidential nominee Joe Biden".[15] Supporting or attacking a candidate is not the only form of involvement by other countries in the 2020 election campaign. From the point of view of the stability of the political system and its legitimacy, disinformation activities by entities linked to the Russian Federation that aimed at undermining the fairness of the elections themselves and the credibility of their official results were much more important. In pandemic conditions, with many states extending mail and absentee voting, it was precisely these methods of voting that was discredited by Russia's actions.[16]

The disinformation that was introduced into the American public debate by foreign entities during and after the election campaign—especially in the period between the elections and the swearing-in of the new president—was accompanied by an exceptional intensive disinformation campaign conducted by internal actors, as well as by candidates in the elections, their co-workers and surrogates. The dissemination of disinformation undermining the credibility of the American electoral system became the leitmotif of President Donald Trump's 2020 election campaign. This does not mean, however, that he had not previously voiced similar opinions: four years earlier, as a presidential

[15] E. Braw, "The Real Hacking Threat," *Foreign Policy*, 25 September 2020, https://foreignpolicy.com/2020/09/25/real-hacking-threat-foreign-election-interference-2020 (accessed 12.01.2022).

[16] *Ibidem*.

candidate, he questioned the fairness of the conduct elections, and the history of his similar public statements as a private citizen goes back to at least 2012.[17] As mail voting was being expanded due to the pandemic, the number of misinformation messages sent by the incumbent president grew,[18] but the climax did not come until after Election Day. It was then that not only the president but also his associates began a large campaign to undermine the results of the elections, both in public appearances and in court. In the period after the presidential elections, they disseminated false information about mail voting, the counting of votes (from the work organisation point of view),[19] and the way in which the ballots were counted (particularly the devices used).[20]

It is difficult to assess the scale of the disinformation—both endogenous and exogenous—regarding the course of the U.S. election process in 2020. There is no doubt, however, about its effectiveness. While Cybersecurity and Infrastructure Security Agency (CISA), the federal government agency responsible

[17] L. Qiu, "Donald Trump's baseless claims about the election being 'rigged'," *Politifact*, 15 August 2016, https://www.politifact.com/factchecks/2016/aug/15/donald-trump/donald-trumps-baseless-claims-about-election-being (accessed 12.01.2022).

[18] Starting in spring 2020, an increasing concentration on the possibility of voter fraud could have been observed in D.J. Trump's statements, see: L. Jacobson, "Donald Trump's dubious claim that 'thousands' are conspiring on mail-ballot fraud," *Politifact*, 9 April 2020, https://www.politifact.com/factchecks/2020/apr/09/donald-trump/donald-trumps-dubious-claim-thousands-are-conspiri (accessed 12.01.2022).

[19] D. Funke, C. Hendrickson, L. Jacobson, N.Y. Kim, I. Strauss, "Fact-checking Trump's election fraud falsehoods in White House remarks," *Politifact*, 5 November 2020, https://www.politifact.com/article/2020/nov/06/fact-checking-falsehoods-trumps-nov-5-election-rem (accessed 12.01.2022).

[20] J. Easley, "More conservatives break with Trump over election claims," *The Hill*, 20 November 2020, https://thehill.com/homenews/administration/526938-more-conservatives-break-with-trump-over-election (accessed 12.01.2022).

for ensuring the cybersecurity of the electoral process, has consistently contradicted all claims of mass-scale voting fraud in the 2020 elections[21] due to activities of foreign entities, as did state agencies responsible for organising voting, in December 2020 as many as 34% of Americans did not believe in the integrity of the results of the presidential election, and an additional 5% expressed doubts. At the same time, confidence in the election results clearly correlates with political sympathies: as many as 72% of the supporters of the Republican Party believed that the elections were fraudulent, while as many as 95% of supporters of the Democratic Party were of the opposite opinion.[22] Thus, it can be concluded that the goal of discrediting the American electoral system and deepening political polarisation, set by the secret services of the Russian Federation through the joint—though uncoordinated—effort of Russian intelligence services, their subsidiaries, and Trump's election campaign, was achieved.

Conclusions

When analysing the disinformation activities carried out during the 2020 election campaign, it is worth focusing on the change in approach to the phenomenon on the part of the U.S. federal administration, technology corporations and the president himself compared to 2016. Reports and statements by the heads of federal agencies responsible for cybersecurity and security in the course

[21] Which ultimately led to the termination of its head by President Trump, who disagreed with the CISA reports, see: M. Gstalter, "Krebs says allegations of foreign interference in 2020 election 'farcical'," *The Hill*, 27 November 2020, https://thehill.com/homenews/administration/527795-krebs-says-allegations-of-foreign-interference-in-2020-election (accessed 12.01.2022).

[22] D. Montanaro, "Poll: Just A Quarter Of Republicans Accept Election Outcome," *National Public Radio*, December 9, 2020, https://www.npr.org/2020/12/09/944385798/poll-just-a-quarter-of-republicans-accept-election-outcome (accessed 12.01.2022).

of elections, such as CISA or the National Counterintelligence and Security Center, cited in this text, clearly point to long-term, large-scale activities, coordinated with state governments, to prepare for and protect against cyberattacks directed against election administrations in individual states, as well as to close observation of the actions taken by those responsible for the disinformation campaign four years earlier. Actions taken by federal agencies and state governments become even more important when contrasted with the attitude of the president himself (Trump), who clearly did not consider disinformation a problem in the election process; on the contrary, he willingly used it himself. The activity of the federal administration during the 2020 election campaign, especially in the field of information policy, also stands out against the 2016 election campaign, when the Obama administration, having data on disinformation activities carried out by entities related to the Russian Federation, decided not to make them public before Election Day, so as not to be accused of trying to influence the voting process. In 2020, the presence in the public debate of documents prepared by agencies responsible for the security of the election process, as well as statements by the heads of these agencies, was manifest precisely in order to influence the course of voting: to counter disinformation activities by strengthening awareness of the problem.

However, probably for the majority of people looking for information on the internet, especially in social media,[23] the most important change was the marking by the largest platforms, such as Facebook, Twitter, and YouTube, of posts on elections as

[23] The internet is the primary source of information on politics for 43% of Americans, of which for 18% it's social media, see: A. Mitchell, M. Jurkowitz, J.B. Oliphant, E. Shearer, "Americans Who Mainly Get Their News on Social Media Are Less Engaged, Less Knowledgeable," Pew Research Center, July 2020, p. 3, www.journalism.org/wp-content/uploads/sites/8/2020/07/PJ_2020.07.30_social-media-news_REPORT.pdf (accessed 12.01.2022).

requiring extreme caution and verification, as well as suspending and deleting accounts responsible for deliberate and consistent disinformation. While the decisions to suspend and delete accounts by platform administrators have raised controversy and questions as to whether freedom of expression is being restricted in the name of the fight against disinformation, it seems that they should rather be viewed as a form of accountability by tech corporations for how tools created by them are used. Even if, in the end, the effectiveness of these actions turns out to be lower than those attributed to them by both supporters and opponents of this type of administrative activity undertaken by technology companies, with a high degree of social polarisation, any attempt to moderate sentiment, including by limiting the possibilities of active and deliberate disinformation, is very valuable from the perspective of not only the election process but also the everyday functioning of the state and society.

JĘDRZEJ CZEREP
Polish Institute of International Affairs
ORCID 0000-0002-4709-1582

Illusion of Attractiveness: Russia's Pursuit of a Success Story in Africa

While Russia's engagements with Africa have been on the rise in the last decade, culminating in hosting the first Russia-Africa Summit in Sochi (2019), the relationship continues to be largely superficial. Russia's goals on the continent had most of the time been fluid and opportunistic, therefore there has not been any clear strategic vision of Africa's role in the country's foreign policy. Still, Russia is quickly expanding its footprint on the continent, in large part thanks to the vigour with which it engages with the infosphere inside and across Africa. Its focus seems to be on strengthening perceptions of Russia as a viable alternative to the Western powers on the continent, primarily France. To this end, Russia has employed several disinformation tools supporting its soft power repertoire to build an image that would resonate positively among local elites and populations. Its messaging aimed at African audiences through media and political discourse involves

a set of continuously repeated themes that make up an apparently coherent—although largely false—narrative regarding local and international developments. Its core is that *the West*, continuing with the *colonial approach*, is *destabilising*, and *neglecting* African states and peoples, while *Russia*, a supporter of *Pan-Africanism*, works to make them *truly independent*, strong, and *developed*.[1] Those tropes exploit deep resentments held by many Africans, particularly that of a lack of justice and respect, for which they often blame the unfair socio-political setting cemented by the postcolonial order. Russia would be playing on those undertones in building its own story of being a serious *alternative*, which proved to be effective in various African contexts.

Russia's attempts to influence perceptions and sentiments among the populations and decision-makers of African states partly derive from its experience in other parts of the world, but it also has its peculiarities. While in relation to the West, the prime goal of Russian disinformation campaigns is to sow discord, undermine public trust, and deliberately strengthen false beliefs to weaken the "enemy" states from within,[2] that is most often not the case in Africa. As Russia sees other global powers as competitors on the continent, and African states as potential partners where it can seek business opportunities and influence, it is interested in seeing them as friendly, functional and stable (preferably authoritarian) rather than in chaos. Therefore, disinformation is not the goal in itself but one of many forms of engagement in the infosphere—instabilities are to be exploited not deepened.

[1] K. Svoboda, P. Matlach, Z. Baddorf, "Russia's Activities in Africa's Information Environment," NATO Strategic Communications Centre of Excellence, December 2020, pp. 20–26.

[2] M. L. Taylor, "Combating disinformation and foreign interference in democracies: Lessons from Europe," *Brookings*, 31 July 2019, www.brookings.edu/blog/techtank/2019/07/31/combating-disinformation-and-foreign-interference-in-democracies-lessons-from-europe (accessed 12.02.2022).

This intersects with specific local contexts. The state of tension in which many African countries remain creates conditions in which the populations are in the mode of constantly pursuing pieces of seemingly relevant information. Those in "survival mode"[3] tend to latch onto rumours or otherwise unreliable sources particularly easily, and where formal media are not trustworthy, it is easier to propose what seems to be a quality alternative.

While the Russian state typically applies its policies through a top-down, hierarchical structure, in Africa, the decision-making processes in building desired perceptions seem to be much more decentralised.[4] This is due to the special position of some individuals, formally not affiliated to the Kremlin, which are the drivers of the Russian presence in Africa. Their positions in promoting Russia's interests are largely autonomous and their endeavours in politicising information sometimes start spontaneously before becoming more or less structured and included into the state machinery. Thus, the successes in opening the gateways are not always followed by the employment of proper policies, and the frames for using information are in a constant state of re-making.

Russia has been able to turn some of its limitations into an asset: it presents its combination of lack of experience on the ground with adaptivity to changing realities as a *no-bias* approach. Aligning with isolated leaders (such as Sudan's Omar al-Bashir, the Democratic Republic of Congo's [DRC] Joseph Kabila, or Eritrea's Isaias Afewerki) on the one hand, has placed Putin

[3] M. LeRiche, "Facebook and Social Media Fanning the Flames of War in South Sudan," Centre For Security Governance, 12 July 2016, https://secgovcentre.org/2016/07/facebook-and-social-media-fanning-the-flames-of-war-in-south-sudan (accessed 18.01.2022).

[4] A. Mackinnon, "The Evolution of a Russian Troll," *Foreign Policy*, 10 July 2019, https://foreignpolicy.com/2019/07/10/the-evolution-of-a-russian-troll-russia-libya-detained-tripoli (accessed 12.11.2022).

within the "club of the dictators", but on the other, may strengthen Russia's reputation as not following the global "imperialist" or "neo-colonial" mainstream politics in Africa. To overcome those paradoxes, Russia's engagement with the continent has developed into a multi-dimensional effort to build a perception of the Russia as Africa's honest and attractive partner.

Setting Agendas for the Public Debate

Russian state-supported media initially focused on North Africa where RT Arabic and Sputnik Arabic, widely exploiting anti-Western sentiments, became the main channels for influencing pro-Russian sentiments. The Arabic-language Russian media have been generating more online content than its main competitors—in 2018, RT Arabic released more than 500,000 tweets, doubling that of Al Jazeera and outnumbering Al Arabiya and BBC Arabic, and eagerly adapting to young audiences' needs by becoming more smartphone-friendly.[5] This focus on youth apparently produced a growing intergenerational divide in views on Russia in North Africa: in 2020, 24% more young adults in Tunisia and Libya saw Russia positively than their older compatriots.[6] Following this path, French-language editions of RT and Sputnik have been widening the outreach[7], and becoming increasingly

[5] A. Borshchevskaya, C. Cleveland, "Russia's Arabic Propaganda. What It Is, Why It Matters," *Policy Note* 57, The Washington Institute for Near East Policy, 2018, pp. 2–4.

[6] C. Huang, J. Cha, "Russia and Putin receive low ratings globally," 7 February 2020, *Pew Research*, https://www.pewresearch.org/fact-tank/2020/02/07/russia-and-putin-receive-low-ratings-globally (accessed 12.01.2022).

[7] This priority was explicitly stated by Xenia Fedorova, the president of RT France, in a March 2019 interview to *Jeune Afrique*. See: J. Crétois, "Forte de son succès sur le web, RT France lance son offre HD à destination du Maghreb," *Jeune Afrique*, 9 March 2019, www.jeuneafrique.com/745388/economie/fort-de-

popular, in French-speaking Sub-Saharan African states.[8] RT placed a correspondent in Tunis and in September 2021 launched the "Africonnect" programme aimed at African audiences.[9] The process further accelerated after the EU banned access to those media after the Russian invasion of Ukraine in 2022—having lost audiences in France, they further focused on French-speaking Africa.[10] RT, through TV-Novosti, sought agreements to share its content and statistics, such as documentaries and analytics, with African media outlets to further accelerate the reach of its messaging.[11]

Following the Russian full-scale invasion of Ukraine on 24 February 2022, such moves have increasingly been supported by Russian diplomacy. While initially, RT planned to set up its main African office in Nairobi, in July 2022 it announced plans for a hub for English-speaking broadcasts to be located in Johannesburg—a politically friendly environment and in an apparent attempt to overcome EU- related ban by MultiChoice Group Ltd., Africa's biggest pay-TV provider.[12] It was to be headed by Paula Slier, a South African journalist, whose experience includes SABC News

son-succes-sur-le-web-rt-france-lance-son-offre-hd-a-destination-du-maghreb (accessed 1.10.2022).

[8] K. Svoboda, P. Matlach, Z. Baddorf, "Russia's Activities ...," *op. cit*.

[9] A. Dassonville, "Le continent africain dans le viseur de la chaîne russe RT," *Le Monde*, 28 March 2022, www.lemonde.fr/economie/article/2022/03/28/le-continent-africain-dans-le-viseur-de-rt_6119392_3234.html (accessed 10.10.2022).

[10] In possible anticipation of the consequences of the forthcoming invasion, in January 2022 RT registered several new domains, such as rt-afrique.com, africa-rt.com, rtafrica.media, and rtafrica.online.

[11] "Proceedings of the panel, 'The Role of Media in Russian-African Relations'," Russia-Africa Economic Forum, 23 October 2019, https://roscongress.org/en/sessions/africa-2019-rossiysko-afrikanskie-otnosheniya-rol-smi/discussion (accessed 7.10.2022).

[12] A. Sguazzin, "Banned in Europe, Kremlin-Backed RT Channel Turns to Africa," *Bloomberg*, 22 July 2022, https://www.bloomberg.com/news/

and as RT's Middle East Bureau chief posted in Jerusalem.[13] Shortly after, Russian Foreign Minister Sergei Lavrov's July Ethiopia visit, Sputnik signed a memorandum of cooperation with the Ethiopian News Agency.[14]

The influence of the Moscow-based media outlets is supplemented by extensive coverage of Russia-Africa issues, within the frames of its narratives, by a number of African journalists with links to both Russia-controlled and neutral, mainstream African channels. Many of these writers were based in Russia for a longer time or studied in Russia before coming back to their home countries. They were particularly active before the Sochi summit in 2019 where RT, Sputnik, and TASS welcomed African journalists for training programmes. This trend continued, and its latest example—at the time of writing—involved the workshop "Media Wars and Fake News: How to Fight Disinformation", held in Addis Ababa for Ethiopian journalists in October 2022 and conducted by Vasily Pushkov, Sputnik's director of international cooperation.[15] Through African journalists' reporting, even extreme pro-Kremlin, and overtly false stories could have spread far beyond the bubble of Russian media producers and consumers. One example is Oman Mbiko, whose texts mixing disinformation with pro-Kremlin narratives about Africa were published by the South Africa-based mainstream CAJNews and later re-published

articles/2022-07-22/banned-in-europe-kremlin-backed-rt-channel-turns-to-africa#xj4y7vzkg (accessed 9.10.2022).

[13] T. Ferreira, "Russia's RT channel eyes African expansion with SA headquarters," *News24*, 26 July 2022, www.news24.com/channel/tv/news/russias-rt-channel-eyes-african-expansion-with-sa-headquarters-20220726 (accessed 10.10.2022).

[14] "Sputnik expands cooperation with African media," *Rossiya Segodnya*, 6 October 2022, https://rossiyasegodnya.com/20221006/312298.html (accessed 18.10.2022).

[15] "Sputnik expands ...," *op. cit.*

by AllAfrica, the biggest accelerator of African news media.[16] A more coherent channel spreading pro-Russian narratives developed with the convergence of interests between the head of the Cameroon-based pan-African Afrique Média TV station, Justin B. Tagouh, and Russia. As Tagouh lost government funding (his preferred business model) from Equatorial Guinea and Chad, he approached Russia with the help of a Belgian pro-Russian far-right activist, Luc Michel, who used Tagouh's media as a platform for anti-Western statements. The Afrique Média channel (and its affiliated *International Afrique Média* magazine) promotes Russia as a preferred partner and a true friend. As part of its collaboration with Tagouh, Russia declared financing the establishment of a pan-African radio station, Radio Révolution Panafricaine (2RP) to broadcast to at least 12 countries, and is likely to further influence an alliance of like-minded African media houses, Conseil Africain des Médias, over which Tagouh also presides.[17] Not all the moves like that work. The short-lived Malabo-based Africa Daily Voice (ADV), a would-be pan-Africa information agency headed by the Ivorian spin doctor Toussaint Alain, launched in 2018 only to become known for arguing, later that year, with the fact-checking website AfricaCheck about the sources of fake news incorrectly attributed to it.[18]

[16] J. Disalvatore, "Central African Republic Media Platforms Push Prigozhin's Pro-Putin Agenda," *Kharon*, 06 October 2020, https://brief.kharon.com/updates/central-african-republic-media-platforms-push-prigozhin-s-pro-putin-agenda (accessed 10.9.2022).

[17] B. Roger, G. Dougell, "Russia-Africa: Behind the scenes of Moscow's soft power," *The Africa Report*, 29 July 2021, www.theafricareport.com/112950/russia-africa-behind-the-scenes-of-moscows-soft-power (accessed 11.9.2022).

[18] T. Alain, "Right of reply: African Daily Voice did not publish these false stories," *Africa Check*, 18 December 2018, https://africacheck.org/fact-checks/blog/right-reply-african-daily-voice-did-not-publish-these-false-stories (accessed 10.11.2020).

Apart from the formal media channels, social media, most notably Facebook, have been instrumentalised to help spread pro-Russian narratives, support Russia's local allies, or counter its regional and global competitors (such as the EU, U.S., and France). Accounts imitating African news sites and research centres, some run by African influencers themselves, are being set up to promote and amplify pro-Russian opinions or influence outcomes of elections. For example, in Madagascar, at least 10 such channels were active in 2019, some taking on an international look (Afrique Panorama), some mimicking national outlets (Ino maresaka eto Madagasikara [What's Happening in Madagascar]) or local news sources (Les échos de Tana, Les échos de Mahajanga, etc).[19] Such attempts have been noted in more than a dozen states across the continent,[20] most intensively throughout 2018-2019. Sham "election observation" missions involving invited far-right and far-left activists from several European countries have been dispatched to Zimbabwe, Madagascar, the DRC, South Africa, and Mozambique under the umbrella of the Association For Free Research And International Cooperation (AFRIC),[21] co-run by a Mozambican academic, the psychologist José Matemulane, and the Kremlin-linked Yulia Afanasieva. An echo of this form of engagement was heard again in September 2022 when youth league of the South African ruling party (African National Congress) sent "observers" to the illegal annexation referendums in the Doneck and Zaporizhzia regions. Leader of the group,

[19] S. Grossman, D. Bush, R. DiResta, "Evidence of Russia-Linked Influence Operations in Africa," *Stanford Internet Observatory*, 29 October 2019, pp. 33–35.

[20] I. Rozhdestvensky, M. Rubin, R. Badanin, "Master and Chef. How Russia interfered in elections in twenty countries," *The Project*, 11 April 2019, www.proekt.media/investigation/russia-african-elections (accessed 9.12.2022).

[21] "Treasury Escalates Sanctions Against the Russian Government's Attempts to Influence U.S. Elections," U.S. Department of the Treasury, 15 April 2021, https://home.treasury.gov/news/press-releases/jy0126 (accessed 23.6. 2022).

Khulekani Skosana, described them as "a beautiful, wonderful process" and enthusiastically defended it in the Russian, and later in South African media[22]. Tapiwa Masenda, a Zimbabwean ruling party activist, served similar role in Kherson and provided reports to the TASS agency.[23]

The social media coverage amplifying certain narratives and the popularity of chosen candidates was supplemented on the ground by the work of so-called "political technologists".[24] These operatives engaged directly with political actors and had been dispatched by Yevgeny Prigozhin, a Russian oligarch infamous for controlling St. Petersburg's Internet Research Agency (IRA), a "troll factory", and Alexander Malkevich, formerly the head of the U.S.-based disinformation website USAReally, then founder of the increasingly Africa-oriented quasi-think tank Foundation for National Values Protection (FZNC).[25] Both became informal, and largely autonomous, enforcers of the Kremlin's activities in the infosphere, while Prigozhin also held patronage over mercenary and extractive businesses in Africa. In the runup to elections expected

[22] P. Fabricius, "A beautiful, wonderful process—ANCYL defends sending observers to Russia's sham referendums in Ukraine", *Daily Maverick*, 28 September 2022, www.dailymaverick.co.za/article/2022-09-28-a-beautiful-wonderful-process-ancyl-defends-sending-observers-to-russias-sham-referendums-in-ukraine (accessed 6.12.2022).

[23] "All conditions in place at Kherson referendum—observer from Zimbabwe," *TASS*, 27 September 2022, https://tass.com/politics/1514217 (accessed 26.9.2022).

[24] P. Goble, "Moscow Exporting 'Political Technologists' Beyond Africa to Europe," *Eurasia Daily Monitor* Volume: 16 Issue: 128, The Jamestown Foundation, 19 September 2019, https://jamestown.org/program/moscow-exporting-political-technologists-beyond-africa-to-europe (accessed 23.8.2022).

[25] Later on, the presidency of the centre was assumed by a Russian sociologist and officially "not a spy" Maxim Shugaley, famous for his imprisonment in Libya after holding talks with the fugitive Saif al-Islam Gaddafi in Russia's name. The story of his Libyan odyssey was depicted in a series of feature films. After his return to Russia, Shugaley became the "face" of the FZNC.

in Libya in 2019—but eventually not held—can serve as an example of an electoral influencing exercise combining online and offline means. In this case, Russia supported a candidate re-entering the political race, Saif-al-Islam, the son of the country's deposed leader, Col. Muammar Gaddafi. Shortly after Saif's representatives travelled to Moscow in December 2018, a Facebook profile named "Mandela Libya" was set up. In the course of a month, it was liked by more than 100,000 accounts, the majority of them fake.[26] Its content quickly started generating more reactions than those of his competitors, or other public personalities. "Mandela Libya" aggressively promoted fake opinion polls showing massive support for its candidate. A very similar scheme of "electoral support" was used a few months later in Mozambique. Again, a last-minute fake electoral poll giving the incumbent Felipe Nyusi a landslide victory, published by another Russian quasi-think tank, the International Anticrisis Centre (IAC), was intended to discourage his opponents.[27] As in Libya, Russian involvement seemed to have been sealed during the Mozambican president's visit to Moscow in August 2019,[28] shortly before elections, as part of a transactional package: political aid to the embattled leader for the promise of lucrative contracts.[29]

[26] "Libya Social Media Monitoring Report December 2018-January 2019," Democracy Reporting International, www.democracy-reporting.org/libya-social-media-report/january/(accessed 23.8.2022).

[27] D. Tsandzana, "Has Russia influenced the general elections in Mozambique?," *Global Voices*, 23 December 2019, https://globalvoices.org/2019/12/23/has-russia-influenced-the-general-elections-in-mozambique (accessed 7.12.2022).

[28] "Rosneft signs agreements on offshore gas field development with Mozambique," *TASS*, 22 August 2019, https://tass.com/economy/1074649 (accessed 23.8.2022).

[29] In Mozambique, the Russian semi-private military company known as the Wagner Group surprisingly won a contract to assist the army in the fight against Islamist insurgents, and Rosneft was promised access to offshore gas fields.

A different way of extending influence comes with Malkevich's and Maxim Shugaley's FZNC. Through its African Discussion Club, it provides a scientific backup to pro-Russian views in Africa. It engages in sociological research in African states (most often in Libya) and publishes reports and policy papers in Russian, English, French, and Arabic in which it promotes the theory that the West is intentionally "lowering the belt of instability" from North to sub-Saharan Africa and fuelling "colourful revolutions"[30] via politicians bought in through scholarships.[31] It argued that Russia, on the contrary, emerged as a stabilising force. In practical terms it meant supporting authoritarian shifts (Guinea), paramilitary strongmen (Sudan) or military rule (West Africa). In late 2020 and early 2021, it conducted interviews in the CAR, Sudan, Chad, and Nigeria to identify the impact of "hybrid warfare" apparently launched by the West against the stability of those countries and publicised polls pointing to Russia's alleged attractiveness on the continent.[32] The African Discussion Club positioned itself as a resource base for African researchers.

Unlike posts by traditional or scientific publications, those produced for short-lived social media channels ended up being ephemeral. As the pattern of creating artificial online traffic to affect political sentiments in Africa has become obvious, in

[30] A. Malkevich, "L'histoire sombre des «révolutions colorées» en Afrique," FZNC, 22 August 2019, https://fr.fznc.world/2019/08/22/l-histoire-sombre-des-revolutions-colorees-en-afrique-l-opinion-d-aleksandr-malkevitch (accessed 23.8.2022).

[31] N. Ponomarev, "Yale 'boot camp' for African politicians," FZNC, 22 August 2019, https://en.fznc.world/2019/08/22/yale-boot-camp-for-african-politicians (accessed 23.8.2022).

[32] "Нигерия: страна, которая может остаться без жителей," FZNC, 1 April 2021, https://fznc.world/afrikanskij-klub/nigeriya-strana-kotoraya-mozhet-ostatsya-bez-zhitelej/; "ЦАР: жители страны не доверяют Франции и ООН," FZNC, 21.06.2021, https://fznc.world/afrikanskij-klub/czar-zhiteli-strany-ne-doveryayut-franczii-i-oon (accessed 7.7.2022).

October 2019 Facebook removed more than 200 Prigozhin-linked social media accounts and other channels reaching one million users in Madagascar, Cameroon, CAR, Mozambique, the DRC, Côte d'Ivoire, Sudan, and Libya.[33] Another, similar clean-up by Facebook took place in December 2020. Contents published on multiple highly influential and otherwise informative accounts (such as CAR's Soutien à la Russie en RCA) disappeared after the removals. Also, apparently more solid structures tended to disintegrate under the pressure of negative coverage—both AFRIC and IAC, conducting election-related observation and influencing activities, practically ended public activity,[34] even discontinuing maintenance of their websites. Still, in real-time, such outlets provided and others continue to provide constant validations for pro-Russian narratives among sections of the grassroots audiences who adopt views presented as theirs.

Co-Opting the Like-Minded

Propagating Russia's declared role in Africa and in the world requires a common understanding of the reality with some established African intellectuals and other influential figures. Their authority, popularity, and charisma help to internalise some pro-Russian voices within the African public discourse, which is often informal. Apparently, collusion was found with some radical elements of the pan-Africanist movement for whom a Russia-supported vision of a multipolar world of sovereign entities, and the rebranded version of anti-colonialism and anti-imperialism seemed particularly appealing. Kémi Séba, a Pan-Africanist

[33] N. Gleicher, "Removing More Coordinated Inauthentic Behavior From Russia," Facebook, 30 October 2019, https://about.fb.com/news/2019/10/removing-more-coordinated-inauthentic-behavior-from-russia (accessed 7.7.2022).

[34] M. Bajek, P. Szczepaniak, "Travel Agency 'Eye of Sauron'," *VSquare*, 4 August 2021, https://vsquare.org/travel-agency-eye-of-sauron (accessed 27.09.2022).

activist, and self-made politician from Benin, was until 2017 mostly known for calling for the abolishment of the post-French CFA franc currencies in West and Central Africa. Later on, he gradually became a key Russian agent of influence. In December 2017, he was invited to Russia and introduced to Alexander Dugin, the theorist of Euro-Asianism. Later, Séba recalled to Sputnik that, "Russia, thanks to people like Dugin, is in the process of constructing a super-powerful Eurasian axis that plays a role maintaining the different sovereignisms in the world (...). It's up to us, African sovereigntists to turn Africa into this powerful pole as the founding fathers of pan-Africanism so desired".[35]

Dugin himself wrote a preface to Séba's 2019 book *L'Afrique Libre ou la Mort* (*Free Africa or Death*) in which he compared the author to Patrice Lumumba and Thomas Sankara, giants of French-speaking Africa's liberation, and framed his activism as a globally relevant part of the struggle for a multipolar world.[36] Russian support to a rebranded pan-Africanism developed naturally due to many similarities to the Russian World (Russki Mir) construct,[37] for example, in the notion of pan-African consciousness and as an element of the multipolar world. It allowed Russian operatives to help fill it with ready-made content and structures and to expect it to become an incubator of new, Russia-friendly opinion leaders whose conviction would allow them to withhold internal

[35] M. Gamandiy-Egorov, "Kemi Seba: souverainistes africains et Russie, «une alliance naturelle»," Sputnik France, 22 December 2017, https://fr.sputniknews.com/points_de_vue/201712221034454553-kemi-seba-souverainistes-africains/ (accessed 9.11.2022).

[36] A. Dugin, "Kemi Seba, African hope of a multipolar world", [in:] K. Seba, "L'Afrique Libre ou la Mort", Fiat-Lux éditions, 2019.

[37] L. Harding, J. Burke, "Leaked documents reveal Russian effort to exert influence in Africa," *The Guardian*, 11 June 2019, https://www.theguardian.com/world/2019/jun/11/leaked-documents-reveal-russian-effort-to-exert-influence-in-africa (accessed 23.6.2022).

contradictions and paradoxes of the Russian narratives they would reproduce.

Séba became a routine guest on Russian media outlets RT and Sputnik. In 2019, he was brought to Madagascar before the elections to heat up the long dormant issue of the Scattered Islands. This French-owned archipelago on the Mozambique channel is considered by some in Madagascar to be disputed territory between the two countries. Séba spoke at the conference entitled "Islands of Hope", organised by Prigozhin's team at the Asia and Africa Hotel in Antananarivo. There, he shouted: "France, get out of our territory, you have no right to be here! Africans trust Russia more than America or France!" Then, he led a demonstration of about 30 people (apparently paid to attend) to the front of the French Embassy.[38] According to leaked files from Prigozhin's informal analytical centre, it identified Séba's NGO, Urgences Panafricanistes, as Russia's key ideological ally, and approved a strategy to expand its network of offices (from 12 countries in 2019 to the target of 26).[39]

Despite the apparent end of the formal cooperation around 2020 due to his resistance to restricting his independence, Séba remained one of the main African promoters of Russia's interests. By 2021, he was particularly vocal in steering anti-French sentiments in Mali, working together with the *Yéréwolo* Movement (calling to "liberate" the country from "French imperialism"), which itself was subject to Russian penetration.[40] Following the January 2022 coup d'état in Burkina Faso, which came after similar moves in Mali and Guinea, he attempted to put an intellectual frame to what he described as the emergence of a new order in Africa, born from the

[38] "Paradise Lost? Russia's Madagascar Election Gamble," *BBC Africa Eye*, 08 April 2019, www.bbc.co.uk/programmes/n3ct5chm (accessed 23.6.2022).

[39] I. Rozhdestvensky, M. Rubin, R. Badanin, "Master and Chef...," *op. cit.*

[40] B. Roger, G. Dougell, "Russia-Africa...," *op. cit.*

alliance of "sovereignist military and a pan-African civil society", which he hoped would continue to overthrow democratic, pro-Western orders in the entire French-speaking Africa.[41] Following Russia's invasion of Ukraine, which he was quick to endorse using opaque anti-imperialist arguments, Séba was received in Moscow in early March 2022 by a top Africa diplomat, the vice minister of foreign affairs, Mikhail Bogdanov of the MGIMO university,[42] and others as one of the few convinced, trusted allies considered key in facilitating a positive reception of Russia's "confrontation with the West". He was also made a star of the MGIMO-held conference involving top Russian officials dealing with Africa in October 2022.[43] Reports from his Russian trips have been enthusiastically followed by his sympathisers.

The likewise pro-Russian flavour of pan-Africanism has been promoted by a Swiss-Cameroonian activist, Nathalie Yamb, a vocal opponent of French influence on the continent and the author of popular YouTube films exploring the international contexts of African politics. Her Facebook page, with more than 433,000 followers in 2022 was illustrated with a background photo of herself speaking at the 2019 Africa-Russia summit[44] where she attacked France and some African governments for continuing what she called a quasi-colonial mode of relationship and

[41] Kemi Seba, Facebook post, 31 January 2022, https://www.facebook.com/KemiSebaOfficial/posts/482405629920508 (accessed 23.6.2022).

[42] "Russie-Afrique: de Kemi Seba à Nathalie Yamb, les « influenceurs » pro-Poutine du continent," *Jeune Afrique*, 31 March 2022, www.jeuneafrique.com/1335015/politique/russie-afrique-de-kemi-seba-a-nathalie-yamb-les-influenceurs-pro-poutine-du-continent (accessed 2.5.2022).

[43] "A Moscou, Kemi Seba cible françafrique et appelle à un partenariat juste avec la Russie," video posted on Kemi Seba's Facebook profile, 25 October 2022, www.facebook.com/watch/?v=677614766924092 (accessed 29.10.2022).

[44] A recording of the speech is also pinned on her Twitter account (https://twitter.com/nath_yamb), which has 136,000 followers.

advocated for Russia to replace France with a more partner-like approach.[45] As a consequence of her provocative activism, she was deported from Côte d'Ivoire where she had resided for the past decade and advised a local opposition party leader. Tweeting from the deportation flight on 2 December 2019, she wrote: "History will prove us right, the fight continues!"[46] From that time on, she proudly refers to herself as the "Lady of Sochi"[47], and banned from entering France, she painted herself as a would-be-martyr for the cause.[48]

The duo pioneering the new brand of pro-Russian pan-Africanism was lately joined by Cameroonian Paul Ella, a self-proclaimed "geostrategist" (director of the poorly visible African Centre on Research of Geostrategy) and president of the African Revival movement, first listed in mid-2021 by Jeune Afrique as one of Moscow's top committed influencers in Africa.[49] He routinely spreads conspiracy theories (e.g., "plandemic"), promoted the pro-Russian Malian junta, calls on Africans to boycott Western media (e.g., RFI, France 24, LCI, BFM TV, BBC, VOA, CNN, EURONEWS)

[45] "Summary of the proceedings of the panel 'The Future of the African Continent: Sovereignty and Traditional Values as Crucial Elements of a Development Strategy'," Russia Africa Forum, 24 October 2019, https://roscongress.org/en/sessions/africa-2019-obraz-budushchego-afrikanskogo-kontinenta-suverenitet-i-traditsionnye-tsennosti-kak-vazhnye-elementy/discussion (accessed 20.11.2022).

[46] Nathalie Yamb, Tweet, 2 December 2019, https://twitter.com/Nath_Yamb/status/1201636295350587394 (accessed 20.12.2019).

[47] Nathalie Yamb, Facebook profile, www.facebook.com/NathalieYambOff.

[48] "Je sais", Nathalie Yamb's Facebook post, 17 October 2022, www.facebook.com/NathalieYambOff/posts/pfbid02z4eZx0jDBVQrJj5fjrxh1Ja7 9DUxDpUBYG7qbWaw14NDEuwSTSYgnhgzTPE5iYPGl (accessed 2.11.2022).

[49] F. Soudan, "Pourquoi les Africains doivent devenir machiavéliques," *Jeune Afrique*, N°3103, 2 August 2021, https://www.jeuneafrique.com/1205170/politique/pourquoi-les-africains-doivent-devenir-machiaveliques-par-francois-soudan/(accessed 29.11.2021).

and to reverse their perspective on who is a true friend (Russia) and enemy (the West). His association had been preparing the launch of its own pan-African TV channel[50] and follows in Séba's footsteps in organising anti-French rallies in Cameroon. On 11 December 2021, his movement hosted the first edition of the Pan African Awards. This Oscars-like gala in Douala attracted some 1,000 guests from across the continent and the diaspora. Multiple notable pro-Russian personalities were nominated in 22 categories, including "opinion leader" (won by Séba), "political analyst" (awarded to Banda Kani, head of the Cameroonian party Nouveau Mouvement Populaire, which by 2022 had become something of a transmission belt for Russian propaganda), "TV station" (Afrique Media), "media influencer", "comic", etc.[51] In 2022, Ella started hosting a radio show "Chronique de Paul Ella" on Radio Révolution Panafricaine where he often spreads Russia's views on global events using pan-African references to elevate his popularity and influence.

Similar undertones of sovereignism and pan-Africanism had been visible on the surface of the Ghanaian NGO called Eliminating Barriers for Liberation of Africa (EBLA). It was used as a front for 2019-2020 operations of Ghanaian and Nigerian "troll factory" franchises targeting mostly African-American, and to a lesser extent African audiences. Its founder, Seth Boampong Wiredu, alias "Amara", was believed to have studied and worked in Russia as an associate of Prigozhin's IRA.[52] If the work of EBLA was not ended by the alarmed authorities, some of the Ghanaian

[50] African Revival, Facebook post, 8 January 2022, www.facebook.com/africanrevivalo/posts/pfbid02sXjDernkmyztq CSg6NmwKRPoTyNqpAGgAvh8jbjr64eH2ZffssYWpWT50RY77GD2l (accessed 2.3.2022).

[51] Soirée de Gala, African Revival Facebook profile, 11 December 2021, https://fb.watch/dNwA-_SRrw (accessed 20.12.2021).

[52] C. Ward, K. Polglase, S. Shukla, G. Mezzofiore, T. Lister, "Russian election meddling is back, via Ghana and Nigeria, and in your feeds," *CNN*,

or Nigerian students attracted by the pan-Africanist posture of the organisation could have eventually become Russia's local agents of influence.

Another increasingly influential convicted Pan-Africanist who adopted pro-Russian narratives was the media-savvy Sylvain Afoua, also known as Egountchi Behanzin (after the 19th-century king of Abomey who resisted colonisation). This France-based leader of the Black Lives Matter-styled Black-African Defence League was originally vocal in denouncing white racism in France and in comparing France-influenced Africa to a concentration camp.[53] But by 2022, he focused on fraternising with pro-Russian figures from Mali to South Africa and promoted anti-Ukrainian conspiracies, such as accusing Ukraine of being a U.S.-controlled aggressor in the war against Russia,[54] or of allegedly hiding President Volodymyr Zelensky at the U.S. embassy in Poland.[55]

Messages of these "new", sometimes amateurish, opinion leaders tended to be elevated to a new level once embraced by established moral authorities. In an interview with for the TV5 Monde promoting his album, the legendary Ivorian reggae singer Alpha Blondy hailed Kémi Séba and Nathalie Yamb as truthtellers when describing Africa's submission to the West as modern slavery.[56] In

12 March 2020, https://edition.cnn.com/2020/03/12/world/russia-ghana-troll-farms-2020- ward/index.html (accessed 15.3.2022).

53 H. Oukili, "Qui est Egountchi Behanzin, l'homme qui est allé menacer "Valeurs actuelles"?", *Causeur*, 8 September 2020, www.causeur.fr/egountchi-behanzin-ldna-valeurs-actuelles-181494 (accessed 15.10.2020).

54 A commentary on AfrqiueMedia TV, reposted in Egountchi Behanzin's Twitter post, 13 October 2022, https://twitter.com/EgountchiLdna/status/1580580918267297793 (accessed 15.10.2022).

55 Egountchi Behanzin's Twitter post, 22 October 2022, https://twitter.com/EgountchiLdna/status/1583843095623319552 (accessed 25.10.2022).

56 L'invité, *TV5 Monde*, 17 June 2022, www.tv5monde.com/emissions/episode/l-invite-alpha-blondy-1 (accessed 15.8.2022).

the chat with the increasingly confused programme host, Patric Simonin, Blondy's universal, pro-justice appeal, for which he had gained respect and a unique status of a peace "ambassador" across the continent, was mixed with wild conspiracy theories such as that of the French allegedly arming Sahelian jihadists or speaking with ambiguity about the war in Ukraine. A similar boost to Russia's image on the continent came with the September 2022 coup in Burkina Faso, heavily accompanied by anti-French and pro-Russian rhetoric. In this context, Mariam Sankara, widow of Thomas Sankara, the country's leftist revolutionary president in the 1980s, remembered as one of the most inspiring, charismatic, and uncorrupted African leaders, published an open letter that commented on current issues. She stressed the need to first support Burkina's own strengths but added that "honest and credible partners" should be called in, if necessary.[57] While Mariam Sankara stopped short of openly embracing pro-Russian Pan-Africanism and its vocal messengers, reading between the lines of her letter offered Russia a trans-generational blessing and a boost in credibility.

Some heavyweight political figures joined—with conviction—the choir of promoters of Russia's role as a kind of messianic avenger, a destroyer of the old, U.S.-dominated world. These included Uganda's Muhoozi Kainerugaba, the erratic son of the country's president and the then-commander of its land forces. After the Russian invasion started, he tweeted that Putin was "absolutely right" to repulse the alleged NATO expansion and that "the majority of mankind (non-whites) support Russia's stand in Ukraine".[58] The statement came in the context of the reports

[57] "Lutte contre le terrorisme au Burkina: Mariam Sankara propose d'aller vers d'autres partenaires," *ActuBurkina*, 15 October 2022, https://actuburkina.net/lutte-contre-le-terrorisme-au-burkina-mariam-sankara-propose-daller-vers-dautres-partenaires (accessed 19.10.2022).

[58] Muhoozi Kainerugaba's Twitter post, 28 February 2022, https://twitter.com/mkainerugaba/status/1498094460580016128 (accessed 15.3.2022).

of mistreatment of African students struggling to leave Ukraine and in the runup to the Ugandan takeover of the presidency over the Non-Allied Movement. The Russian embassy thanked him by publishing graphics of Kainerugaba modelled on the Barack Obama "Hope" poster on his birthday.[59] In South Africa, Duduzile Zuma-Sambudla, daughter of the populist ex-president Jacob Zuma, used her Twitter account, which is followed by 200,000 people, to popularise the hashtag "#Istandwithrussia".[60] Also, the influential far-left South African Economic Freedom Fighters (EFF) party's leader, Julius Malema, jockeyed to encourage Russia to "teach them [NATO and the U.S.] a lesson" so that a new world order emerges,[61] while his deputy, Floyd Shivambu, in a parliamentary debate stated there was "nothing wrong with preventing imperialist expansion of NATO" and assured that the Russians "do not target civilians or civilian infrastructure."[62] These and other cases further mainstreamed the notion that Russia was the right bet in the looming global confrontation.

Another kind of alignment was being achieved through Russia's posturing as the defender of traditional values against Western "novelties", particularly the LGBTQ+ rights through forums such as the World Family Congress (WFC). The WFC was founded by

[59] Russian Embassy in Uganda Twitter post, 24 April 2022, https://twitter.com/RusEmbUganda/status/1518094160376565760 (accessed 1.5.2022).

[60] "Russia-Africa: From Kemi Seba to Duduzile Zuma-Sambudla, the continent's pro-Putin 'influencers'," *The Africa Report*, 7 April 2022, www.theafricareport.com/191778/russia-africa-from-kemi-seba-to-duduzile-zuma-sambudla-the-continents-pro-putin-influencers (accessed 15.6.2022).

[61] "Quels sont les réseaux pro-russes en Afrique?", *TV5 Monde*, 9 April 2022, https://afrique.tv5monde.com/information/quels-sont-les-reseaux-pro-russes-en-afrique (accessed 15.6.2022).

[62] R. Chanson, "War in Ukraine: Malema's party in South Africa acts as Russia's mouthpiece," *The Africa Report*, 21 March 2022, www.theafricareport.com/186080/war-in-ukraine-malemas-party-in-south-africa-acts-as-russias-mouthpiece (accessed 15.6.2022).

U.S. and Russian conservatives in 1997 to become an influential vehicle for supporting anti-LGBTQ+ sentiments across the world. Until recently, it used to be dominated by wealthy U.S. Protestant movements with heavy outreach to Africa (including Uganda, Zambia, and Zimbabwe).[63] However, since 2010, it has been increasingly influenced by prominent Russians, such as the Putin-trusted "Orthodox oligarch" Konstantin Malofeev, who is also one of the driving forces of Russia's push into Africa. Since 2019, he has led the International Agency for Sovereign Development (IASD). This new investment group with informal links to the Russian MFA, aimed to assist African states in achieving "economic independence".[64]. In practice, its non-transparent partnerships are used to avoid sanctions on Russian companies.[65] The IASD composed its narrative by mixing "traditional values" and the supposed "Western plot against Africa"[66] with heavy Soviet-era nostalgia. Malofeev was a financier of the 2018 WFC annual conference in Chisinau, Moldova, the agenda of which was dominated by speeches by high-level Russian politicians and ideologues, but notably involved prominent Africans.[67] Among

[63] L. Whyte, "US and Russian religious Right unite against 'invasion of radical liberalism'," *Open Democracy*, 26 September 2018, www.opendemocracy.net/en/5050/us-and-russian-religious-right-unite-against-radical-liberalism(accessed 15.3.2022).

[64] C. Okeke, "Pan-Africanism in Foreign Policy," *The Republic*, 8 March 2021, https://republic.com.ng/february-march-2021/pan-africanism-in-foreign-policy (accessed 5.4.2022).

[65] M. Maldonado, "Russia's Hardest Working Oligarch Takes Talents to Africa," *Ponars Eurasia*, 28 September 2020, www.ponarseurasia.org/russia-s-hardest-working-oligarch-takes-talents-to-africa (accessed 12.10.2022).

[66] Such was the title and the leitmotif of Melofeev's presentation during the Sochi summit. Another visible Africa-focused IASD representative shuttling the continent is Kirsan Ilyumzhinov, the eccentric but well-connected ex-president of the Kalmyk Republic.

[67] "Anti-LGBT hate group World Congress of Families to gather in Moldova this week," SPLC (Southern Poverty Law Center), 12 September 2018,

them was Theresa Okafor, director of the African Cultural Heritage Foundation, who led the campaign to criminalise homosexuality in Nigeria and suggested links between LGBTQ+ activists and Boko Haram terrorists, and the Malawian MP Justin Majawa, who was denouncing pressure from bilateral aid donors who would "seek to promote same-sex marriage rights" in his country.
In at least one instance, Russian "political technologists" attempted to exploit the potential of highly influential and media-savvy pastors of the new, African Pentecostal megachurches. Apart from performing charismatic, "miracle-making" services, they routinely discuss political developments, oppose LGBTQ+ rights, and have a record of spreading conspiracy theories.[68] This made them fit for potential roles as "transmission belts" for disinformation disguised as promoting morality. In Madagascar in 2019, Russian operatives approached Pastor André Mailhol, leader of the Apocalyptic Church, claiming to have 1.5 million followers and 1,000 churches. He was offered support in covering the expenses of his eventually unsuccessful presidential campaign.[69] It is likely that pattern could be explored more in the future.

The Central African Republic (CAR): A *Success Story* Constantly in the Re-Making

Flexibility, actively shaping public opinion and turning its newcomer status into an asset can best be illustrated by Russia's experience in the CAR. Russia hardly had any relations with the country prior to 2016. The lack of progress in solving the post-2012

www.splcenter.org/hatewatch/2018/09/12/anti-lgbt-hate-group-world-congress-families-gather-moldova-week-reveals-details-last (accessed 15.11.2019).

[68] P. A. Ikem, C. N. Ogbonna, C. N. Nwoke, "Pentecostalism and Electoral Politics: A Projection of Nigeria's Soft Power in Africa," *Covenant University Journal of Politics & International Affairs*, Vol. 7, No. 2, Dec. 2019.

[69] "Paradise lost? ...," *op. cit.*

civil conflict, marred by increasing fragmentation of armed groups, solidification of social and religious divisions, and lack of a developmental agenda on the side of the CAR authorities, made international players frustrated and unwilling to engage. The presence of UN forces was haunted by repeated scandals involving sexual exploitation, and the French intervention mission was withdrawn in October 2016. The next year, Russia hosted CAR President Faustine Archange Touadera in Sochi, and in December 2017, it persuaded the UN Security Council to grant it a waiver of the arms embargo to supply and professionalise the government forces.[70] This was rapidly followed by an extensive deployment of private military contractors, advisors, and entering the extraction of mineral resources, mainly diamonds.[71] The rapid surge in Russia's visibility and actual influence on the ground surprised observers and pushed France, CAR's former colonial metropolis, out of its traditionally privileged position in the country.[72]

Multiple forms of Russia's engagement in the CAR have been conducted under the locally registered Lobaye Invest company, a subsidiary of Prigozhin's M-Finans, dependent on his international Concord consortium, which is headed by Yevgeny Khodotov, who specialises in the extraction of gems. The seemingly local firm—later sanctioned by the U.S.—apart from offering cover to the mercenary and diamond businesses linked to Prigozhin, became a powerful transmission belt for Russia's multiple public relations initiatives. Seconding conducting economic, political, security, and soft power policies to a formally independent, non-state actor

[70] "UN gives green light on Russia arms to C Africa," *News24*, 16 December 2017, www.news24.com/news24/Africa/News/un-gives-green-light-on-russia-arms-to-c-africa-20171216 (accessed 5.3.2022).

[71] J. Czerep, "Russia's Political Offensive in Africa," *PISM Strategic File,* No. 1 (88), November 2018, p. 5.

[72] This was quickly achieved thanks to providing personal security for CAR's president and filling an office of his security advisor with a Russian national.

(factually very close to the Kremlin) offered Russia an opportunity to overlook the usual diplomatic constraints and act with little comprehension of the consequences. This made CAR synonymous with state weakness and hopelessness, and perfect ground for an experiment to paint a picture of a role-model picture of a Russian "success story" in Africa that would be difficult to challenge. Opening of the void in CAR for Russia to fill offered it with "proof" of what Russian opinion-shapers were already telling the African audiences: that Russia, unlike the West, has *no prejudice* towards Africa. Its eagerness to go where all the others were leaving could have been framed as seeing value where the West didn't.[73]

On 10 October 2018, Bangui's only five-star hotel, Ledger, hosted an unusual event—a beauty contest for Miss Bangui. It was sponsored by Lobaye Invest and the Russian embassy. During the show, all eyes were on the Russian VIPs: Valery Zakharov, security advisor to CAR's president, and Russian Ambassador Viktor Tokankov. Zakharov, a former GRU officer who became the civilian "face" of Russia's engagement, took to the stage to congratulate the winner—23-year-old Charlène Sombo. A month later, she also won over the previously selected Misses of Nana, Berberati, Bouar, Bossangoa, Nola, and Mbaiki in a Bangui stadium-held final of Miss Centroafrique, where Elmira Abdrazakova, Miss Russia 2013, crowned her and handed over a CFA 5 million ($8,650) donation to

[73] Such an approach followed the path of the Turkish "big entry" into Somalia. By 2011, it was arguably the most feared place on Earth, where UN aid agencies were not eager to establish a permanent presence. In the middle of the famine and when the capital Mogadishu was still fighting Al Qaeda-linked al-Shabaab jihadists, PM Erdogan arrived as the first non-African leader in two decades, bringing in—apart from officials and businessmen—his family, Turkish actors, and singers to initiate a shockingly extensive relationship (see: J. Czerep, "Turkish Soft Power Experiments and Dilemmas in Somalia," [in:] J.-N. Bach (ed.), *Routledge Handbook of the Horn of Africa*, 2022). As Turkey did with Somalia, Russia intended to build a success story around its presence in the CAR, which would symbolise its attractivity and honesty of its intentions on the continent, something Western diplomats would strongly disagree with.

a local clinic.[74] The competition represented a much-appreciated sign of a return to relaxed, community entertainment after years of divisive violence. Importantly, by bringing together young women from across the country, it presented Russia as committed to reconciliation. By bringing a female celebrity from Russia into the war-torn country, Russians presented themselves as visibly more courageous than others in fostering people-to-people relations. Other public events of this kind designed to win the sympathy of the general audience involved football tournaments, martial arts and fitness competitions, and film screenings. Lobaye sponsored an open-air "Russian Cinema" where Russian films translated into French were presented. Another set of activities targeted schools. They were approached with "friendship lessons", which included a special course of history, designed by the Russian embassy. In a much-advertised campaign, schools were given trampolines. Banners presented when sport equipment was being handed over were often written in the local Sango language, not French.[75] Scholarships to study in Russia were quickly organised and winners of the 2018 poetry and drawing competitions, hosted by the embassy, could travel for a holiday to the Russian-occupied Crimea.[76]

Events like that have been routinely covered by the newly established Radio Lengo Songo ("building solidarity" in Sango), a Russian-funded station with coverage wider than the country's state radio. Allegedly, for its launch Prighozhin flew his employees from St. Petersburg. Throughout 2018, promotional billboards for the station were ever-present across the capital, Bangui. The radio

[74] "Russian influence on show in C. African beauty contest," *France24*, 12 December 2018, www.france24.com/en/20181212-russian-influence-show-c-african-beauty-contest (accessed 1.3.2022).

[75] J. Losh, "Inside Russia's soft power battle...," *op. cit.*

[76] K. Svoboda, P. Matlach, Z. Baddorf, "Russia's Activities ...," *op. cit.*, p. 24.

station hired a local staff of journalists and presented a mix of entertainment, African music, local reporting, and Russian language tutorials, with pro-Russian narratives and disinformation.[77] Its aim was to compete with the EU-funded Radio Ndeke Luka and the UN mission's Guira FM and keep the atmosphere about Russian involvement positive. Radio Lengo Songo became a routine media patron of Russian-sponsored events. Despite instances of having promoted false pro-Kremlin stories, its reporting found ways into the media mainstream: a popular social media news aggregator, 236 News, routinely republished contents from the radio's website. Radio Lengo Songo, together with French-language versions of RT and Sputnik News, as well as the free weekly newspaper *La Feuille Volante du Président* became key formal channels of spreading Russian narratives in the country. However, the biggest effort was put on building heavy, quasi-grassroots social media support. Those activities have been coordinated by the French-educated Dmitry Sytyi and run from the information and communication office within the CAR president's administration.[78] From there, overtly pro-Russian social media accounts have been employed to control the direction in which Central Africa, Russia, and the West were being discussed in the CAR, particularly by denouncing the alleged hypocrisy of the UN, calling some local politicians "enemies", and praising cooperation and friendship between Russia and the CAR.

Apart from Russia's efforts to play above its league and artificially create an impression of being attractive and impactful, Russia's footprint in the CAR is also marked with real achievements. Contrary to the EU's long record of missed opportunities to

[77] J. Losh, "Inside Russia's soft power battle...," *op. cit.*

[78] M. Olivier, "Russia/Africa: Wagner, an investigation into Putin's mercenaries," *The Africa Report*, 28 July 2021, www.theafricareport.com/112649/russia-africa-wagner-an-investigation-into-putins-mercenaries (accessed 7.01.2023).

promote its own successes, Russia was quick to capitalise on its. The first one came with the arrangement of the Khartoum Peace Agreement, signed on 6 February 2019 in the capital of Sudan, which involved the CAR government and representatives of 14 armed groups. It followed Russian shuttle diplomacy that brought together a bigger number of factions from across the spectrum than in any previous attempts, and eventually put some key rebels in government positions.[79] No matter how fragile, the agreement offered a noticeable reduction of tensions and space for social bonds to rebuild. The agreement was followed by the arrival of a Russian humanitarian convoy crossing from Sudan,[80] recalling such aid to the separatist regions of eastern Ukraine[81] (initiated in mid-2014 and widely suspected of bringing armaments, not aid, to pro-Russian fighters).

From an earlier transport of this kind, in May 2018, a RIA FAN correspondent, Kirill Romanovsky, known for his previous work in Syria popularising Russia's involvement,[82] was invited to take occasional footage.[83] To make the Russian engagement more

[79] "Central African Republic: Don't Reward Warlords," Human Rights Watch, 24 April 2019, www.hrw.org/news/2019/04/24/central-african-republic-dont-reward-warlords (accessed 30.7.2019).

[80] *Midterm report of the Panel of Experts on the Central African Republic extended pursuant to Security Council resolution 2454 (2019), S/2019/608*, UN, p. 20.

[81] "3rd Russian humanitarian aid convoy arrives in Donetsk," *RT*, 20 September 2014, www.rt.com/news/189224-ukraine-humanitarian-convoy-donetsk (accessed 8.3.2020).

[82] "Final Report on the Murder of Orkhan Dzhemal, Aleksandr Rastogruev and Kirill Radchenko in the Central African Republic," *Dossier*, 30 July 2019, https://dossier.center/car-en (accessed 27.9.2020).

[83] I. Barabanov, S. Reiter, A. Soshnikov, A. Zakharov, S. Goryashko, "Золото Пригожина. Чем занимались россияне в ЦАР, когда погибли журналисты," *BBC*, 31 January 2019, www.bbc.com/russian/features-47005604 (accessed 7.02.2020).

popular, in July 2019, an animated video, "Lion et Ours" (Lion and Bear), credited as created for Lobaye Invest, and possibly originally meant for the "friendship classes", was posted on YouTube.[84] Its narrator, a child, tells in French the story of a Central African lion who tries to defend animals on the farm from an attack by hyenas. Overwhelmed, the lion is surrounded. Chaos and destruction prevail. Then, a bear moves in all the way from Russia to stop the fighting. Together with the lion and the rest of the animals, they sit down to put the place in order again. Obviously, the argument on the farm represented the CAR's civil war; the bear's intervention, the arrival of the Russian instructors and mercenaries; and the animals' meeting to sort out problems and re-arrange roles, the Khartoum agreement. In the video, the lion and the bear became partners and worked as equals. This was to symbolise the apparent harmony between Russians and the citizens of the CAR, and their joint work for the public good. A format of a children's story brought the civilians' perspective on the conflict to the front and stresses peace and people's wellbeing as the ultimate point of reference. The way the story was told pointed to the ability of Russian experts on public relations to speak the cultural language of the CAR, using strong and understandable symbols. Simultaneously, the video served to promote the friendly face of Lobaye, otherwise responsible for the destructive exploitation of CAR's natural resources and incidents involving notorious mercenaries.

Another important achievement came in the context of the national elections scheduled for December 2020. As ex-president Francois Bozize was excluded from standing, he organised a new rebel alliance, including factions from opposite sides of the civil conflict that began in 2012. They embarked on a march on Bangui in a bid to topple the re-elected Touadera. CAR authorities called in

[84] Улыбаемся Машем's channel, www.youtube.com/channel/UCeEpLsJYoxLow-JkutsYKnA/videos (accessed 20.12.2022).

Russian and Rwandan troops to help its army repel the rebels. The Russian assistance was successful and the CAR government retained control over the capital and restored authority in towns previously captured by the rebels. Touadera was sworn in on 30 March 2021. Just five weeks later, on 5 May, a trailer of the blockbuster-style feature movie "Tourist" was presented. The promotional video was put online two days after RFI published its investigation into rapes and killings by Wagner in the CAR, based on UN-collected data.[85] Advertised as a Russian-Centroafrican co-production (with CAR actors listed among the Russians), it premiered on 14 May during a ceremony at Bangui stadium attended by 10,000 spectators. Officials, including CAR's minister of culture, religious leaders, and several athlete-looking Russians representing "instructors" praised the cooperation between the forces of both countries. The ceremony painted a strikingly different picture to the one from the recent UN and media findings.

The Hollywood-style action film, which presented the story of the Russian "instructors" assisting the CAR army, had been shot in the CAR, with real scenery (including the otherwise unaccusable Berengo base, the Russian headquarters in this state) and was anchored in the very real political context. Contrary to stylistically similar American ("Black Hawk Down") or even Chinese ("Wolf Warrior 2") productions shot on the continent, the Russian movie was clearly made for African audiences. It showed the idealistically driven Russian soldiers as good friends and honest partners to CAR's troops. In the film they don't drink, don't swear, and don't patronise Africans—a very unlikely depiction of the frontline realities. The love story between a Russian serviceman (played by Vladimir Petrov) and a Central African female soldier

[85] F. Morice, C. Cosset, "In the Central African Republic, victims of Russian abuses break the law of silence," *RFI*, 3 May 2021, www.rfi.fr/fr/afrique/20210503-en-centrafrique-des-victimes-des-exactions-russes- brisent-la-loi-du-silence (accessed 8.8.2022).

(Flavia-Gertrude Mbayabe) is very modest, not even a kiss is shown. Central African and foreign protagonists, even if they play Russia's adversaries, respect and admire it. A character of a Frenchman organising the rebellion says: "Russia is like a cement which keeps the FACA [CAR's army] together"—a reference to the complementary nature of the Russo-Centroafrican partnership, as Russia presents it. The final scene shows Touadera's inauguration ceremony and crowds chanting "Thank you, Russia!"

Although apparently the idea for the movie on Russian "instructors" in the CAR dated back to 2018, the peculiar political context of the rebellion and call for Russia's assistance pushed for the super-fast pace of its production to immediately capitalise on the unfolding military success. The movie was also intended to whitewash the Wagner contractors' image, tarnished by reports of abuses and allegations the force could have been behind the mysterious killing of three Russian opposition-linked journalists in July 2018 who attempted to investigate the mercenaries' activities in the CAR.[86] While the name "Wagner" is not mentioned even once and the Russian personnel is solely described as "instructors", apparently real Wagner foot soldiers play extras in the movie,[87] and one of the main actors strikingly resembles the force's true commander, Dimtry Utkin. The movie itself was financed by Prigozhin and heavily advertised on his associated RIA FAN news website. The film's crew involved the same screenwriter and producer behind earlier films mythologising Russian quasi-secretive operatives in Africa ("Shugaley" and "Shugaley 2", both released in 2020 and set in Libya). They depicted the imprisoned FZNC's "sociologist", actually involved in multiple operations of

[86] "Final Report on the Murder ...," *op. cit.*

[87] "Tourist" also served as a "souvenir" for pro-Russian personnel involved in Africa. For example, Seth Wiredu, head of the Ghanaian "troll factory" branch exposed in a March 2020 CNN report, played the character of a priest in the movie.

influencing elections in African states.[88] By releasing "Tourist", Russia offered CAR and African viewers a popular story, which locally became an immediate classic. For CAR's audiences, it was dubbed into Sango and many proudly have worn its promotional t-shirts ever since. Even if massively distorting reality, Africans could identify with it and feel being part of the global pop culture.

Real successes in the CAR apparently lifted the country's profile on the Kremlin's agenda and accelerated efforts to solidify the "success story". Despite AFRIC's going dormant and Russia-friendly "election observations" in Africa being on hold, the "observers" arrived again for December 2020's CAR's elections—this time under the Germany-based but Russia-linked front institution Europäisches Zentrum für Geopolitische Analyse.[89] In less than three months following the vote, the RIA FAN agency covered news from the country more than 450 times.[90] The Russian consul became personally involved in teaching "geopolitics" at the local university.[91] Simultaneous to the "Tourist" premiere, FZNC held a public meeting in Bangui with CAR journalists, bloggers, and social activists, who had been gathered to discuss "hybrid wars" and "confrontation with international fakes" and to discuss the results of its sociological survey, according to which 88% of the CAR's citizens were grateful to Russia for its recent role.[92] A quasi-scientific seminar for the elite audience of influencers and a press

[88] L. Yapprova, "'We fight for justice'. Russian mogul bankrolls action movie about his mercenary troops in Africa amid allegations of war crimes," Meduza, 28 May 2021, https://meduza.io/en/feature/2021/05/28/we-fight-for-justice (accessed 7.11.2022).

[89] M. Bajek, P. Szczepaniak, "Travel Agency...," *op. cit.*

[90] *Ibidem*.

[91] "Central African Republic: Russia's Testing Ground," VPRO documentary, 23 July 2022, www.youtube.com/watch?v=u6ORt4Spihw (accessed 1.8.2022).

[92] Фонд защиты национальных ценностей, Facebook profile, 14 May 2021, www.facebook.com/nationalvalue/posts/3024015831189839 (accessed 8.11.2022).

conference held in an African country was a novelty—routinely, FZNC holds its Africa-oriented events in Moscow. Blurring the lines between fiction and reality continued when a monument of Russo-Centroafrican brotherhood of arms—in short, a Wagner monument—was erected in Bangui in November 2021. Although it visually follows earlier monuments of Russian PMCs seen in Luhansk and Syrian Palmyra (the motif of a protected child), its design is more advanced, and the characters' look is obviously based on the "Tourist" cast.[93] Its location next to the stadium where the movie premiered further added to the mythologisation of the Russian intervention.

Echoes of that "solidarity" intervention in CAR resonated again in the aftermath of the invasion of Ukraine when Russia reported the alleged readiness of its overseas friends—most notably from Assad's Syria—to come and join the war on its side. Among the "spontaneous" videos with such pledges came two recorded by CAR military personnel. A dozen heavily armed, masked fighters declared their willingness to go to the Ukrainian front to help bring "peace and order" to their "Russian brothers" and fight "Ukrainian nationalism". The viewer could have learned that for them, the Russia-CAR bond meant more than that with other global powers: "Even if the world says they can fight Russia, we, Russia's partners, are ready to help Russia to fight in Ukraine!", narrated the group's spokesman. And that was because "Russia helped us fight in our country and we won!"[94] Although the troops called themselves the national army, they might have been ex- Union for Peace (UPC)

[93] L. Andriukaitis, "First Russian mercenary statue in Africa identified in the Central African Republic," The Atlantic Council's Digital Forensic Research Lab, 20 December 2021, https://medium.com/dfrlab/first-russian-mercenary-statue-in-africa-identified-in-the-central-african-republic-55f9d5ac3abd (accessed 1.12.2022).

[94] "Добровольцы из ЦАР заявили о готовности участвовать в военной операции на Украине," *RIA*, 11 March 2022, https://web.archive.org/

rebels whom the Russians recently fought but who switched sides and were being prepared to constitute the core of a locally recruited "black Wagner". The group of about 200 of them had reportedly been flown into Russia for training shortly before the invasion of Ukraine and came back to Bangui days before the videos were released.[95]

Finally, in order to put up strong "proof" of the alleged attractivity of Russian culture on the continent—in CAR, mainly noticeable by the promotion of its vodka, allegedly offering its consumers "the secrets of Russian power" and "Siberian health",[96] it convinced the CAR authorities to make Russian language compulsory for university students[97] and eventually to have it added as a third official national language along with Sango and French.[98] In doing so, it built a message that Russia's culture was as strong in CAR as the French one and that getting closer to it meant investing in the country's own future.[99]

web/20220311131244/https://ria.ru/20220311/tsar-1777683572.html (accessed 1.05.2022).

95 P. Obaji, "Insiders Warn Notorious Foreign Rebels to Fight With Russia in Ukraine," *The Daily Beast*, 24 March 2022, https://www.thedailybeast.com/central-african-republic-officials-warn-notorious-union-for-peace-rebels-to-join-putins-war-in-ukraine?ref=scroll (accessed 2.05.2022).

96 O. Imhof, N. Naber, R. Buschmann, "Wie die Zentralafrikanische Republik ihren Wald an Russland verscherbelte", *Der Spiegel*, 26 July 2022, www.spiegel.de/ausland/tropenholz-fuer-soeldner-wie-die-zentralafrikanische-republik-ihren-wald-an-russland-verscherbelte-a-ebb24a05-d9fd-43bf-8740-c5c84825dc84 (accessed 30.07.2022).

97 "Russian Language Added to Central African Republic University Curriculum," *The Moscow Times*, 29 November 2021, www.themoscowtimes.com/2021/11/29/russian-language-added-to-central-african-republic-university-curriculum-a75686 (accessed 3.06.2022).

98 B. Posthumus, "Analysis: The curious case of Russia in Central African Republic," *Al Jazeera*, 20 May 2022, www.aljazeera.com/features/2022/5/20/the-curious-case-of-russias-romance-in-central-african-republic (accessed 8.09.2022).

99 The Turks succeeded in Somalia a decade earlier, but only after leaving an incomparably stronger footprint in the country.

The Mirage of a Russian Alternative

To build a poster image of its presence in Africa, Russia's efforts to resonate positively in the CAR went further and deeper than in any other place on the continent. While sticking to the main themes of its Africa-oriented narrative, Russia was able to exploit new opportunities of its CAR presence to constantly re-invent its image as an "alternative" to France, the EU, or the UN. This *modus operandi*, as well as the very contents of pro-Russian narratives, proved adaptive in other parts of Africa.

The greatest opportunity to transplant and develop the CAR experience materialised when Russia was given the chance to fill another post-French vacuum—this time in Mali. The Taliban takeover of Kabul brought a new context to plans for a drawdown of French forces in the Sahel. The Malian military junta was given justification to seek an alternative force that would assist it in the fight against the jihadists so that another Kabul could be avoided. The flow of pro-Russian narratives emanating from the CAR and the neo-Pan Africanists made the entry of the paramilitary Wagner Group into Mali—speculated by media since mid-September 2021[100]—a self-fulfilling prophecy. The CAR-like repertoire could have been used again to build on the emerging momentum. When enthusiastic crowds demonstrated in Bamako in favour of the anticipated deployment of the Russians, Yéréwolo's speaker, Adama Ben Diarra, commented from the protest site: "To the asymmetric war, we propose an asymmetric solution, which is called Wagner. If Wagner went to liberate Syria and the CAR, then we welcome Wagner to Bamako to liberate

[100] M. Durmaz, "Talk of Wagner mercenary deal shines light on Mali power politics," *Al Jazeera*, 21 September 2021, www.aljazeera.com/news/2021/9/21/talk-wagner-mercenary-deal-shines-light-mali-power-politics (accessed 12.02.2021).

Mali (...) Today, it is the end of French Africa".[101] A little more than a week later, Malian M7TV screened "Shugaley 3", the then-latest Russian feature film[102] glorifying Russia's political technologists and mercenaries in Africa, the FZNC, and its head. In its final scene, CAR-based "instructors" discuss going to Mali for future operations. Simultaneously, the FZNC itself followed suit with the promotion of a fresh opinion poll supposedly conducted in Mali indicating that 87.4% of its citizens supported the deployment of Russian paramilitaries.[103] As planes with military equipment and mercenaries begun to land in Bamako around December 2021, so did transports of gifts for Malian children,[104] following the paths of the CAR-bound trampolines and convoys. Maxim Shugaley, who shined in Bangui after the "Tourist" premiere, embarked to Bamako to stage another anti-French show during the anticipated (but eventually cancelled) visit by the French President Emmanuel Macron.[105]

[101] "Mali youth back deployment of Russian fighters as France issues warning," *Africa News*, 16 September 2019, www.africanews.com/2021/09/16/mali-youth-back-deployment-of-russian-fighters-as-france-issues-warning (accessed 23.09.2022).

[102] "Озвученный на французском языке фильм «Шугалей-3. Возвращение» показали в Мали," *PolitExpert*, 26 September 2021, https://politexpert.net/262146-ozvuchennyi-na-francuzskom-yazyke-film-shugalei-3-vozvrashchenie-pokazali-v-mali (accessed 28.09.2022).

[103] "Малийцы приветствуют обращение своего президента к российским военным компаниям," FZNC, 28 September 2021, https://fznc.ru/o-fonde/nashi-issledovaniya/malijczy-privetstvuyut-obrashhenie-svoego-prezidenta-k-rossijskim-voennym-kompaniyam (accessed 30.09.2022).

[104] S. Coulibaly, "Un avion en provenance de Russie a apporté des cadeaux sucrés aux enfants maliens", *MaliActu*, 23 December 2021, https://maliactu.net/un-avion-en-provenance-de-russie-a-apporte-des-cadeaux-sucres-aux-enfants-maliens (accessed 3.01.2022).

[105] "Максим Шугалей: Бамако больше нечего обсуждать с Парижем", *Inforeactor*, 21 December 2021, https://inforeactor.ru/22623898-maksim_shugalei_bamako_bol_she_nechego_obsuzhdat_s_parizhem (accessed 7.01.2022).

The key novelty that differed in the Malian case in comparison to the CAR was that work on building favourable sentiments among the elite and the population started a long time before the actual arrival of the Russian-affiliated forces. Although their eventual deployment was conducted discreetly and surrounded with plausible denial, politically the Russians entered in the spotlight. While in the CAR to explain the already ongoing developments on the ground they must have built the entire story afterwards, and then they entered the already well-prepared stage. Still, similarly to how it played out in the CAR, the show required radical moves to limit counter-narratives. Not long after Wagner's first deployment to Mali, major French media—France24 and RFI, both investigating controversies around the Russian presence—were kicked out of the country in a bold step that made earlier calls by Russia's sympathisers to boycott Western media look innocent. No matter how much Wagner's involvement contributed to brutalisation of the conflict, a rise in targeting of civilians, which in consequence turned embattled ethnic Fulani civilians' sympathies towards the jihadists,[106] Kémi Séba would have firmly defended its record in Mali.[107] Keeping the story within the familiar anti-imperialist, pan-Africanist frames, he would have easily overcome shortcomings in the narrative's consistency: both Russian and Malian authorities officially denied Wagner's very presence on the ground. Voices such as Séba's overweighted parallel work of the investigative journalists tracing human rights abuses and resource

[106] L. Serwat, H. Nsaibia, V. Carbone, T. Lay, Wagner Group Operations in Africa. Civilian Targeting Trends in the Central African Republic and Mali, The Armed Conflict Location & Event Data Project, 30 August 2022, https://acleddata.com/2022/08/30/wagner-group-operations-in-africa-civilian-targeting-trends-in-the-central-african-republic-and-mali (accessed 5.09.2022).

[107] Kemi Seba's appearance on Le Grand Jury show, *Renouveau TV*, 26 September 2021, www.youtube.com/watch?v=ZYcD8_rMowE (accessed 9.10.2021).

exploitation by Wagner in the CAR and Mali, such as of Nigerian Philip Obaji Jr. Therefore, a phantom of Russia's (and Wagner's) intervention as a golden recipe for solving security problems and historic injustices continued to loom across the Sahel and beyond.

In this context, throughout the first part of 2021, public rallies in several countries on the continent (and diaspora centres) saw surprising exposures of Russian flags by protestors. After Mali, the trend continued during anti-government and anti-French demonstrations in Niger, Chad, and Burkina Faso. While some real grassroots, Russia-inspired groups like Mali's Yéréwolo or Niger's M62 were responsible for adding Russian flavour to the protesters' mobilisation, it was also clear that some of the countries' authorities had begun to play the card of the alleged "Russian alternative". In the case of Ethiopia's pro-government demos in May 2021[108] it was a means to give the West a signal: *Don't go too far with condemning us [for the conduct of the Tigray war], because we can always replace you [as partners] with the Russians*. Such calculation was even more evident in October 2022 when Ethiopia's signalling of a possible (although financially non-sustainable) pivot to Russia and China was meant to discourage the U.S. and EU drive to bring the Tigray file to the UN Security Council.[109] In Burkina Faso, soldiers staging the 30 September 2022 coup surfed on top of the popular pro-Russian sentiments, the hottest political novelty in a country particularly receptive to French-language Sputnik,[110] consolidate power but also to raise stakes before talks with foreign

[108] R. Lwere Kato, "Why are protestors in Ethiopia and Mali waving Russian flags?," *Africa News*, 31 May 2021, www.africanews.com/2021/05/31/why-are-protestors-in-ethiopia-and-mali-waving-russian-flags (accessed 3.06. 2021).

[109] A. de Waal, "Will the US use its leverage now to end the killing in Ethiopia?", *Responsible Statecraft*, 24 October 2022, https://responsiblestatecraft.org/2022/10/24/will-the-us-use-its-leverage-now-to-end-the-killing-in-ethiopia (accessed 3.11.2022).

[110] A. Dassonville, "Le continent..."

envoys.[111] Images of officers surrounded with Russian flag-bearing crowds, apparently following their Malian colleagues' footsteps,[112] sent a powerful signal that a major re-alignment might be on the way. Paradoxically, on the very day of the Burkina Faso coup, the Wagner-associated VKontaktie channel reported that due to the group's focus on Ukraine, recruitment for African missions was being put on hold.[113] For the moment, it seemed as if the Burkinabe people had more faith in Russia's and Wagner's capacities than Wagner itself.

While the Malian adventure opened a brand-new chapter to the continued story of Russian experiments in winning and manipulating hearts and minds in Africa, which at the time of writing continue to develop and evolve, the CAR model firmly stood in the display window for how a cherished partnership should look like. The fallout and cost of the war in Ukraine would obviously affect the Russians' abilities to maintain the continuity of their African soft power efforts. Some strategic calculations, particularly the importance of African gold and diamond extraction, largely controlled by Wagner, for the survival of the Russian economy under sanctions[114] suggest the importance of developing a friendly reception in Africa was growing. Also, declarations by major

[111] "West Africa bloc mediator 'satisfied' after meeting Burkina Faso new military leader", *Reuters*, 5 October 2022, www.reuters.com/world/africa/burkina-fasos-new-military-government-meets-west-africa-bloc-2022-10-04 (accessed 13.10.2022).

[112] "Is Moscow involved? Supporters of Burkina Faso coup wave Russian flags", *Euractiv*, 3 October 2022, www.euractiv.com/section/global-europe/news/is-moscow-involved-supporters-of-burkina-faso-coup-wave-russian-flags (accessed 13.10.2022).

[113] Post on VKontaktie profile Вакансии в ЧВК Вагнер / Работа / Курсы / PMC, 30 September 2022, https://vk.com/wall-188474281_132715 (accessed 5.10.2022).

[114] T. Collins, "How Putin prepared for sanctions with tonnes of African gold", *The Telegraph*, 3 March 2022, https://www.telegraph.co.uk/global-health/

propagandists seem to acknowledge that. Timofey Sergeytsev, in the now-infamous article "What to do with Ukraine", which called for the radical dismantling of the Ukrainian national project—published and then deleted from RIA Novosti—stated that Russia's breakup with the West was non-reversible.[115] At the end of his text, he declared: "From now on, Russia will follow its own way (...) relying on another part of its heritage—the leadership in the global process of decolonisation. As part of this process, Russia has a high potential for partnerships and alliances with countries that the West has oppressed for centuries." It looked like a declaration of seriousness of maintaining ties to Africa, coming from the inside and aimed at the Russian elite. Also, Vladimir Solovyov, top host of the militant political TV shows, related to "people who support us in Africa" when contemplating the prospects for building a new international, "anti-fascist" coalition with Syria, Venezuela, Cuba, Iran, Nicaragua, and North Korea.[116] A similar notion of the depth of ties to Africa resonated in Russia's near neighbourhood. Tajikistan's president, Emomali Rahmon, at the Central Asia-Russia summit in Astana in October 2022 complained that his country had not been receiving a similar level of respect from Russia as the African states.[117] All of these references proved

terror-and-security/putin-prepared-sanctions-tonnes-african-gold (accessed 3.06.2022).

[115] T. Sergeytsev, "Что Россия должна сделать с Украиной," *RIA Novosti*, 3 April 2022, https://web.archive.org/web/20220403212023/https://ria.ru/20220403/ukraina-1781469605.html (accessed 3.06.2022).

[116] Extracts from the Вечер с Владимиром Соловьёвым talk show, Rossiya 1, reposted on Francis Sarr's Twitter account, 15 September 2022, https://twitter.com/francis_scarr/status/1570350377878585346?s=46&t=hNCJNqjDDgoWmiLWsQyu_A (accessed 17.09.2022).

[117] Extracts from the conference, *AKITV*, 14 October 2022, https://twitter.com/Peter__Leonard/status/1581017812264398848 (accessed 16.10.2022).

a growing internalisation of the discourse developed for and with African allies in Russia itself.

No matter how vague, misinformative, and illusionary the notion of a Russian "alternative" might have been in Africa, it has succeeded in becoming a point of reference, as leverage for shifting public sentiments, and a recurring feature in the real-life politics on the continent and beyond.

MARCIN PRZYCHODNIAK
Polish Institute of International Affairs

Chinese Disinformation: Ideology, Structures, Efficiency

Disinformation as a deliberate falsehood promulgated by design[1] has a long history in China's foreign policy. The Chinese Communist Party (CPC), even before the victory of the *Long March*, created false narratives, redesigned its public image, and reconstructed the facts on purpose in order to serve its economic and political interests. A very significant example in this regard, important from today's perspective of the Sino-U.S. rivalry, was the publication of "Red Star over China", a book about revolutionary China written in 1937 by American journalist Edgar Snow. At the time, being the only English-language account of the CPC's reality and Mao Zedong's personality and written by a foreigner, it was globally (but especially in the U.S.) perceived as an insightful

[1] Disinformation is a form of propaganda involving the dissemination of false information with the deliberate intent to deceive or mislead, www.oxfordreference.com/view/10.1093/oi/authority.20110803095721660 (accessed 6.09.2022).

source of information. But the book itself was written under careful guidance of Party authorities, which suggested a specific approach to controversial topics (ideology, party governance) and checked the content before publication.[2]

Whole segments of Chinese international relations strategy in the 1960s and '70s were based on the idea of using the image of a "successful Maoist revolution". These "success stories", ideas, and projects were distributed worldwide among members of left-wing organisations and guerrillas. Their activities were financed by the PRC in several African, South American, and Asian countries. The promotion and teaching of revolutionary ideology required a "re-creation" and manipulation of certain facts from Chinese history and its policy actions. Chinese partners were constantly disinformed about, for example, the real condition of the Chinese economy (which hardly was in excellent shape when Maoist strategies failed to be efficient in governance), or the poor results of several Chinese political campaigns. Also, the global promotion of Maoism—an ideology used by Chinese to claim leadership over the USSR in the "Marxist revolution"[3]—apart from the transfer of weapons or financial assistance, contained a solid amount of disinformation.[4]

Chinese Disinformation in the Modern Era

After the end of the Cold War, China had to adopt to the relative decline of the importance of ideology in public debate. A significant change in communication due to the technological revolution and new channels of communication (especially the internet and social media) provided China with the possibility to utilise a different approach that included both propaganda

[2] *Ibidem*, p. 9.

[3] L.M. Lüthi, *The Sino-Soviet split. Cold War in the Communist World*, Princeton University Press, New Jersey 2008. p. 114.

[4] J. Lovell, *Maoism. A global history*, Vintage, New York 2020, p. 20.

(strengthening narratives already existing in the global debate) as well as disinformation (creating and distributing new narratives).

To utilise the opportunities offered by the new technological era, it required the Chinese authorities also to modernise their thinking about international relations and Western countries (*xifang guojia)*, such as the United States and its partners. To influence and shape Western debates according to its interests, the Chinese authorities had to overcome the existing differences in the concept of information, state propaganda, soft power, and communication between people and the authorities.[5] In the Chinese context, information is perceived as a political tool for the authorities to manage public opinion in order to enhance the image of the party leadership and prevent society from destabilisation. Such an understanding makes the existence of censorship and penalisation of serious actions violating the system necessary. It also requires the creation of institutions and mechanisms responsible for disseminating the official narratives, both internally and externally. These entities include state- (and party-) owned media, as well as institutions such as the Cyberspace Administration of China (CAC) and security apparatus controlling internet providers and content published in the Chinese internet. Media (and all other producers of information) must "uphold the party's leadership over the news and public opinion work".[6] During the Party's News and Opinion Work Conference in February 2016, Xi Jinping explicitly stated that, "[t]he Party's news and public opinion work is an important task

[5] Yu Shujing, Jing Xuemin, "Zi meiti shidai de Zhongguo zhengzhi chuanbo ji qi zhili, (China's political communication and governance in the era of social media)," *Aisixiang*, 2 November 2020, www.aisixiang.com/data/123380.html (accessed 7.09.2022).

[6] Wei Hong, "Dang guan meiti jie bu shuli (Party manages the media and never loses sight of it)," *Aisixiang*, 13 June 2016, www.aisixiang.com/data/100180.html (accessed 4.09.2022).

in the work of the Party, and a major matter in the management of state affairs and in the peace and stability of the country. " [7]

A different understanding of "informing the public" and "mass communication" changes the Chinese attitude to disinformation. From China's perspective, the fabrication of "news" in order to fulfil political goals is not contradictory to the concept of "providing the public with reliable information". On the contrary, it should be considered as a supplement to the existing mechanisms of presenting the news to internal and external audiences. The issue of credibility of publicly disseminated information is judged on the basis of whether it is profitable for the interests of CPC and China itself. Hence, trustworthiness and eventual legal punishment of distributing manipulated information and images are judged from the perspective of the Party's interests. Being in line with Party ideology and policy motives is crucial in assessing the credibility of information. It is also the most important condition for information that is to be published online. Chinese experts explicitly mention an important responsibility of journalists (and broader, producers of information). These people should not be focused on "controlling the government", as they are not the "fourth estate", but to be "socially responsible for the society and the people".[8] Such a condition stands against the concept of "Western media", which in the Chinese view "often deliberately abandon the

[7] China Youth Online, "Xi Jinping xinwen sixiang de qu ge xin (Seven news of Xi Jinping`s thoughts on media)," 10 July 2018, www.dangjian.cn/djw2016sy/djw2016sytt/201807/t20180710_4751414.shtml (accessed 1.09.2021); see also: China Media Project, "Mapping Xi Jinping News Thought," 19 October 2018, https://chinamediaproject.org/2018/10/19/introducing-xi-jinping-news-thought (accessed 1.09.2022).

[8] Fan Jingyi, "Xin wen gong zuo zhe de she hui ze ren (Social responsibility of journalists)," 21 April 2016, www.aisixiang.com/data/98899.html (accessed 20.08.2022).

principle of objective reporting".[9] From the Chinese perspective, an efficient fight with disinformation requires manoeuvring over freedom of expression. Some of the experts underline the positive aspects behind the tight state control of the internet in China and present the "Great Firewall" as a better solution to the problem of disinformation ("information which stands against the official Chinese line") than Western liberal concepts.[10]

The idea of "telling China's stories well" has been present in the CPC's ideology and agenda since Xi Jinping was elected secretary-general in 2012.[11] But it was mostly during his second term in office when the emphasis was put not only on underlining the positive aspects of China's policies but also on creating new narratives. Since then, the aspect of "information competition" in the ideological, political, and economic rivalry with the U.S. (and its partners) became crucial in China's policymaking.

The Goals of China's Disinformation

What is crucial for understanding China's disinformation attempts in their "information competition" with the West is that its internal significance prevails over the external one. No matter how amateur, full of propaganda, sometimes even ridiculous the content of the communication of Chinese entities sounds from the perspective of the "West", it is because these are mostly

[9] Zheng Baowei, *Xifang* "'xin wen zi you' shi shei de zi you? (Western freedom of the press is who's freedom?)," 7 April 2016, www.aisixiang.com/data/98541.html (accessed 22.07.2021).

[10] Zou Yilu, "Gei xin wen: shi shen me? Wei shen me? Zen me ban? (Fake news: what is it? Why is it? What to do with it?)," 28 April 2021, www.aisixiang.com/data/126264.html (accessed 22.07.2021).

[11] J. Szczudlik, "Tell China`s Stories Well: Implications for the Western Narrative," *PISM Policy Paper*, no 9(169), 17 September 2018, www.pism.pl/publikacje/Tell_Chinas_Stories_Well_Implications_for_the_Western_Narrative (accessed 7.09.2021).

a repetition of instruments used in internal political campaigns, which the Party has practiced since 1949. The CPC's Department of Propaganda, Politburo, and even Standing Committee members have years of experience in political and educational campaigns with (entirely or partially) false accusations, fabricated information and evidence, as well as deliberately falsified GDP statistics in several provinces.[12] These were and still are instruments of intra-party governance, personnel changes, and ongoing party struggles between different factions and high-ranking Party members. The CPC is trying to use these experiences in the global arena in foreign policy, but its main motives are still mostly internal.

Disinformation is also considered an important factor in the evaluation of CPC members from the perspective of their efficiency and loyalty. The creativity of the actions, complexity, and even level of toxicity of the prepared messages may be considered a cause for promotion. These supposedly happened, i.e., in the cases of a former Chinese diplomat (deputy ambassador) in Pakistan[13] (currently spokesperson of the MFA) and the former ambassador to Poland[14] (promoted to the position of MFA special

[12] Chen Yawen, Ryan Woo, "Another Chinese city admits 'fake' economic data," *Reuters*, 17 January 2018, www.reuters.com/article/us-china-economy-data-idUSKBN1F60I1 (accessed 24.07.2022).

[13] While being a diplomat in Pakistan, he got engaged in a heated debate on Twitter with then U.S. National Security Advisor Susan Rice, among other disputes. He described Washington as a city where places restricted for Caucasians (he explicitly used the words "white people") exist and later replayed Susan Rice's answer as her being "a disgrace" and "shockingly ignorant". Although he later deleted the tweets, he always stood by them. In 2019, he became a deputy director of the MFA's Department of Information and then the MFA's spokesman.

[14] During his tenure, he often engaged in a heated debate on Twitter and published articles in the Polish press with propaganda and China's official narrative on, e.g., the situation in Hong Kong. These were a direct response to messages and interviews posted by the U.S. ambassador to Poland accusing China of offensive policies.

representative in Hong Kong). For diplomats and officials to create, follow, repeat, and use in diplomatic work these kinds of narratives and disinformation seems to be part of signalling subordination to the CPC and an element of showing off their dedication to the ideological core and to "Xi Jinping's thought". It serves in the "top-down" management scheme in the CPC and is an efficient tool in the process of assessing and evaluating the performance of party officials.

China also wants to be a part of the global debate in order to influence it with (false) statements and narratives on controversial but important political topics. The external goal of China's disinformation is perceived in the official line as part of the narrative struggle between China and "liberal democracies", the U.S. especially. Together with informational campaigns, the disinformation techniques are used to strengthen the main lines of China's propaganda focusing mainly on two issues: 1) downgrading and falsifying the Western critique of China's poor standard of protection of human rights, economic coercion against other countries, and unfair trade practices in relations with several states and organisations; 2) strengthening China's success story with the promotion of reasonable political and economic solutions on different issues seen as superior to the liberal policies of Western states. Disinformation is also supposed to strengthen China's image of its abilities in global governance in the context of the assertion of a "failure of American democracy". It is also oriented to raise the attractiveness of cooperation with China for other partners.

From the Chinese perspective, the ongoing critique of the West concerning China's policies not only requires *dementi* but something stronger, the promotion of a different narrative. The reality of today's global debate (especially in social media) requires the creation of a strong emotional, but positive connection between recipients of the message and China. It implies radical, efficiently

prepared images and stories on the internal situation in China and its foreign policies. There are certain expressions used in the debate (introduced into political discussions and transformed in the academic world) where certain accusations and labels are put against the West and its representatives, such as the phrase "Cold War mentality".[15]

Cases

Among all the main topics in China's disinformation attempts, there is, however, one common idea, exploited by both propaganda and disinformation campaigns, and repeated in other forums. It is the general assertion of a "falling United States incapable of leadership", an idea crucial from the perspective of China's main foreign policy activity, namely its long-term rivalry with the U.S. China's disinformation is supposed to generally highlight and amplify any mistakes of the United States government, not only in foreign relations but also in other ways, such as those that make living in the U.S. almost impossible or show incompetence of the U.S. administration. Specific messages include several controversial cases such as, "U.S. and gun laws", "U.S. claims on Xinjiang and human rights", "U.S. and discrimination", "U.S. and India coronavirus", "U.S. and violence", etc.[16] One important part of the disinformation attempts was the situation in Afghanistan during and after the U.S. withdrawal, with several Chinese media and commentators using false information about a lack of U.S. assistance and evacuation of Afghani people. All of it was part of

[15] Zhao Qisheng, "Yu lun dou zheng pin de jiu shi jiang gu shi (The struggle of public opinion to tell stories)," *Aisixiang*, 10 April 2020, www.aisixiang.com/data/125951.html (accessed 2.09.2022).

[16] R. Burley, "Analysis of the Pro-Chinese Propaganda Network Targeting International Narratives," Centre for Information Resilience, 5 August 2021, www.info-res.org/post/revealed-coordinated-attempt-to-push-pro-china-anti-western-narratives-on-social-media (accessed 7.09.2022).

one general message: the U.S. is in decline and lacks the ability to be still considered a global hegemon and reliable partner. The U.S. factor is sometimes also a part of China's internal debate, where certain tragic events (flooding, building collapses, etc.) echo in media with accusations towards the American authorities involving conspiracy theories. The producers of this disinformation are hard to identify, however, some of these messages are transmitted by Chinese with millions of followers on social media, which is tolerated by officials and not censored. One example of this kind of disinformation was the group of accusations distributed via Chinese social media accounts (Weibo) that the Henan floods in 2021 were caused by an American secret weapon.[17]

Besides the general repeated messages about the U.S. since 2019, there were five main topics in China's disinformation attempts—the situation in Hong Kong, policy involving the Uyghurs in Xinjiang, relations with Taiwan, justification of the Russian invasion of Ukraine and the COVID-19 pandemic, with a special emphasis on the origins of the virus. The first topic focused on an interpretation of international law obligations coming from the Sino-British Joint Declaration on Hong Kong in the context of the application of the National Security Law in Hong Kong in 2019. The second involved creating mythical living conditions in the Xinjiang region. The third questioned the status of Taiwan, its rights, and capabilities in the international arena. The fourth topic amplified the false Russian statements about security concerns stemming from NATO enlargement in Central and Eastern Europe, the supposed lack of Ukrainian sovereignty, and purported U.S. involvement in the Maidan. The fifth topic included the distribution of messages about the EU's

[17] Tweet by Zhaoyin Feng, BBC correspondent in Washington, https://twitter.com/ZhaoyinFeng/status/1418582524205359104 (accessed 7.09.2022).

and U.S. supposed incompetence in dealing with the coronavirus in comparison to China's abilities and accomplishments.

Mechanisms and Institutions

China uses its disinformation abilities in both an offensive and passive way, with both an internal and external angle. The offensive mechanism is designed to undermine the credibility of any Western institution, organisation, state, high-level politician, journalist, or researcher that is seen as endangering China's interests. The entities attacked are responsible, the in Chinese view, for disseminating information on topics China considers crucial. Examples of propaganda campaigns include ones against Adrian Zenz,[18] the Australian Policy Institute,[19] Reuters, and the BBC. Falsified information was created and transmitted to undermine the credibility of the findings and reports of these individuals or organisations. At the same time, hate campaigns strengthened by postings and the messaging of Chinese officials and on social media were conducted, for example, against journalists from the BBC operating and living in China.

The passive style of Chinese disinformation operations is not designed to unleash an attack on a specific person or entity accusing China of wrongdoing or distributing an image against China's interests but to globally promote a different, mostly false narrative. Such a narrative is often carefully adjusted to create a feeling of probability and influence the opinion of people all around the world. It gives China the fuel to defend its policy in

[18] A scholar who published extensive reporting on China's Xinjiang policies, including the evidence on the system of concentration camps where mostly Uyghurs are kept for re-education and forced labour.

[19] An Australian think-tank that extensively published reports on the situation in Xinjiang, developments in the system of camps, as well as Chinese disinformation policies.

different arenas (such as the UN's Human Rights Council) and strengthen its image in the global arena. One example was the video campaign posted by thousands of users on the global internet in response to the accusations of genocide committed by Chinese authorities in Xinjiang. According to the analysis made by the *New York Times*,[20] these videos, although oriented to look like independent profiles, were orchestrated and carefully prepared by the Chinese government. Another was the creation of a fake scientist, "Wilson Edwards", who commented on the origins of COVID-19 and the WHO's independence.[21]

Although the motivations are different, the instruments used in both mechanisms are similar. Due to the nature of modern communication and lack of official confirmation, the whole process is fluid and difficult to generalise. It is also not precisely regulated and orchestrated, but rather depends on the creativity and decision-making of different institutions themselves. The decision-making patterns used are also subject to the existing Party hierarchy. There are, however, certain patterns that can be described. The disinformation campaign starts with policy directives issued at the highest levels of the Party authorities. The main, political message, consistent with the CPC's ideology, may even be discussed within the Standing Committee, but is distributed through speeches, statements by Xi Jinping himself, or in communiques after certain meetings of the Politburo or CPC's

[20] P. Mozur, "How China spreads its propaganda version of life in Xinjiang," *New York Times*, 22 June 2021, www.nytimes.com/interactive/2021/06/22/technology/xinjiang-uyghurs-china-propaganda.html (accessed 2.09. 2021).

[21] S. Tawari, "China: Swiss embassy urges media to remove scientist fake news," BBC News, 11 August 2021, www.bbc.com/news/world-asia-china-58168588 (accessed 7.09.2021); see: C. Carter, "Translation: Imaginary friends and the fruitless search for Wilson Edwards," *China Digital Times*, 12 August 2021, https://chinadigitaltimes.net/2021/08/translation-imaginary-friends-and-the-fruitless-search-for-wilson-edwards (accessed 7.09.2022).

Central Committee. The practices, techniques, and messaging is supposed to be (according to the division of power within the party) decided on the level of the Central Committee's Department of Propaganda[22] and the CPC's United Front Work Department[23], through which it is distributed to certain institutions for implementing. These include the People's Liberation Army as well as governmental bodies (State Council and its sub-institutions, such as the Taiwan and Hong Kong and Macau Affairs Offices), internet and media regulators (Cyberspace Administration of China, State Administration of Press and Publication, State Administration of Film and State Administration of Radio and Television), or media entities (Xinhua, China Radio International).

The security apparatus and Ministry of Foreign Affairs are also highly involved in the process. The MFA remains the main entity directly responsible for transferring Party messages to the foreign audience, through regularly organised "press-conferences"[24] (usually on working days) for Chinese and foreign journalists. Chinese experts on foreign policy issues with a reputation of being experts on "the West" are the main substantive "transmitters" of disinformation and narratives through social media accounts on the Chinese web, Twitter, or Facebook, and their participation in global debates (through conferences, webinars, publications). The credibility and attractiveness of the message (enhanced by official confirmations during the MFA's press conferences) is to be

[22] One of the departments in the CPC's Central Committee responsible for ideology work, as well as the dissemination of pro-China narratives internally but also externally.

[23] One of the departments in the CPC's Central Committee responsible for the supervision of China's activities abroad, especially gathering information, maintaining contacts, and influencing individual elites and organisations, as well as organising and controlling the Chinese diaspora.

[24] These press conferences are prepared (with a list of suitable questions that journalists are allowed to ask), delivered every day by one of the MFA's spokespersons for Chinese and foreign journalists.

strengthened by their reputation. Trusted and loyal local voices from several countries (academics, students, journalists) are also engaged in the process. For example, Chinese media (like CRI) offered payment for persons willing to record and disseminate messages corresponding with the Chinese official line, using exact phrases and statements (through videos, articles, posts). Other institutions responsible for disseminating the message through cultural and scientific channels include the Confucius Institutes and universities (also through their cooperation with foreign partners). This creates an "echo" in the debate which is then transferred and amplified by a larger amount of less-substantive sources ("50 cent army"[25] and troll farms), mostly fake accounts created on social media. Twitter is considered the most popular social media instrument for disseminating Chinese disinformation, with hundreds of accounts created.[26] The levels of engagement and the structure of messaging may be different depending on the topics, from the apparently reasonable "objective" analysis of Chinese state think-tanks (always in line with the Party interests and directives) through university researchers and media outlets (Xinhua, CRI) to media-celebrities and officials like Hu Xijin.[27] These patterns can be observed in most of the disinformation campaigns introduced in both the internal and external environments.

[25] K. Twigg, K. Allen, "The disinformation tactics used by China," BBC, 12March 2021, www.bbc.com/news/56364952 (accessed 7.09.2022).

[26] D. Lee, "Hong Kong protests: Twitter and Facebook remove Chinese accounts," BBC News, 20 August 2019, www.bbc.com/news/technology-49402222 (accessed 7.09.2022).

[27] Editor-in-chief of *Global Times* (*Huanqiu Shibao*), a radical, Party-controlled newspaper (part of the *Renmin Ribao* group), published in two language versions—English and Chinese. It is often used as a trial balloon for inseminating the debate with controversial issues in order to test the reaction of global audience.

Sino-Russian Cooperation

These mechanisms are mostly China-made, with no direct cooperation with other states, especially with Russia, which has convergent political and ideological interests in relation to the EU and the U.S. Until now there are no direct confirmations of China-Russia practical cooperation on disinformation activities, but there are certain techniques in China's disinformation (use of local voices, social media campaigns, creation of fake accounts[28]) that may suggest China is "learning" *best practices* from the Russians. Although there is no evidence of direct cooperation between China and Russia, the similarity of content in both states' disinformation campaigns reinforces their messaging about the weakness of Western institutions.[29] However, Russia's activities are usually a bottom-up approach (Russian media using local topics and local voices in the debate) and China's are always the top-down approach (the message starts from the highest levels of the Party and is transferred downwards through local media). Analysts with Map Influence identified occasional examples of direct, technical cooperation between media entities from China and Russia such as shared offices by Russia Today and China Daily in Bulgaria.[30] Cooperation with the Russian Federation is also useful for the Chinese, especially when it involves a debate

[28] J. Brandt, T. Taussig, "The Kremlin`s disinformation playbook goes to Beijing," Brookings, 19 May 2020, www.brookings.edu/blog/order-from-chaos/2020/05/19/the-kremlins-disinformation-playbook-goes-to-beijing (accessed 7.09.2022).

[29] A. Legucka, M. Przychodniak, "Disinformation from China and Russia during the COVID-19 Pandemic," *PISM Bulletin*, no 86(1516), 21 April 2020, www.pism.pl/publications/Disinformation_from_China_and_Russia__during_the_COVID19_Pandemic (accessed 30.09.2022).

[30] Based on research by Ivana Karaskova from MapInfluence. See: "Ivana Karaskova outlines Beijing`s disinformation operations," 12 September 2020, https://mapinfluence.eu/en/ivana-karaskova-outlines-beijings-disinformation-operations (accessed 5.09.2021).

in the UN. When this occurs, the coalition of friendly countries is involved in issuing letters of confidence, for example, within the UN institutions and supporting China's claims on specific topics using the disinformation messages and narratives. Sometimes, Russia and China compete with each other on disinformation capabilities, for example, when Chinese entities administer more financial resources and attract employees of Russian media companies with better wages and conditions. Such technical differences will increase in time with the growing imbalance of economic potential between China and Russia but the political and ideological complementarity will remain, which was explicitly pictured in the Chinese presentation of the Russian invasion of Ukraine.

The mechanisms of the dissemination of disinformation could be observed clearly in the campaign that started as a response to then U.S. Secretary of State Mike Pompeo's accusations of China committing "genocide in Xinjiang" and the difficult conditions for Uyghurs in that region. The mechanism of the video campaign was described by the *New York Times* reporters.[31] After Pompeo's statement, the CPC decided to start the campaign using different channels of dissemination. Several party cells in Xinjiang collected messages of denunciation and "evidence" that Pompeo was wrong. The videos or posts were staged as selfies to look like authentic postings by Uyghurs. Some were reposted by Party institutions (Communist Youth League) or Party-owned media (Xinjiang Daily). On social media, too, they were spread far and wide, giving credit to CCP-run sites. Afterwards, the videos began to appear on YouTube and Twitter. An *NYT* analysis found here close coordination—the videos would appear on YouTube, and 20 minutes later go out via a bot network on Twitter.

[31] J. Kao, R. Zhong, P. Mozur, A. Aufrichtig, N. Morgan, A. Krolik, "'We are very free'. How China spreads its propaganda version of life in Xinjiang," 22 June 2021, https://www.nytimes.com/interactive/2021/06/22/technology/xinjiang-uyghurs-china-propaganda.html (accessed 6.09.2021).

Efficiency

As there are two main goals from the perspective of the Chinese on the use of disinformation, the issue of efficiency also requires a double-sided approach—one internal and the other external. There are no trustworthy sources that can identify the levels of satisfaction of the authorities with the disinformation campaigns among the Chinese in general. But we can still estimate the level of positive evaluations of China in Western countries, mainly the U.S.,[32] but also in the EU and Central Europe. These internal disinformation campaigns are not supposed to raise China's popularity or its *soft power*. These are mainly to boost the position of the CPC, its propaganda and efficiency, as it is an ordinary tool in China's totalitarian political model, marked by the lack of a free press or democratic institutions. And, despite the lack of credible polls, that goal can be identified as fulfilled. Without disinformation and strong narrative campaigns, the Xi Jinping's current power, based on centralisation, control over society (and Party officials), and fear of penalisation, would not be so overwhelming. The main topics—Hong Kong, Xinjiang, Taiwan, invasion of Ukraine and China-Russia relations and COVID-19—were also the main political issues from the perspective of the authorities. Imposing successful messaging and creating a narrative of efficiency reduced the negative impacts on Xi's power within the Party coming from the difficulties caused by, for example, the pandemic, and helped him stabilise the political ground before the Party conference in 2022. In that context, the internal aspect of the Chinese disinformation campaigns also should be evaluated as an important part of the complicated process of managing Party officials on different

[32] J. Kurzlantzcik, "How China ramped up disinformation efforts during the pandemic," Council on Foreign Relations, 10 September 2020, www.cfr.org/in-brief/how-china-ramped-disinformation-efforts-during-pandemic (accessed 7.09.2022).

levels, with different ambitions, and from different, competing provinces.

The external efficiency of the disinformation campaigns is a different story. Here, the ability to construct and disseminate different (than "Western") narratives generally failed to convince and address the most "valuable" groups of recipients. These are mostly Europeans, citizens of EU Member States, as the EU has become an important actor from the Chinese perspective in the rivalry with the U.S. Disinformation on Hong Kong, Taiwan, Xinjiang, COVID-19, and Russia especially, not only did not convince the European public that China has reasonable policies, cooperates fruitfully, and offers positive solutions. Rather, they tended to reduce the trust in and positive opinions of China, the Chinese in general, and the possibilities of cooperation. Two independent polls conducted in 2021 on the perception of China within Europe paint a similar picture of a sceptical attitude among most European (and global) societies researched. Both polls, conducted by Pew[33] and Sinophone[34], showed a generally decreasing level of trust in most of the EU Member State populations towards China. In Pew's research, the European country with the most unfavourable attitude towards China ("have negative opinions of China") was Germany (71%), while the least unfavourable was in Belgium (67%). According to Sinophone, Swedish respondents reported the most negative feelings, with 60% holding very negative or negative feelings of China. The only predominantly

[33] L. Silver, K. Devlin, C. Huang, "Large majorities say China does not respect the personal freedoms of its people," Pew Research Center, 30 June 2021, https://www.pewresearch.org/global/2021/06/30/large-majorities-say-china-does-not-respect-the-personal-freedoms-of-its-people (accessed 6.09.2022).

[34] R. Q. Turcsanyi, M. Simalcik, K. Kironska, R. Sedlakova, "European public opinion on China in the age of COVID-19. Differences and common ground across the continent," Sinofon, November 2020, https://sinofon.cz/surveys (accessed 6.09.2022).

positive view of China at the time was Latvia where about 43% had positive views of China. Another PEW opinion poll from 2022 confirmed these tendencies, with large majorities of European countries holding negative views about China. [35]

As long as the internal aspect of disinformation prevails in the hierarchy of the Chinese authorities, the question of the efficiency of its external aspect will not be so difficult to contain and strengthening cooperation with Russia will be less probable. But there already are signs that China is willing to use more sophisticated instruments and mechanisms in its disinformation attempts and narratives, such as artificial intelligence, in order to better shape and design attractive messages for the Western audience.[36] If successful, those efforts would require much stronger preparation by the EU and the U.S. to counter them compared to the current level of defence against Russian disinformation and the already inadequate engagement against the Chinese.

[35] L. Silver, C. Huang, L. Clancy, "Negative views of China tied to critical views of its policies on human rights", *Pew Research Center*, 29 June 2022, www.pewresearch.org/global/2022/06/29/negative-views-of-china-tied-to-critical-views-of-its-policies-on-human-rights (accessed 21.10.2022).

[36] Kyodo, "China's military aims to use AI to dominate cyber and outer space, Japanese think tank warns," *South China Morning Post,* 13 November 2020, www.scmp.com/news/china/military/article/3109803/chinas-military-aims-use-ai-dominate-cyber-and-outer-space (accessed 10.12.2022).

TOMASZ CHŁOŃ
Ambassador (ret.)

Countering Disinformation

The key to success in counteracting contemporary forms of disinformation at the national level and in relations between states is social and individual resilience[1] based on broad education, effective legal regulations, and coordination of activities within national structures and supranational institutions and organisations.

"Social Polygraph"

The authors of the *Prague Manual* prepared by European Values, a Czech think-tank with great merit in the field of counteracting disinformation, rightly emphasise that the most important role

[1] Resilience (individual and collective), understood as the ability to recognise and solve problems, the ability to assess situations and reactions, and the ability to act in response to the situation, in this case to false, manipulated or incorrectly prepared and disseminated information, in a systemic and long-term manner.

in this task is necessarily the civil society, especially research, teaching, and media communities. They not only help to recognise disinformation and understand this problem, provide expertise, advice, and a training base for public service employees in this regard, but above all educate users and actors in the information space, especially young generations who derive knowledge mainly from its new digital sources.[2] In most countries aware of the dangers of disinformation, various expert initiatives carrying out this type of activity are becoming more and more active.

In the international dimension, the American and British centres are the most influential in terms of their research potential, resonance, scope, and scale of impact. In many cases, they use the knowledge of experts from other countries. As part of, for example, the American Atlantic Council, there are dedicated teams dealing with disinformation, the analytical work of which is used not only by the U.S. government but also other countries or international organisations. The Center for European Policy Analysis, RAND Corporation, and the Brookings Institution prepare regular analysis and recommendations for governments. The German Marshall Fund of the United States inaugurated the Alliance for Securing Democracy project, which contributes to raising awareness of the dangers of disinformation: it publicises the results of scientific research, and its website Hamilton 2.0 Dashboard regularly presents narratives and disinformation activities from Russia, China, and Iran.

A lot of work is carried out at universities individually or as part of international research clusters. Other valuable civic projects are also coming out of academic centres. In Ukraine, StopFake

[2] Naturally, it is impossible to list all research and scientific centres dealing with disinformation on these pages. The achievements of many of them are illustrated by the bibliography of this study, and earlier by an interactive list of sources used in, among others, their work by the North Atlantic Treaty Organisation.

is one of the most effective networks for tracking and revealing disinformation. It is active in many countries and in many languages, including Polish, and was established on the initiative of university staff and journalism students.[3]

Media education is an essential aspect of reducing the effects of disinformation. Media education not only imparts knowledge on how to consume content from traditional and social media in an informed and responsible manner but it also breaks down communication barriers and allows for interaction between diverse communities that hold different views. In other words, it provides a method through which discussion and the exchange of opinions on the internet can occur in a civilised manner.

Media education can be particularly effective if it becomes a component of a holistic approach to curbing disinformation. Through a public-private partnership, the state must develop strategies, legal frameworks, and institutions that have tasks of their own, but which also (and perhaps most importantly) support the building of social resilience to disinformation.

As in the case of the scientific community, this study can only highlight some examples of civic and media projects that are worth getting to know more closely, if not imitate: in Finland, one of the first journalistic organisations verifying the truthfulness of information, Faktabaari,[4] and in the UK, a phenomenal team of investigative journalists, Bellingcat.[5] In France, in 2017, many months before the presidential election, a consortium of national and local media tracking

[3] www.stopfake.org/pl/o-nas-pl (accessed 14.12.2020).

[4] E. Mackintosh, "Finland is winning the war on fake news. What it's learned may be crucial to Western democracy," CNN, www.edition.cnn.com/interactive/2019/05/europe/finland-fake-news-intl (accessed 5.12.2022).

[5] "Digital investigation collective Bellingcat to expand into NL," *DutchNews.nl*, www.dutchnews.nl/news/2018/11/digital-investigation-collective-bellingcat-to-expand-into-nl/?utm_source=newsletter (accessed 4.12.2022).

down and disclosing examples of electoral disinformation was established. This consortium may have saved Emmanuel Macron's presidency.[6]

A massive social movement of so-called elves[7] tracking internet trolls and a creative Dutchman, Ruurd Oosterwoud, inspired not only his own countrymen but also the Germans, the British Ministry of Foreign Affairs, and even NATO with the idea of the DROG programme—training for officials, journalists, as well as education for young people through games and simulations.[8]

It is also worth noting the important role that parliaments play at the interface between citizens and governments in combating disinformation. In 2016, the European Parliament launched a process that led to the adoption of the EU's Action Plan against Disinformation. On the one hand, national parliaments listen to social demands, and on the other, they serve to strengthen civic awareness of threats (the Library of Congress in the U.S. is, for example, a goldmine of knowledge about the problem

6 F. Bell, "Here's a list of initiatives that hope to fix trust in journalism and tackle 'fake news'," www.medium.com/@ferg/heres-a-list-of-initiatives-that-hope-to-fix-trust-in-journalism-and-tackle-fake-news-30689feb402 (accessed 10.12.2022).

7 K. Sengupta, "Meet the Elves, Lithuania's digital citizen army confronting Russian trolls," *The Independent*, www.independent.co.uk/news/world/europe/lithuania-elves-russia-election-tampering-online-cyber-crime-hackers-kremlin-a9008931.html (accessed 20.12.2022).

8 The British Foreign Office decided to finance the translation or creation of national versions in 12 other languages. DROG conducted training for 200 Dutch military who received, among others, the task of carrying out a simulated attack on NATO, see: "Dutchman's shock treatment against fake news Ruurd Oosterwoud wants to make Europeans aware of disinformation—by teaching them how to do it," *Politico*, www.politico.eu/article/ruurd-oosterwoud-bad-news-drog-meet-the-dutchman-who-wants-to-make-us-immune-to-fake-news (accessed 4.12.2022).

of disinformation[9]) and put pressure on governments to adopt administrative countermeasures, not only defensive but also offensive such as sanctions.

Governments—Selected Cases

For the purposes of this chapter, several examples of systemic actions of states and their governments in the field of counteracting disinformation have been selected, which, in the author's opinion, are worth getting to know in depth, as well as being imitated within local possibilities and conditions.

Australia

Australia can be considered a model country in its robust efforts to combat disinformation. It has created one of the best-rated systems for counteracting disinformation, which, apart from internal political aspects, is undoubtedly more influenced by the threat of disinformation operations by China than by Russia. According to the GDI "Disrupting Disinformation 2021" study, Australia is the only country in the world that has developed policies that cover the five crucial areas of resistance to disinformation: organisation of elections; transparency of election campaigns; the functioning of government institutions and task forces; sanctions for media entities that violate the applicable regulations; and combating hatred.[10]

[9] "Government Responses to Disinformation on Social Media Platforms: Sweden," Library of Congress (USA), www.loc.gov/law/help/social-media-disinformation/sweden.php (accessed 6.12.2022).

[10] R. Kupiecki, F. Bryjka, T. Chłoń, *Dezinformacja międzynarodowa. Pojęcie, rozpoznanie, przeciwdziałanie*, Wydawnictwo Naukowe Scholar, Warszawa 2022, p. 267.

Finland

"The kindergarten tutor is on the first line of defence against disinformation, and children love to be detectives," media education experts say.[11] With this approach, it should come as no surprise that the Finnish model for counteracting disinformation is recognised as one of the best in the world and the Finns are ranked number one by the Open Society Institute Sofia in terms of resistance to fake news.[12] But what is needed to support it is a well-thought-out and organised education system. At every level, a whole education system teaches creativity and a critical approach to the surrounding world. It should be emphasised that it is based on strong systemic foundations: methodological and didactic (teacher education system) and economic (expenditure on education).

At the same time, experts emphasise that developing the abovementioned skills in students cannot be an end in itself as they are intended to help them develop a broader ability to identify and assimilate higher values related to living in a democratic society. An important systemic rule is also the fact that government experts only develop general goals and programme recommendations, leaving the freedom of implementation to schools, and schools leave it to individual educators.

Media education, and within its framework the problem of disinformation, although it is not a separate subject at the primary and secondary levels, is treated in a cross-sectional way in Finnish school curricula, that is, according to the complexity of the world around us. In mathematics lessons, students learn about

[11] J. Henley, "How Finland starts its fight against fake news in primary schools," *The Guardian*, www.theguardian.com/world/2020/jan/28/fact-from-fiction-finlands-new-lessons-in-combating-fake-news (accessed 4.12.2022).

[12] "The Media Literacy Index 2019: Just think about it," Open Society Institute Sofia, www.osis.bg/?p=3356&lang=en (accessed 6.12.2022).

the manipulation of statistics, in art education, how images are falsified, and in history, how the past is distorted.

As part of a comprehensive approach to media education in schools, the government supports start-up projects to develop teaching materials that take into account the issue of disinformation, and the journalistic collective Faktabaari cooperates with schools under the *Faktana, kiitos!* (Facts, please!) initiative, aimed at developing practical skills in identifying and understanding disinformation.

France

Following the 2017 presidential elections, risks and threats were reviewed and analysed by the General Secretariat for National Defence and Security at the Prime Minister's Office and within the National Cybersecurity Agency, and the results were presented to national stakeholders. Actions were also taken in the fields of public communication and diplomacy, including at the level of the presidents of France and Russia, where warnings were made against disinformation. A military doctrine of information operations was also adopted that defines operations (combat) of influence using the network (fr. *lutte informatique d'influence*) as "military activities in the information domain of cyberspace in order to detect, assess, and counterattack, support strategic commands, obtain information or misrepresentation, as a standalone operation or as part of a wider activity"[13].

In media law, a penalty of up to €445,000 was introduced for publishing and disseminating false information in an effort to violate public peace. A penalty of up to €135,000 was introduced if the false information concerns military discipline and morale

[13] D. Kolesnyk D., *France Unveils Information Operations Doctrine*, Military Technology, https://kolesnyk.fr/images/miltech62021_franceL2I_kolesnyk.pdf (accessed 28.03.2022).

or interferes with war efforts of the nation. A new law, which was adopted in November 2018, also aims to fight electoral disinformation. It imposes an obligation of transparency in the dissemination of sponsored information, as well as the possibility for the Radio and Television Council to suspend content broadcasted by media entities that are supervised by foreign countries or related to them. At the same time, the law provides for judicial review of such decisions. Established in 2021 as part of the Prime Minister's office, the Viginum unit for combating external interference has a budget of around €12 million.[14]

Germany

In connection with the parliamentary elections of 2021, demonstrative measures were taken, including warnings levied by the spokesman for the Ministry of Foreign Affairs, who publicly identified and attributed disinformation actions associated with the Russian authorities. The Central Election Commission conducted a special information campaign devoted to the transparency of the election process, and separate websites were created to provide fact-based information around the elections. In addition to these awareness-raising campaigns, working groups focused on hybrid threats were also established in various state institutions. Knowledge and expertise were shared within interministerial teams, including a specific task force at the Ministry of the Interior that included participating representatives of the Ministry of National Defence and the Ministry of Foreign Affairs.

The National Cybersecurity Centre developed a new cybersecurity strategy that was adopted by the government, and the Federal Office for Information Security prepared and conducted trainings for politicians, decision-makers, and officials.

[14] R. Kupiecki, F. Bryjka, T. Chłoń, *Dezinformacja międzynarodowa.... op. cit.,* pp. 256–257.

Furthermore, it strengthened its cooperation with platforms such as Facebook and Google and established a team for detecting bots and coordinated inauthentic behaviour on the internet.

In addition to these targeted actions by the government, political parties implemented their own anti-disinformation programmes. The Christian Democrats created a fact-checking page, and the Green Party established a "fire brigade" in the Netfeuerwerk network. Fact-checking initiatives were also created and implemented by mass media. DPA (Deutsche Presse-Agentur), for instance, created "Fakt21", which focused on training, education, and cooperation in journalistic circles. Anti-disinformation programmes were also launched in the research community, with local and international think tanks participating.[15]

Lithuania

While in Finland, counteracting disinformation is primarily a function of the education system, in the case of Lithuania, one can speak of a kind of militarisation of the media space, treated by the authorities almost as a separate domain of military activities. In the Lithuanian armed forces, initiatives have been initiated since 2005 to provide quick, timely information on the situation in the information space, supporting the military and civil decision-making process in the field of counteracting disinformation. Military and civilian experts in the field of psychology, social sciences, cybersecurity and intelligence monitor media and analyse and react by reporting incidents that may affect state security. The Lithuanian Ministry of National Defence conducts its own projects to educate citizens, media representatives, and institutions in the field of disinformation activities, thus contributing to strengthening society's resilience to foreign propaganda. As in Finland, cooperation between government

[15] *Ibidem*, pp. 258, 259.

institutions and the public enables Lithuanians to effectively mitigate the impact of disinformation and to sort of "clean up" the information environment, thus protecting national political and civic decision-making processes.

A separate Lithuanian phenomenon is a kind of "mass mobilisation" consisting of mass public involvement in the state's information security. In 2017, a team of professionals and volunteers from various fields—the social sciences, media, and business specialists, and even people of the arts—united to form the Debunk EU project and began to jointly counter the growing problem of disinformation in Lithuania. As part of it, an analytical tool for monitoring internet media was created using artificial intelligence techniques. It has the ability to detect false information in the media space just minutes after it appears.

Another example of social mobilisation in Lithuania is the mass movement of "elves"—state sponsored anonymous activists tracking down internet trolls. This ever-growing community, as is the case with Debunk EU, brings together journalists, IT specialists, businesspeople, students, and scientists.

Sweden

Sweden can impress with its comprehensive approach to the problem of disinformation from both the government and civil society. The general rehearsal of the created system, for which the Swedes meticulously prepared, was the parliamentary elections in 2018,[16] which drew on the experiences of other countries. U.S. experts, among others, were invited to Stockholm, a nationwide media fact-checking platform covering major mainstream media

[16] E. Colliver, T. Mauer, "How Sweden is preparing for Russia to hack its election," *BBC*, www.bbc.com/news/world-44070469 (accessed 5.12.2022).

was created, and foreign-funded advertising was banned.[17] At the same time, the National Media Council prepared teaching materials for students and high school students.

In 2019, based on the experience gained, the Swedish Civil Contingency Agency (MSB) issued a special guide[18] for public officials and officials dealing with social communication, and the MSB itself began transforming into the Psychological Defence Agency by 2022, with an appropriately allocated budget and tasks adapted to new needs.

The United Kingdom

Due to its importance in the Euro-Atlantic community despite Brexit, and the role of its governmental and non-governmental entities, media, and expert centres in the international information space, the United Kingdom remains (also for Poland) one of the most important actors and allies in the fight against disinformation. It is British experts who co-shape the assumptions of NATO's communication strategy and participate in its implementation.

They transposed the OASIS (Objective, Audience insight, Strategy, Implementation, Scoring / evaluation)[19] model of information campaigns to NATO. It is a specific tool of strategic communication and communication campaigns in which all five

[17] A comprehensive report on disinformation in Sweden in connection with the 2018 parliamentary elections was prepared by the London School of Economics, see: Ch. Colliver, P. Pomerantsev, A. Applebaum, J. Birdwell, "Smearing Sweden International Influence Campaigns in the 2018 Swedish Election," London School of Economics, Institute of Global Affairs, www.lse.ac.uk/iga/assets/documents/arena/2018/Sweden-Report-October-2018.pdf (accessed 3.12.2022).

[18] "Countering information influence activities A handbook for communicators," *msb.se*, www.msb.se/RibData/Filer/pdf/28698.pdf (accessed 4.12.2022).

[19] *Guide to campaign planning: OASIS*, www.gcs.civilservice.gov.uk/guidance/marketing/delivering-government-campaigns/guide-to-campaign-planning-oasis (accessed 15.12.2022).

elements are equally important. It has been to a greater or lesser extent duplicated in the information policy of other countries, but the last component of the system, i.e., the audit of the effects of own actions, deserves particularly in-depth analysis and reflection also in Poland.

Like the Swedes, the British have prepared a public toolkit for counteracting disinformation for their officials.[20] For obvious reasons, British solutions are subject to analysis and imitation around the world. Anne Wilding, commissioned by the British Council, developed guidelines for conducting lessons with elements, games, simulations, quizzes (available in media, e.g., Buzzfeed), class debates, and competitions.[21]

The United States

Russia has declared a real information war against the United States as the leader of the world's democratic community. Its course and effects as well as American countermeasures are reflected in official documents, such as the Robert Muller report on Russia's interference in the U.S. presidential election in 2016 and in numerous reports by research centres, of which the studies of Harvard, University of Texas in Austin, MIT, and the RAND Corporation and Atlantic Council provide particularly valuable and updated information. These reports are important sources of conclusions and recommendations for experts, decision makers,

[20] RESIST Counter-disinformation Toolkit (netdna-ssl.com), www.3x7ip91ron4ju9ehf2unqrm1-wpengine.netdna-ssl.com/wp-content/uploads/2020/03/RESIST-Counter-Disinformation-Toolkit.pdf (accessed 10.12.2022).

[21] A. Wilding, "How to use fake news critically in the classroom," *Voices Magazine*, British Council, www.britishcouncil.org/voices-magazine/use-fake-news-classroom-critically (accessed 4.12.2022).

and practitioners in both the United States and other democratic countries.[22]

Despite the controversy surrounding Trump's presidency, the United States has responded to Russia by levying sanctions against the perpetrators of disinformation attacks and influence operations. Before the 2018 midterm elections, they carried out preventive cybernetic operations against the Russian 'troll factory' in St Petersburg. As a result, in 2017, the federal legislation was adopted to counteract foreign propaganda. There, the Departments of State and Defence were obliged to develop a strategy, including assistance to third countries. In the State Department, the Centre for Global Engagement was established, which cooperates with U.S. security services and works on information technology issues, international cooperation, and preparation of content to counter disinformation.

In 2021, senator Amy Klobuchar presented a bill in the U.S. Senate on the culpability of companies that allow misleading information about vaccines and other health issues to be spread over the internet. It also proposes the introduction of an exception to the Internet Law, which thus far has protected companies such as Facebook, Google, and Twitter from legal accusations relating to content published on their platforms. The level of sensitivity around this topic is demonstrated by the proposal to limit liability to "current threats to public health", i.e., epidemics or other exceptional events with a similar potential to have catastrophic implications.[23]

The State of California asked RAND to diagnose the disinformation problem during the 2020 elections and make

[22] R. Kupiecki, F. Bryjka, T. Chłoń, *Dezinformacja międzynarodowa...*, *op. cit.*, pp. 260, 261.

[23] S. Ghaffary, R. Heilweil, "A new bill would hold Facebook responsible for Covid-19 vaccine misinformation," *Vox*, www.vox.com/recode/2021/7/22/22588829/amy-klobuchar-health-misinformation-act-section-230-covid-19-facebook-twitter-youtube-social-media (accessed 28.8.2021).

appropriate recommendations for future interventions. RAND's findings indicated that content prepared by Russian-associated perpetrators of disinformation was considered by voters that lean Republican as a product of the Democratic Party and vice versa. Most of the disinformation materials identified focused on public and social affairs that divide American voters. "Russia knows who does not like whom and what is the cause of divisions, and fills the information space with messages that prevent agreements", noted the report, which recommended that the authorities issue public service announcements to alert the public about the perpetrators and content of such campaigns during elections.[24]

International Organisations

NATO

Thanks to British experts, among others, NATO can be considered a textbook example of the effectiveness of an international organisation in countering disinformation. Alliance communication is evidence-based, timely, transparent, and coordinated. This allows NATO to exert significant influence in the international and national information spaces. The essence of the organisation's activities in this respect—consisting of specific strategic preventive communication—are two basic elements: understanding and engagement. A full understanding of the information environment, and disinformation in particular, is crucial to enabling a credible response. NATO, also using leading external services and monitoring, examines and analyses the information environment in a non-stop mode, and on this basis

[24] M. Posard, H. Reininger, T. Helmus, *Countering Foreign Interference in the U.S. Election*, RAND Corporation 2021, www.rand.org/content/dam/rand/pubs/research_reports/RRA700/RRA704-4/RAND_RRA704-4.pdf (accessed 3.2.2022).

formulates its strategies and messages, coordinated with allies, based on facts and credibility.

Staying ahead of disinformation is more effective than reacting. This philosophy guides the approach of counteracting the achievement of opponents' goals through campaigns dedicated to supporting NATO's role and mission in the societies of member and partner countries. An important element of the allied public diplomacy in this context was also active (though usually difficult) work with Russian media, opinion leaders, academics, and students, also conducted in Russian, and using the NATO Information Office in Moscow and its social networks before it was closed down in December 2022 after Russia withdrew its accreditation.

The organisation supports member and partner countries by advising and co-financing social and scientific projects that strengthen their resilience to disinformation. Rapid reaction teams under the anti-hybrid strategy were put at the disposal of the Member States. The organisation strengthened its cooperation with the European Union so that the EU's disinformation alert system would also serve the Alliance.

From the research, analytical, and operational side, these activities are supported by the Centre of Excellence for Strategic Communication located in Riga (www.stratcomcoe.org), affiliated with NATO but not formally its organ. The Centre's expertise and reports on counteracting disinformation, as well as the relevant work of the NATO Defense College in Rome (www.ndc.nato.int), a school that is directly part of the Alliance, guarantee the highest level of understanding and response.

Since Russia's illegal annexation of Crimea and start of its aggression against Ukraine in 2014 and 2022, NATO has stepped up efforts to counter disinformation. [25] The organisation followed the advice of Alliance Heads of State and Government contained

[25] "NATO-Russia, Setting the Record Straight," NATO, www.nato.int/cps/en/natohq/115204.htm (accessed 20.12.2022).

in the 2018 Brussels Summit Declaration, which noted the challenges of disinformation campaigns and cyberattacks. In the 2019 London Summit Declaration, Alliance Heads of State and Government stated that NATO is strengthening its deterrence and defence capabilities against hybrid threats.

Also in 2019, NATO adopted an updated and structured package of relevant anti-disinformation assumptions, measures, and actions. To this end, it works most closely with the European Union, but also with the UN, the G7, and partner countries. In the past years, NATO has shown that it is able to maintain its missions and operations and remains prepared despite the COVID-19 pandemic, ensuring that the global health crisis does not turn into a global security crisis as well.

The following table lists the research centres and media selected by the author, monitored during their NATO duties during the pandemic.

Atlantic Council Digital Forensic Research Lab, www.atlanticcouncil.org/programs/digital-forensic-research-lab
Balkan Insight, www.balkaninsight.com
Brookings, www.brookings.edu
Carnegie Europe, www.carnegieeurope.eu
Chatham House, www.chathamhouse.org
Center for European Policy Analysis (CEPA), www.cepa.org
Center for Security and Emerging Technology (specialised), www.global.georgetown.edu/georgetown_units/center-for-security-and-emerging-technology
Center for Strategic International Studies, www.csis.org
Clingendael, Netherlands Institute of International Relations, www.clingendael.org
Council on Foreign Relations, www.cfr.orgEU DisinfoLab, www.disinfo.eu
European Values Think Tank (Prague), www.europeanvalues.net
Foreign Policy, www.foreignpolicy.com
Foreign Policy Research Institute, www.fpri.org
German Council on Foreign Relations, www.dgap.org/en

German Marshall Fund (GMF), www.gmfus.org
Global Disinformation Index, www.disinformationindex.org
Globsec, www.globsec.org
Graphika, www.graphika.com
Harvard Kennedy School of Misinformation Review, www.misinforeview.hks.harvard.edu
Institute for Strategic Dialogue, www.isdglobal.org
International Strategic Action Network for Security (ISANS), www.isans.org/en
Center for Eastern Studies, www.osw.waw.pl/pl
Oxford Internet Institute, www.oii.ox.ac.uk
Pew Research Center, www.pewresearch.org
Polish Institute of International Affairs (PISM), www.pism.pl
The Jamestown Foundation, www.jamestown.org
RAND Corporation, www.rand.org
Reuters Institute, www.reutersinstitute.politics.ox.ac.uk
Royal United Services Institute (RUSI), www.rusi.org
Stanford Internet Observatory, www.cyber.fsi.stanford.edu/io/io
Visegrad Insight, www.visegradinsight.eu
Woodrow Wilson Center, www.wilsoncenter.org
Global Engagement Center (USA) and Disinfo Cloud, www.state.gov/disinfo-cloud-launch
Google, www.google.com
NATO Defence College, www.ndc.nato.int
NATO's Strategic Communications Centre of Excellence, www.stratcomcoe.org
Polish government website, www.premier.gov.pl/en.html
Twitter, www.twitter.com
United Nations Department of Global Communications, www.un.org/en/sections/departments/department-global-communicationsBBC Reality Check, www.bbc.com/news/reality_check
Bellingcat, www.bellingcat.com
Buzzfeed News, www.buzzfeednews.com
Atlantic Council Digital Forensic Research Lab, www.atlanticcouncil.org/programs/digital-forensic-research-lab
Balkan Insight, www.balkaninsight.com

Brookings, www.brookings.edu
Carnegie Europe, www.carnegieeurope.eu
Chatham House, www.chathamhouse.org
Center for European Policy Analysis (CEPA), www.cepa.org
Center for Security and Emerging Technology (specialised), www.global.georgetown.edu/georgetown_units/center-for-security-and-emerging-technology
Center for Strategic International Studies, www.csis.org
Clingendael, Netherlands Institute of International Relations, www.clingendael.org
Council on Foreign Relations, www.cfr.org
EU DisinfoLab, www.disinfo.eu
European Values Think Tank (Prague), www.europeanvalues.net

Source: Own compilation

NATO's toolbox, created in 2019 to combat hostile outreach, reflects a two-pronged response model: (1) "understand" and "act", and (2) "coordinate". Its purpose is to provide the Allies with the tools to assess hostile information activities, including disinformation, and to help identify possible directions of action. In addition, experts from the NATO International Secretariat organise regular (bi-weekly) briefings on Russian and other disinformation activities in various Alliance committees, including the Civil Emergency Planning Committee.

Following Russia's full-scale invasion of Ukraine in February 2022, the Allies emphasised that resilience against non-military, subliminal, or hybrid threats, being first and foremost a national responsibility, is also a collective obligation, according to Article 3 of the North Atlantic Treaty. First noted in the 2010 Lisbon Strategic Concept, the new Madrid edition emphasises that resilience-building is a key element in the Alliance's core mission of collective defence, which requires incorporating new efforts to counter hybrid threats in a more comprehensive way than before. This need for more comprehensive action stems from the growing sophistication

of the threats, both from Russia and other state and non-state actors, which present a greater challenge than they did a decade earlier.

The overall package therefore covers a broad spectrum of actions to counter hybrid threats in the areas of cyber and disinformation operations. It also includes measures aimed at strengthening energy security, ensuring energy supply for the armed forces, and providing more robust chemical, biological, radiological, and nuclear defence.

Taking into account the increasing aggression of Russia in the last decade and a half, its war against Ukraine, energy blackmail, espionage and cyberattacks, interference in democratic processes, and the security risks resulting from the COVID-19 pandemic, the Allies announced measures aimed at:

- strengthening critical infrastructure, supply chains, and health systems; increasing investment in stable and reliable delivery of essential public services; and ensuring continuity of government.
- investing in capabilities to deter and defend against political, economic, energy, information, and other hybrid tactics from state and non-state actors.[26]

European Union

Among international organisations and institutions, the European Union has developed the most comprehensive mechanism for counteracting disinformation supporting the Member States. In response to Russia's aggression against Ukraine and the increase in hybrid and disinformation threats, in 2015, the

[26] "NATO 2022 Strategic Concept," NATO, 29 June 2022, www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf (accessed 10.7.2022); "Madrid Summit Declaration," NATO, 29 June 2022, www.nato.int/cps/en/natohq/official_texts_196951.htm?selectedLocale=en (accessed 10.7.2022).

EastStratCom[27] team was established under the European External Action Service, which currently has a base of 15,000 examples of disinformation that it regularly analyses, describes, and discloses. In 2018, the European Commission presented the Action Plan Against Disinformation, which includes the Rapid Alert System, in which Member States communicate and coordinate responses to disinformation incidents.

An important source for educators in counteracting disinformation is a report on the practice of media education in primary and secondary schools in European Union countries, commissioned by the European Commission.[28]

The EU has also agreed on a Code of Conduct for Combating Disinformation, which has been voluntarily adopted by technology companies, regulating for the first time more comprehensively the rules for conducting political campaigns on the internet and on social networks and transparency in this regard.[29]

Lessons from its implementation were considered in the EU's Digital Services Act (DSA), adopted on 19 October 2022, which imposes new obligations on large online actors such as Facebook, YouTube, and Twitter. In a departure from the voluntary commitments outlined in the EU Code of Conduct on Countering Disinformation, the DSA includes an obligation to cooperate with independent researchers and allow them to access and participate in complaint and appeal

[27] "Questions and Answers about the East StratCom Task Force", www.eeas.europa.eu/headquarters/headquarters-homepage/2116/-questions-and-answers-about-the-east-stratcom-task-force_en (accessed 20.12.2022).

[28] J. McDougall, M. Zezulkova, B. van Driel, D. Sternadel, "Teaching media literacy in Europe: evidence of effective school practices in primary and secondary education," NESET II report. Luxembourg: Publications Office of the European Union, 2018, www.eprints.bournemouth.ac.uk/31574/1/AR2_Teaching%20Media%20Literacy_NESET.pdf (accessed 10.12.2022).

[29] "The 2022 Code of Practice on Disinformation," https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation (accessed 02.03.2023).

procedures regarding content moderation, dispute resolution, and to access the relevant database of the digital platforms.

At the social level, the document provides for consultations with other stakeholders like civil society organisations and the introduction of watchdog institutions to notify about a suspected crime. The DSA also provides for the establishment of a European Digital Services Council and an advisory body of national coordinators responsible for implementing legislation at the national level. It defines the responsibility of service providers and their obligations, as well as the rules for dealing with complaints, including out-of-court dispute resolution mechanisms. It also imposes additional obligations on very large digital platforms (whose services are accessed by 45 million users or more per month), including assessments of systemic risk resulting from their services, indications of measures to reduce these risks, independent audits, conditions of algorithmic recommendations, and transparency measures for advertisements.[30]

Other organisations

Although the importance of other international organisations and institutions in counteracting disinformation is much more limited compared to NATO and the European Union, it should be noted that in the UN system (UNESCO, UNODC) and the Council of Europe actions encouraging the governments of the Member States to intensify efforts to counter disinformation, especially as related to COVID-19, were undertaken. Important work is performed by the United Nations Office of Global Communications. International organisations come up with joint initiatives and statements on disinformation threats, but they also see threats to media freedom resulting from counteracting disinformation.

[30] "The Digital Services Act package," European Commission, https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package (accessed 25.10.2022).

The Council of Europe promotes resilience to disinformation through education. Its education division supports initiatives that teach a critical approach to media. UNESCO has developed a training guide for journalists.[31] Since 2018, the OECD has included the results of media education in PISA surveys.

In 2018, at the initiative of Canada, the G7 agreed on the so-called Rapid Response Mechanism to exchange information and coordinate responses to threats.

Technology Companies

For several years, under social and government pressure, operators of social networking sites such as Facebook, Twitter, and Google, have been introducing solutions based primarily on self-regulation in the field of counteracting disinformation and hate speech online. They include the massive removal from social networks of accounts that violate these rules and greater transparency in the conduct of political campaigns and advertising.[32]

Business and governmental experts, as well as those from the European Union, collaborate in developing new solutions. However, these measures are still insufficient. Some governments, such as the French, are pushing through fines against companies for being slow to counter disinformation, but such attempts are successfully prosecuted in courts based on the principles of freedom of speech.

The assessment of the first year of operation of the EU Code of Conduct on Combating Disinformation was not uncritical and indicates the lack of evaluation criteria for its implementation, clear commitments, structured cooperation or the involvement

[31] "Journalism, 'Fake News' and Disinformation: A Handbook for Journalism Education and Training," *En.unesco.org*, www.en.unesco.org/fightfakenews (accessed 11.12.2022).

[32] "Social Media Manipulation Report 2020," NATO Stratcom Centre of Excellence, www.stratcomcoe.org/social-media-manipulation-report-2020 (accessed 21.12.2022).

of the advertising industry in its implementation. These shortcomings have influenced the provisions of the DSA, which will undoubtedly affect the functioning of these digital giants but will not solve every problem.

Poland

Compared to other countries, Poland is mixed when it comes to counteracting disinformation. European Values ranked Poland in 2018, if not among the leaders, then among the countries with a high awareness of the threats, but above all among state bodies and institutions.[33]

It seems that the situation looks better when it comes to research on disinformation. Among Polish centres with an international reputation, regular research is conducted and published by experts from the Polish Institute of International Affairs[34] and the Centre for Eastern Studies.[35] Periodical reports are issued by Visegrad Insight[36] and the College of Eastern Europe in Wrocław.[37]

---

[33] V. Vichova, J. Janda, "The Prague Manual. How to counter the Kremlin's influence in Europe," Federal Academy for Security Policy Working Paper, Issue 22/2018, www.baks.bund.de/sites/baks010/files/working_paper_2018_22.pdf (accessed 4.12.2020).

[34] See, e.g.: A. Legucka, "Countering Russian Disinformation in the European Union," *Bulletin PISM*, no 111(1357), 6 August 2019, www.pism.pl/publications/Countering_Russian_Disinformation_in_the_European_Union (accessed 6.12.2022).

[35] See, e.g.: J. Darczewska, "Between overt disinformation and covert practice: The Russian special services' game," *Point of View*, no 73, www.osw.waw.pl/en/publikacje/point-view/2019-03-28/between-overt-disinformation-and-covert-practice (accessed 7.12.2022).

[36] D. Bartha, "Countering Disinformation at Home. Tools to combat state-controlled amplifiers," *Visegrad Insight*, https://visegradinsight.eu/disinformation-home-hungary (accessed 13.12. 2022).

[37] P. Pogorzelski, *Zagrożenie rosyjską dezinformacją w Polsce i formy przeciwdziałania*, Raport Kolegium Europy Wschodniej www.kew.org.pl/2017/10

Individual studies are carried out at many universities, crowned with interesting events, reports, and projects. In the field of school education, the Modern Poland Foundation (Fundacja Nowoczesna Polska) performs valuable work through the Media Education Service (Serwis Edukacja Medialna) for teachers in which more than 230 lesson plans in the field of broadly understood media education for all levels of primary and secondary schools are available, although with a very limited scope relating directly to disinformation.

In the third sector, the Info Ops Polska Foundation seems to be the most dynamic (also active on Twitter).[38] The initiatives of the Panoptykon Foundation, which in cooperation with the Reporters Foundation, prepared the publication "Stop disinformation. A guide for journalists and editors". The Demagog Association, on the other hand, became the first member of the International Fact-Checking Network.

Many media naturally deal with disinformation problems on an ongoing basis, but some of them also conduct projects dedicated directly to it. For example, *Gazeta Prawna*, CyberDefence24.pl, or the Polish edition of EuroActiv.

It is also worth following the work of OKO Press journalists devoted to revealing the activities of Russian trolls in Poland. An example is the report by Anna Mierzyńska, who analysed the network in the period between the first and second round of the local government elections in Warsaw in 2018, discovering thousands of entries written in incorrect Polish.[39]

In the state and government administration, including the Ministry of Foreign Affairs and the Ministry of National Defense, cells dedicated to counteracting disinformation were created. The

/23/piotr-pogorzelski-zagrozenie-rosyjska-dezinformacja-polsce-formy-przeciwdzialania; Podcasty: *Wojna informacyjna,* Nowa Europa Wschodnia, www.new.org.pl/858,podcasty_wojna_informacyjna.html (accessed 10.12.2022).

[38] www.infoops.pl.

[39] www.oko.press/o-nas (accessed 9.12.2022).

Ministry of Foreign Affairs is the operator of the EU RAS (Rapid Alert System) and conducts training in this area, also for the management of the central government. As part of wider competences, the issues of disinformation are dealt with by the National Security Bureau, the Department of National Security at the Chancellery of the Prime Minister, the intelligence and counterintelligence services, the Government Centre for Security, as well as the National Radio and Television Council, which monitors political advertisements. In 2022, a government plenipotentiary for the security of the information space was appointed.

Cross-sectional activity devoted to research, training, and consulting in the field of internet use is carried out by the Scientific and Academic Computer Network (NASK)–the National Research Institute. As part of its mission to promote and implement the concept of the information society, it also deals with education, mainly of children and adolescents, aimed at safe use of the internet and new technologies. NASK is also responsible for running the Bezpiecznewybory.pl platform (www.nask.pl).

Response to Russia's Invasion of Ukraine

Meanwhile, Russia's full-scale invasion of Ukraine in February 2022 created, for many reasons, a completely new reality in the fight against Russian manipulation and propaganda. The invasion defied the Kremlin's earlier propaganda about its intentions towards Ukraine, as international society witnessed the brutal destruction of Kyiv and its suburbs, Kharkiv, and, above all, Mariupol—the "Ukrainian" Aleppo. The ruthless actions taken by Russia against civilians (including women and children), the deaths of thousands, and the exodus of millions of Ukrainians brutally exposed the cynicism and reality of Vladimir Putin's plans, as well as the hypocritical state machine behind him. This propagandistic Waterloo (at the time of writing, the outcome of

the war is still unclear) may suggest that strategically, the pre-war hybrid actions, including disinformation, were not effective against the West. However, this thesis does not seem justified.

The rules of the period of peace have given way to the laws of war; the democratic world has stood for the victim and stigmatised the aggressor. At the same time, the question can be raised whether decisive action by the West against Russia's propaganda and disinformation apparatus, if taken earlier (as many civil society circles have postulated), could have clipped the wings of the Russian propaganda and avoided the current war with Ukraine. This would have been an expression not only of the West's resolve and unity but also an opportunity to build its societies' real resilience to falsehood, manipulation, and political corruption on the part of Russia. In the information war, before its hot phase, it was not the Russians who were particularly effective, but the West that was unprepared.

Whether the war could have been avoided in its entirety remains uncertain. Undoubtedly, though, in defending the victim of such brutal aggression, and in the face of an attack on the foundations of the international order, the Western world has stood united as never before. However, despite this promising show of unity, it is difficult to declare victory over disinformation, let alone a victory of democracy over authoritarianism. In the face of this war, the long-term repercussions for Russia and Russian society remain unclear. Will there be a bloody farewell to imperial ambitions, as was the case with the French war in Algeria (*toutes proportions gardées*)?

On a global scale, China will no doubt learn important lessons from this war. While the war has exacerbated existing problems, it also has revealed the potential for unity and effective decision-making in the face of a common threat. What once seemed complicated procedures that required onerous bargaining within the European Union became easily implementable joint actions in the face of war. The "anti-war" information campaign broke

the monopoly of states, traditional media, and specialised non-governmental organisations in combating disinformation in a spectacular way. With ordinary internet users and circles, such as Anonymous, expressing a willingness to play a major role in fighting disinformation in a way that previously was unimaginable, it also exposed the crucial role that effective leadership plays through the example of Ukrainian President Volodymyr Zelensky. At the same time, it showed the absolute domination of social media platforms in today's information environment, including their strength and their double sidedness (i.e., channels used by the Russian authorities on the Telegram platform).

The sanctions imposed in the aftermath of the war were met with expected countermeasures by the Russian regime, including restricted access to Western traditional and social media and the closure of the last independent editorial offices in Russia (*Echo Moskvy* and TV Dożdż). The resulting challenge has been less a matter of defending against Russian disinformation in the West and more one of reaching the indoctrinated Russian society.

The (dis)informational "Russian Wall" created by Putin is not airtight, however. Millions of Russians have installed VPNs (6.4 million in the first three weeks after the invasion, based on data from Apple and Google applications, compared to 230,000 in the previous three weeks). These VPNs bypass censorship using Tor technology, which allows the creation of portals and networks (including Twitter) in a "grey area". Russians have received tens of millions of informational messages about the war via simple text messages, e-mails, and online advertisements. Efforts by traditional Western media outlets have led to Russian- and/or Ukrainian-language information about the war being published in the largest newspapers of the Nordic countries (e.g., *Helsingin Sanomat*), Poland (e.g.,*Gazeta Wyborcza*) and Germany (e.g., *Bild*). Most Russians are overwhelmingly influenced by the regime's propaganda, but the most important battlefield "for

souls" remains within large cities like Moscow and among the younger generations. It is because of these audiences that Putin closed the last independent media, *Echo Moskvy* and TV Dozhd. Meanwhile, the extraordinary NATO summit on 24 March 2022 led to the decision that the Alliance will continue to oppose Russia's lies about its war in Ukraine and that it will expose fabricated narratives, operations, and provocations.[40] The decision was also made to increase the resilience of societies and the infrastructure of member states against Russian influence, including new measures to strengthen cyberdefence capabilities and respond to disinformation. NATO also called on China to stop reproducing the Kremlin's false narratives, particularly in relation to the war and NATO. In turn, the EU adopted the Strategic Compass (2022) that set its path forward in the areas of international security, foreign influence, and manipulation of information.[41] Time will show how durable the determination of the Alliance, the European Union, and the West will prove to be in the face of disinformation in international politics. It already appears, however, that such a fight need not be quixotic. On the contrary, the free world is well placed to win it, particularly, it seems, under the condition of war.

Conclusions

Seven years have passed since the first attempts to systematise national and international activities aimed at disinformation, the scale and scope of which have been particularly worsened since the start of Russia's aggression against Ukraine. The world seems

[40] "Statement by NATO Heads of State and Government," www.nato.int/cps/en/natohq/official_texts_193719.htm?selectedLocale=en (accessed 27.03.2022).

[41] "A Strategic Compass for a Stronger EU Security and Defence in the Next Decade," European Council, March 2022, www.consilium.europa.eu/en/press/press-releases/2022/03/21/a-strategic-compass-for-a-stronger-eu-security-and-defence-in-the-next-decade (accessed 23.8.2022).

to have realised at that time the significance of disinformation threats and the challenges of harnessing disinformation into wider hybrid activities.

From the experience of this period, it can be concluded that counteracting disinformation by states and the international community, including organisations such as NATO and the European Union, has become more and more effective over time. Nevertheless, disinformation threats are constantly evolving, and China has appeared in a new role among the actors in the field of disinformation as a result of the COVID-19 pandemic, with which the West is gathering new experiences in this confrontation.

However, obstacles resulting from the political and economic interests of individual members of the Euro-Atlantic community in their relations with both China and Russia will remain a problem in counteracting disinformation in the long term. There are also fundamental legal issues, democratic freedoms and values that naturally limit the room for manoeuvre by Western governments and institutions such as the European Union in introducing new restrictive legal regulations in the field of social media. However, there are some trends in all this that may evoke relative optimism. It seems that the frustration of a number of important actors on the international scene, especially Germany, is growing due to the aggressive actions of Russia and, increasingly, China. The Biden administration in the United States has returned to multilateralism, which has once again become the rule regulating international affairs. Finally, the limitations of the current self-regulatory approach to disinformation and hate speech on the internet, and especially on social networks, which are increasingly becoming the dominant source of knowledge about the world around people, have become clearly visible.

Therefore, three requirements for which it seems realistic to garner support from most Euro-Atlantic community states require fundamental improvement: education, identification, disclosure

and more effective punishment of perpetrators of disinformation, and regulation of the social media sector.

Media education will remain primarily the domain of states and societies, and it is they who are responsible for increasing its range and effectiveness, especially in terms of counteracting disinformation.

Identifying and disclosing the perpetrators, attributing disinformation and, more broadly, hybrid activities to specific actors also belongs, first and foremost, to national prerogatives. But there are opportunities within the European Union and NATO to coordinate these activities, agree standards or even protocols in this regard, and take action in a more collective manner.

More offensive measures using cyber capabilities should also be considered to not only expose but also to penalise the creators and perpetrators of disinformation, including through the wider application of individual and collective sanctions to them.

The regulation of the internet environment, due to its supranational, global nature, seems to require not only more significant and decisive interference by international institutions, including, in particular, the European Union, but also robust implementation of the new regulations by the Member States. Care for the internet ecosystem must, as many experts on the subject emphasise, be comprehensive, including regulation of the internet market so that—as in the case of energy—disinformation does not poison the environment. Therefore, the work on reforming the EU Code of Conduct on Combating Disinformation and subsequently transforming its provisions from a self-regulatory instrument into legally binding actions outlined in the Digital Services Act is an important step in the right direction.

At NATO, the recent developments in Russia's aggression towards Ukraine and confrontational policy towards the West warrant a further shift in attitudes in tackling disinformation. Even if Putin steps down or is removed, Russia's behaviour will not necessarily

change for the better, and the West will have to reckon with more challenging disinformation warfare by Russia and Belarus. Moreover, China will soon present a formidable challenge with its own set of methods and tools of disinformation. Therefore, where appropriate, the Allies should overcome any remaining reluctance and uncooperative tendencies that limit the role of NATO in combating new threats, especially hybrid ones. First, tackling disinformation should gain greater political attention among all Allies. National countermeasures undertaken in some member states (e.g., France, Germany, the Baltic States and the UK) or partner countries (e.g., Finland and Sweden, soon to be members) testify to the importance they attach to the problem of falsehoods in international politics. When allowed, NATO could better serve as a coordinator and multiplier of good practices (of which these countries are, to a significant extent, a model). Second, there is no need to reinvent the wheel. The work ahead can be built on the existing *acquis* and institutions without substantial additional resources, which is important given budgetary constraints. Third, there is clearly more scope and possibility for NATO to better foster synergies with other organisations—most notably the EU—in helping each other and partner countries to fight foreign disinformation. Overall, NATO and the West must take a more offensive approach in tackling this ever more dangerous scourge.[42]

[42] T. Chłoń, "NATO and Countering Disinformation The Need for a More Proactive Approach from the Member States," Globsec, www.globsec.org/publications/15591 (accessed 22.10.2022).

FILIP BRYJKA
Polish Institute of International Affairs
Institute of Political Studies, Polish Academy of Sciences
ORCID: 0000-0002-8613-1030

Detecting and Countering Disinformation —A Proposal for a Syllabus for a University Course

We are a network society.[1] This obvious statement has non-obvious consequences. Socio-economic changes, including the dynamic technological development of the last decades, have irretrievably changed the way we operate, communicate, acquire knowledge, and perceive the world every day. In cyberspace, we make purchases, learn, work, communicate (regardless of geographic distance), and follow events around the world. The internet has become such a common tool of everyday use that the vast majority of its users have lost their elementary distance and security reflexes related to its content. The amenities offered by cyberspace were particularly felt during the COVID-19 pandemic,

[1] M. Castells, "The Rise of the Network Society," Wiley-Blackwell, West Sussex 2011, DOI: 10.1002/9781444319514.

in which the global spread of the virus forced billions of people to limit their contacts with others to the necessary minimum. Despite this, many have had the opportunity to continue working remotely, participate in webinars or learn without leaving home. Against this background, the areas of social exclusion, development disproportion between states, and their internal weaknesses are also visible.

There are about 4.57 billion active internet users worldwide. Every second, each of them produces 1.7 megabytes of data, and the whole of humanity creates 2.5 trillion MB of data every day. Everything indicates that in the future, these numbers will only increase, which will be combined not only with socio-economic dynamics and lifestyle pressure but also with technological acceleration, resulting in faster, more powerful computing powers (quantum computers), new applications for them (Internet of Things), or quasi-human possibilities of machines (artificial intelligence).[2] All this will only increase the temptation and provide new opportunities for variously motivated entities operating in the domain of deliberate disinformation, half-truths, and alternative realities to achieve political and financial benefits, if not only to harm individuals, nations, and the international community.

Over the last two decades, as much as 90% of all existing global data has been produced. According to forecasts, this number will increase to 463 exabytes by 2025.[3] So how are people and nations to find themselves in the deluge of information? How to

[2] R. Kupiecki, "Sztuczna inteligencja a bezpieczeństwo międzynarodowe w przyszłości," [in:] R. Kuźniar, A. Bieńczyk-Missala, P. Grzebyk, R. Kupiecki, M. Madej, K. Pronińska, A. Szeptycki, P. Śledź, M. Tabor, A. Wojciuk (eds.), *Bezpieczeństwo międzynarodowe*, Wydawnictwo Naukowe Scholar, Warszawa 2020, pp. 472–497.

[3] An exabyte is 1 billion gigabytes (GB). See: J. Bulao, "How Much Data Is Created Every Day in 2020?," *Tech Jury*, www.techjury.net/blog/how-much-data-is-created-every-day (accessed 23.11.2022).

select them and assess their credibility? How to distinguish true information from manipulated or completely false information? How to permanently test the reliability of information sources and producers? Continuous social changes, accelerated by the development of modern means of communication, allow some observers of reality to call our times the epoch of "post-truth". Within it, real authorities, verified information, and knowledge coexist with various forms of deliberate falsehood (also used as a weapon in political conflicts and long-lasting operations on human consciousness), or the "silliness" of pseudo-authorities[4] popularised by the tabloidised media. The answers to the above questions are of particular importance for the world (in its geographic, social, and mental spheres), in which the reliability and credibility of information is not what counts, but its monetised "click-through rate", distribution rate, and range of impact.

Facts (true information), coexisting with falsehood, may therefore increasingly not affect the recipient, who is to decide for themself what to believe. This is a great privilege of freedom, the full use of which, however, requires elementary knowledge of the world, intellectual effort, and basic intellectual standards. Today, however, computer algorithms collect data on user activity on the web, analyse preferences and interests, and then make suggestions in line with the anticipated expectations or "needs". Contemporary technological possibilities in the field of profiling provide wide room for manoeuvre for social engineering, including directly and effectively influencing the attitudes and political decisions of

[4] I use the term "silliness" on purpose, understanding its unscientific and hardly definable nature. In the context of this text, however, I mean the consequences of the lack of knowledge, refusal to know and popularisation of similar attitudes by media, in each case leading to irrational behaviour, i.e., not using reliable and complete information in order to make optimal decisions.

individuals and states.[5] Therefore, the challenge for every human being today is the proper and safe use of the possibilities offered by the virtual world.

In the 21st century, cyberspace also became a field of modern influence (for civil or military purposes), information warfare, cyberattacks, data theft, creation of a false identity, cyberespionage, tracking, and surveillance of our activities. New technologies offer wide opportunities to create an alternative reality through the mass production and distribution of manipulated or completely false information, used by some countries systematically and over long periods to influence social attitudes and decisions made by the opponent or competitor. These actions can also be used to cause riots, social unrest, and even armed conflicts. In the latter, they can also be one of the areas of conflict.

The use of information as a tool of politics, diplomacy, trade, and warfare is, in fact, an age-old strategy. Chinese general and philosopher Sun Tzu stated that "warfare is based on deception (...) Therefore, a hundred victories in a hundred battles is not the pinnacle of skill. The greatest skill is to defeat the opponent without a fight. So, the most important thing is to hit your opponent's very strategy". Although these words were formulated in the 6th century BC, they also accurately reflect the essence of modern armed

[5] Such practices raise serious ethical questions, which is exemplified by the role of Cambridge Analytica (CA) in the presidential elections in the United States (2016), the referendum on the withdrawal of United Kingdom from the European Union, and the separation of Catalonia from Spain (2017). Without the users' knowledge, CA obtained data from 50 million Facebook users, thanks to which it developed a model for segmenting and targeting voters. On this basis, special content and methods of its distribution on social media have been developed in order to reach voters and influence their attitudes, for more, see: E.L. Boldyreva, N.Y. Grishina, Y. Duisembina, "Cambridge Analytica: ethics and online manipulation with decision-making process," *The European Proceedings of Social & Behavioural Sciences*, 2018, pp. 91–102, DOI: 10.15405/epsbs.2018.12.02.10.

conflicts, known as "hybrid" wars.[6] A contemporary adaptation of Sun Tzu's strategic thought is the Chinese concept of unrestricted warfare.[7]

So how do you prevent disinformation? How to distinguish real information from "fake news"? How do you assess the credibility of an information source and make an appropriate selection? How can you immunise yourself and our surroundings against massive disinformation attacks? How can we teach this to adults and teenagers from the earliest stages of education? the academic syllabus below proposes a basic educational approach to recognising and combating disinformation. The subject matter of the course focuses on information and psychological operations undertaken by the Russian Federation against the transatlantic community. Since 2014, we have observed a significant increase in the offensive activity in cyberspace of entities that are part of Russian state structures, or act on their behalf, and conduct mass-scale disinformation campaigns aimed at NATO and EU countries.

Of course, this phenomenon is not limited to the Russian direction. Similar activities are also undertaken by other participants in international relations who aspire to global

[6] The essence of "hybrid war" is the combination of conventional and unconventional methods of fighting, for more, see: F.G. Hoffman, "Hybrid Warfare and Challenges," *Joint Force Quarterly*, 2009, no 52; M.A. Piotrowski, "Konflikt nigdy nie jest prosty: amerykańska teoria i doktryna wojen oraz przeciwników hybrydowych," *Sprawy Międzynarodowe*, 2015, no 2, pp. 7–38.

[7] Its authors believe that China should (without any legal and moral restrictions) resort to all methods of weakening, exhausting, and defeating opponents with a military advantage. When formulating these assumptions, they meant primarily the military power of the United States. They included combined military and paramilitary operations, psychological, media, computer, financial, economic, criminal, and terrorist activities as "integrated attacks", see: Q. Liang, W. Xiangsui, *Unrestricted Warfare: China's Master Plan to Destroy America*, Pan American Publishing Company, Panama City, 2002.

or regional superpower roles. The cases of China[8] and Iran[9] are well described. However, all countries in the world use information tools of influence and modern information carriers (on a different scale). However, not all of them systematically use disinformation or prepared information strings. Also, not all of them make it a permanent instrument of politics, diplomacy, or offensive influence. Information warfare[10] is not only the domain of state actors. Activities in this area are also carried out by non-state entities, including terrorist organisations, such as ISIS.[11] Information manipulation is also a tool of political competition in the domestic or local dimension.

Taking into account the extremely wide scope of this subject, the following syllabus focuses on threats from the eastern direction. In this context, Russia is not only a historical pioneer, but also a "model" of (dis)informational influence in the contemporary world. Also, in this form, it is today the greatest challenge for Poland and the transatlantic community.

However, individual parts of the course can be modified and adapted to the needs of lecturers and individual target groups. It is a basic course. Its completion primarily equips students with the necessary theoretical knowledge and practical skills in detecting, analysing and unmasking disinformation. It is also supposed to

[8] I. Karásková, "One China under media heaven: How Beijing hones its skills in information operations," *Hybrid CoE Strategic Analysis* 23, 2020, www.hybridcoe.fi/wp-content/uploads/2020/06/20200625_Strategic-Analysis_23_China_Web.pdf (accessed 30.11.2022).

[9] C. Kasapoglu, M. Fekry, "Iran's proxy war in Yemen: the information warfare landscape," NATO StratCom COE, 2020, www.stratcomcoe.org/irans-proxy-war-yemen-information-warfare-landscape (accessed 30.11.2022).

[10] See: T. Aleksandrowicz, "Podstawy walki informacyjnej," *Editions Spotkania*, Warszawa 2016.

[11] Ch. Winter, "Daesh Propaganda, Before and After its Collapse," NATO StratCom COE, 2019, www.stratcomcoe.org/daesh-propaganda-and-after-its-collapse (accessed 30.11.2022).

supplement their skills allowing the use of information and its modern sources and carriers in a manner consistent with the standards of "safety and occupational hygiene".

The syllabus consists of three related modules:

1) Detecting disinformation;
2) Identifying and analysing disinformation;
3) Fighting disinformation.

Each of them contains five detailed topics of classes, carried out in the form of lectures, seminars, or practical exercises. The course has been designed as a standard academic cycle of 30 hours of class time. Depending on the needs, it can be extended or limited to elements of interest to individual audiences. A list of basic literature is attached to each module of the course. It could, of course, be much wider and selected according to other criteria. The following material focuses on information (content), leaving the methodological issues to the decisions of users who are subject to different didactic conditions.

The course is addressed primarily to academic teachers conducting classes in international relations, security (international and internal), various political science subjects, history, sociology, journalism, law, or the broadly understood information warfare. Its components, however, should constitute the integral content of education in all modern fields of study, regardless of the scientific discipline or type of institution. An important group of students should also be civilian and military students at military academies and other uniformed services. In its advanced form, the syllabus can also be implemented as part of specialist courses for journalists, analysts, soldiers, or experts in the field of information warfare and/or Eastern affairs, as well as public administration employees. In its simplified form, it can be used in earlier stages of education, for example, in secondary schools. One of the key practical elements of the syllabus are classes in critical thinking,

fact-checking, media education, and safe use of social media and other information carriers.

MODULE I
DETECTING DISINFORMATION

Topic 1—Disinformation as an element of information warfare

- The concept of disinformation - general characteristics.
- Goals of disinformation - general characteristics: individual and collective, civil and military applications.
- Disinformation as a tool of information warfare/information influence.
- Characteristics of the information warfare phenomenon: definition framework, main assumptions, goals, and methods of implementation.
- The influence of new technologies on the development of the information warfare phenomenon.
- Elements of information warfare: press and information activity (Public Affairs), public diplomacy, strategic communication (StratCom), propaganda (white, grey, black), information operations (InfoOps), psychological operations (PsyOps), influence operations (Influence Ops).
- Similarities and differences in the Western and Eastern understanding of information warfare.
- Information warfare methods: disinformation, inspiration, deception, *maskirovka*, social engineering, "fake news", "deep fake", "clickbait".
- Disinformation techniques.
- Entities participating in disinformation activities: intelligence services, "trolls", "agents of influence", "useful idiots", "bots".

Topic 2—Militarisation of information in the strategic culture of the Russian Federation

- Historical outline: the use of disinformation by tsarist Ochrana, the development of information and the psychological ability to influence the creation and strengthening of the totalitarian regime of Soviet Russia; operation "MOCR-Trust" - case study analysis; use of "active measures" by the KGB during the Cold War.
- Intellectual foundations of the modern Russian information warfare strategy: Alexander Dugin's network war concept, Igor Panarin's information warfare school, the concept of "reflective control", the importance of information and psychological activities in the Russian concept of "new generation wars", also known as the "Gerasimov doctrine".
- Information struggle in Russian strategic documents.

Topic 3—Russian information-psychological operations in practice

- The role of Russian intelligence services in leading and inspiring disinformation operations: Federal Security Service (FSB), Foreign Intelligence Service (SVR), Main Intelligence Directorate of the General Staff of the Russian Federation (GRU).
- Russian institutions participating in disinformation activities: Moscow State Institute of International Relations (MGIMO), Russian Institute of Strategic Studies (RISI), Internet Research Agency (RIA), Council for Foreign and Defense Policy (SVOP), Russian Council of International Affairs, (RIAC), Valdai Club, Centre for Strategy and Technology Analysis (CAST), Centre for Energy and Security Research (CENESS), Centre for Strategic Research (CSR).

- Russian disinformation distribution channels: traditional media (including RT, TASS, Rossija Siegodnia, Novosti), online platforms (e.g., Sputnik, Regnum), whistle-blower portals (WikiLeaks, DCLeaks), "alternative media" and groups on social networks, bloggers (e.g., Alex Jones and his InfoWars).
- The main goals, areas, methods, and techniques of Russian disinformation operations against NATO countries since 2014.

Topic 4—Russian (dis)information interference in the political processes of selected NATO member states

- Case study of the presidential elections in the United States (2016).
- A case study of the disinformation campaign on "Brexit" – the UK leaving the structures of the European Union.
- Case study of Montenegro's accession to NATO (2016)
- Case study of presidential elections in France (2017).
- Case study of the disinformation campaign on the secession of Catalonia from Spain (2017).
- A case study of parliamentary elections in Germany (2017).

Topic 5—The importance of information and psychological operations in contemporary military operations

- A case study of the Russian aggression against Georgia (2008).
- Case study of the illegal annexation of Crimea and Russian aggression in eastern Ukraine (since 2014).
- A case study of the Russian military intervention in Syria (from 2015).
- Disinformation activities accompanying military exercises with the participation of Russian troops - a case study of the *Zapad-17* and *Zapad-21* manoeuvres.

- Information and psychological actions taken by Russia against the countries of NATO's Eastern Flank.
- Russian disinformation regarding the invasion of Ukraine.

Literature for Module I:

Aleksandrowicz T., *Podstawy walki informacyjnej*, Editions Spotkania, Warszawa 2016.

Analysis of Russia's Information Campaign Against Ukraine, NATO StratCom CoE, Riga 2015.

Applebaum A., Pomerantsev P., Smith M., *"Make Germany Great Again": Kremlin, Alt-Right and International Influences in the 2017 German Elections*, Institute for Strategic Dialogue, London-Washington-Beirut-Toronto, 2017, www.isdglobal.org/wp-content/uploads/2017/12/Make-Germany-Great-Again-ENG-061217.pdf (accessed 30.11.2022).

Bagge D., *Unmasking Maskirovka: Russia's Cyber Influence Operations*, Defense Press, New York 2019.

Bajrović R., Garčević V., Kraemer R., "Hanging by a Thread: Russia's Strategy of De- stabilisation in Montenegro," *Russia Foreign Policy Papers*, June 2018.

Barbashin A., Graef A., *Thinking Foreign Policy in Russia: Think Tanks and Grand Narratives*, www.atlanticcouncil.org/wp-content/uploads/2019/11/Thinking-Foreign-Policy-in-Russia_-Think-Tanks-and-Grand-Narratives-Atlantic-Council-11.12.19.pdf (accessed 12.04.2022).

Bechev D., "The 2016 Coup Attempt in Montenegro: Is Russia's Balkans Footprint Expanding?," *Russia Foreign Policy Papers*, April 2018.

Bryjka F., "Russian Disinformation Regarding the Attack on Ukraine," *PISM Spotlight*, 2022, no 15.

Bryjka F., "Nationalism as a Tool of Russian Subversive Foreign Policy in the Western Balkans—a case of Montenegro," *Integrations*, October 2017, p. 8–10.

Bryjka F., Legucka A., "Russian and Belarusian Disinformation and Propaganda in the Context of the Polish-Belarusian Border Crisis," *PISM Bulletin*, no 212 (1908) 9 December 2021, www.pism.pl/publications/russian-and-belarusian-disinformation-and-propaganda-in-the-context-of-the-polish-belarusian-border-crisis.

Charen M., *Useful Idiots: How Liberals Got It Wrong in the Cold War and Still Blame America First*, Lahnam 2003.

Darczewska J., "The anatomy of Russian information warfare. The Crimean operation, a case study," *Point of View*, no 42, https://www.osw.waw.pl/en/publikacje/point-view/2014-05-22/anatomy-russian-information-warfare-crimean-operation-a-case-study (accessed 12.12.2022).

Darczewska J., "The devil is in the details. Information warfare in the light of Russia's military doctrine," *Point of View*, no 50, www.osw.waw.pl/en/publikacje/point-view/2015-05-19/devil-details-information-warfare-light-russias-military-doctrine (accessed 12.12.2022).

Darczewska J., Żochowski P., "Russophobia in the Kremlin's strategy. A weapon of mass destruction," *Point of View*, no 56, https://www.osw.waw.pl/en/publikacje/point-view/2015-11-02/russophobia-kremlins-strategy-a-weapon-mass-destruction (accessed 30.11.2022).

Darczewska J., Żochowski P., "Active measures. Russia's key export," *Point of View*, no 64, pp. 12–14, www.osw.waw.pl/en/publikacje/point-view/2017-05-30/active-measures-russias-key-export (accessed 12.12.2022).

Darczewska J., "Between overt disinformation and covert practice The Russian special services' game," *Point of View*, no 73, www.osw.waw.pl/en/publikacje/point-view/2019-03-28/between-overt-disinformation-and-covert-practice (accessed 30.11.2022).

Darczewska J., "Russia's armed forces on the information war front. Strategic documents," *Point of View*, no 57, www.osw.waw.pl/en/publikacje/osw-studies/2016-06-27/russias-armed-forces-information-war-front-strategic-documents (accessed: 12.12.2022).
DiResta R., Grossman Sh., *Potemkin pages and personas. assessing GRU online operations 2014–2019*, Stanford University, Stanford 2019.
Galeotti M., "Putin's Hydra: Inside Russia's Intelligence Services," *Policy Brief*, European Council on Foreign Relations, 2016, nr 169.
Giles K., *Handbook of Russian information warfare*, NATO Defence College Fellowship Monograph, 9, Rome 2016, www.ndc.nato.int/news/news.php?icode=995 (accessed 30.11.2022).
Giles K., Sherr J., Seaboyer A., *Russian reflexive control*, Royal Military College of Canada, Kingston 2018.
Helmus T.C. (in.), *Russian Social Media Influence: Understanding Russian Propaganda in Eastern Europe*, RAND Corporation, Santa Monica 2018, www.rand.org/pubs/research_reports/RR2237.html (accessed 30.11.2022).
Juurvee I., "The resurrection of 'active measures': Intelligence services as a part of Russia's influencing toolbox," *Hybrid CoE Strategic Analysis*, 2018.
Kasapoglu C., "Russia's Renewed Military Thinking. Non-linear Warfare and Reflexive Control," *NATO Defence College Research Paper*, 121, Rome 2015, www.ndc.nato.int/news/news.php?icode=877 (accessed 30.11.2022).
Kupiecki R., Bryjka F., Chłoń T., *Dezinformacja międzynarodowa. Pojęcie, rozpoznanie, przewciwdziałanie*, Wydawnictwo Naukowe Scholar, Warszawa 2022.
Kupiecki R., "'Mit założycielski' polityki zagranicznej Rosji," *Sprawy Międzynarodowe*, 2019, no 4, p. 77–105,

DOI: 10.35757/SM.2019.72.4.03, www.researchgate.net/publication/344069207_ROBERT_KUPIECKI_Mit_zalozycielski_polityki_zagranicznej_Rosji (accessed 9.12.2022).
Kupiecki R., "Sztuczna inteligencja a bezpieczeństwo międzynarodowe w przyszłości," [in:] R. Kuźniar, A. Bieńczyk-Missala, P. Grzebyk, R. Kupiecki, M. Madej, K. Pronińska, A. Szeptycki, P. Śledź, M. Tabor, A. Wojciuk, *Bezpieczeństwo międzynarodowe*, Wydawnictwo Naukowe Scholar, Warszawa 2020, pp. 472–497.
Lange-Ionatamishvili E., Svetoka S., *Strategic Communications and Social Media in the Russia Ukraine Conflict*, NATO Cooperative Cyber Defence CoE, Tallinn 2015.
Laurinavičius M., A *Guide to the Russian Tool Box of Election Meddling: a Platform to Analyse the Long Term Comprehensive Kremlin Strategy of Malign Influence*, International Elections Study Center, December 2018, www.iesc.lt/app/uploads/2018/10/IESC_Guide_ToolBox_2018_FINAL.pdf (accessed 30.11.2022).
Kupiecki R., Legucka A., (eds.), *Disinformation, Narratives and Memory Politics in Russia and Belarus*, Routledge, London 2022.
Mitrochin W., *KGB Lexicon: The Soviet Intelligence Officer's Handbook*, London 2002.
Nimmo B., *Backdating the Blame How Russia Made NATO a Party to the Ukraine Conflict*, NATO StratCom CoE, Riga 2015.
Paul Ch., Matthews M., *The Russian "Firehose of Falsehood" Propaganda Model*, RAND Corporation, Santa Monica 2017, www.rand.org/content/dam/rand/pubs/perspectives/PE100/PE198/RAND_PE198.pdf (accessed 30.11.2022).
Polyakova A., Hansen F.S., Van der Noordaa R., Bogen Ø., Sundbom H., *The Kremlin's Trojan Horses 3.0. Russian Influence in Denmark, The Netherlands, Norway, and Sweden*,

www.atlanticcouncil.org/in-depth-research-reports/report/the-kremlins-trojan-horses-3-0 (accessed 30.11.2022).
Polyakova A., Kounalakis M., Klapsis A., Germani L.S., Iacoboni J., Lasheras F.B., Pedro N., *Kremlin's Trojan Horses 2.0. Russian Influence in Greece, Italy, and Spain*, Atlantic Council, 2017, www.atlanticcouncil.org/in-depth-research-reports/report/the-kremlin-s-trojan-horses-2-0 (accessed 30.11.2022).
Polyakova A., Laruelle M., Meister S., N. Barnett, *Kremlin's Trojan Horses. Russian Influence in France, Germany, and the United Kingdom*, Atlantic Council, 2016, www.atlanticcouncil.org/in-depth-research-reports/report/kremlin-trojan-horses (accessed 30.11.2022).
Rid T., *Active Measures: The Secret History of Disinformation and Political Warfare*, Macmillan, New York 2020.
Rychlak R., Pacepa I.M., *Disinformation: Former Spy Chief Reveals Secret Strategies for Undermining Freedom, Attacking Religion, and Promoting Terrorism*, WND Books, Washington 2013.
Sazonov V., Müür K., Mölder H. (eds.), *Russian Information Campaign Against Ukrainian State and Defence Forces*, NATO StratCom CoE/Estonian National Defence College, Tartu 2016.
Smagliy K., *Hybrid Analytica: Pro-Kremlin Expert Propaganda in Moscow, Europe and the U.S. A Case Study of Think Tanks and Universities*, Institute of Modern Russia, Research Paper, October 2018, www.static1.squarespace.com/static/59f8f41ef14aa13b95239af0/t/5c6d8b38b208fc7087fd2b2a/1550682943143/Smagliy_Hybrid-Analytica_10-2018_upd.pdf (accessed 30.11.2022).
Stengel R., *Information Wars: How We Lost the Global Battle Against Disinformation and What We Can Do About It*, Grove Press UK, London 2019.
Szwed R., *Framing of the Ukraine – Russia Conflict in Online and Social Media*, NATO StratCom CoE, Riga 2016.

Thomas T.L., "Russia's reflexive control theory and the military," *Journal of Slavic Military Studies*, 2004, no 17(2), pp. 237–256, DOI: 10.1080/13518040490450529.
Weiss M., *Aquarium leaks. Inside the GRU's psychological warfare program*, *4FreeRussia*, www.4freerussia.org/aquarium-leaks-inside-the-gru-s-psychological-warfare-program (accessed 9.12.2022).
Van Herpen M., *Putin's propaganda machine. Soft power and Russian foreign policy*, Rowman & Littlefield Publishers, London 2015.

MODULE II
IDENTIFYING AND ANALYSING DISINFORMATION

Topic 1—Introduction to critical thinking, fact-checking, and media education

- Critical thinking and intellectual standards—general remarks.
- Critical analysis of media messages (news literacy).
- Asking questions as a critical thinking tool.
- Filter bubbles.
- Selected fact-checking organisations (FactCheck.org., PolitiFact, The Washington Post Fact-Checker, Full Fact, Demagog, AllSides).
- The basic principles of information verification as set out in the International Fact-Checking Network (IFCN), The Code of fact-checking organisations.
- Information verification methods: CRAAP analysis (currency, relevance, accuracy, authority and purpose); Admiralty Code.
- Systems for assessing the reliability of information and its sources used by fact-checking organisations.

Topic 2—Workshop on critical thinking and fact-checking

- Identifying disinformation techniques.
- Distinguishing between facts and opinions.
- Critical analysis and fact-checking of content containing true, partially true, manipulated and/or completely false information about vaccines.
- Critical analysis and fact-checking of content containing true, partially true, manipulated and/or completely false information about the COVID-19 pandemic.
- Critical analysis and fact-checking of content containing true, partially true, manipulated and/or completely false information about 5G technology.

Topic 3—Identifying disinformation campaigns using open-source intelligence (OSINT) methods

- Introduction to the subject of open-source intelligence: definition, place and meaning of OSINT in the intelligence cycle, examples of open sources of information.
- Open-source recognition methodology: determining the object of recognition, formulating intelligence questions, pattern of open-source recognition, methodology of data collection and management, a tool supporting the data-collection process (e.g., Maltego).
- Operational security (OpSec) of open-source activities (anonymisation and masking of own activity in cyberspace, risk analysis).
- Analysis of information obtained with the use of open-source interview methods.

Topic 4—The practice of open-source activities

- Advanced methods of obtaining information in search engines (including Google, DuckDuckGo, Bing, Entireweb, Yandex).
- Tools for collecting statistical data, tracking trends and distributing information on the Internet (including Google Trends).
- Social media analysis tools (including Netlytic, Socialbearing, Follow The Hashtag, TweetDeck).
- Tools for advanced image search and analysis (including Google Images, TinEye, FotoForensics).
- Tools for analysing video materials (including YouTube Data Viewer).
- Search for information on changed or deleted websites (including The Internet Archive Wayback Machine).
- Tools for obtaining and verifying information about people and other entities (including Email Checker, PIPL, Facebook Graph Search).

Topic 5—Workshops on identifying disinformation campaigns with the use of open-source intelligence methods

- Practical application of acquired knowledge and skills in the course of an own investigation based on specially prepared materials (e.g., Russian disinformation activities after the shooting down of Malaysian Air Flight MH-17 over Ukraine; Russian disinformation activities concerning a chemical attack in Syria).

Literature for Module II:

Akhgar B., P.S. Bayerl, F. Sampson, *Open Source Intelligence Investigation: From Strategy to Implementation*, Springer, Cham 2016.

AllSides, www.allsides.com (accessed 4.12.2022).
Bal M., *Narratology. Introduction to the Theory of Narrative*, University of Toronto Press, Toronto 2009.
Bazzel M., *Open Source Intelligence Techniques*, 7th Edition, independently published, 2019.
Benes L., "OSINT, New Technologies, Education: Expanding Opportunities and Threats. A New Paradigm," *Journal of Strategic Security*, 2013, no 6(5), pp. 22–37, DOI: 10.5038/1944-0472.6.3S.3
Bertram S., *The Tao of Open Source Intelligence*, ITGP, 2015.
Bielska A., Kurz N.R., Baumgartner Y., Benetis V., *Open Source Intelligence Tools and Resources Handbook*, I-intelligence GmbH, www.i-intelligence.eu/uploads/public-documents/OSINT_Handbook_2020.pdf (accessed 29.11.2022).
Broadbent H., *Fake News and Critical Thinking*, www.saferinternet.org.uk/blog/fake-news-and-critical-thinking (accessed 04.12.2020).
Brożek B., *Myślenie. Podręcznik użytkownika*, Copernicus Center Press, b.m.wyd., 2016.
Cherubini F., Graves L., *The Rise of Fact-Checking Sites in Europe*, University of Oxford, Reuters Institute for the study of Journalism, Oxford 2016, www.reutersinstitute.politics.ox.ac.uk/sites/default/files/research/files/The%2520Rise%25200f%2520Fact-Checking%2520Sites%2520in%2520Europe.pdf (accessed 29.11.2022).
EEAS Special Report Update: Short Assessment of Narratives and Disinformation around the COVID-19 Pandemic, www.euvsdisinfo.eu/eeas-special-report-update-short-assessment-of-narratives-and-disinformation-around-the-covid-19-pandemic-update-may-november (accessed 9.12.2020).
FactCheck, www.factcheck.org/fake-news (accessed 4.12.2022).

Hassan N.A., Hijazi R., *Open Source Intelligence Methods and Tools. A Practical Guide to Online Intelligence*, Apress, Berkeley 2018, DOI: 10.1007/978-1-4842-3213-2
Ireton Ch. Posetti, J., *Journalism, Fake News & Disinformation: Handbook for Journalism Education and Training*, www.unesdoc.unesco.org/ark:/48223/pf0000265552 (accessed 9.12.2022).
Kahneman D., *Pułapki myślenia. O myśleniu szybkim i wolnym*, Media Rodzina, Poznań 2012.
Kozłowski J., *Teoria i praktyka działań analityczno-informacyjnych*, Akademia Sztuki Wojennej, Warszawa 2016.
Levitin D.L., *Weaponised Lies: How to Think Critically in the Post-Truth Era?*, Penguin Random House, New York 2016.
Lucas G., *Deciding What's True. The Rise of Political Fact-checking in American Journalism*, Columbia University Press, New York 2016.
Moore D.T., *Critical Thinking and Intelligence Analysis*, National Defence Intelligence College, Washington D.C. 2009.
PolitiFact, www.politifact.com (accessed 4.12.2022).
Quis on Critical Thinking, www.quislet.com/6376125/six-principles-of-critical-thinking-flash-cards (accessed 4.12.2022).
Tekir S., *Open Source Intelligence Analysis: a Methodological Approach*, VDM Verlag, 2013.

MODULE III
FIGHTING DISINFORMATION

Topic 1—Fighting disinformation by state institutions

- Legal regulations as a form of combating disinformation with the example of selected NATO countries.
- The role of intelligence and counterintelligence services.

- Fighting disinformation by military institutions.
- Examples of state institutions to combat disinformation.

Topic 2—International cooperation in the field of recognising and combating disinformation

- International cooperation in combating disinformation: the case of NATO and the European Union.
- International cooperation in fighting disinformation: opportunities and limitations.
- The role and tasks of the NATO Centre of Excellence for Strategic Communications in Riga (Latvia).
- The role and tasks of the EU StratCom Task Force.
- The role and tasks of the European Centre of Excellence for Combating Hybrid Threats in Helsinki (Finland).

Topic 3—Non-governmental initiatives in the field of identifying, analysing, and combating disinformation

- Atlantic Council Digital Forensic Research Lab.
- The Kremlin Watch programme implemented by the Czech think-tank European Values Center.
- GMFUS Alliance for Securing Democracy.
- Strategic communication programmes of the Slovak think-tank GLOBSEC.
- The international StopFake initiative.
- InformNapalm - the Ukrainian front of information warfare.
- Bellingcat - an international open-source intelligence agency.

Topic 4—Non-governmental initiatives in the field of identifying, analysing, and combating disinformation in Poland

- DisInfo Digest programme implemented by the INFO OPS Polska Foundation.
- Center for Propaganda and Disinformation Analysis (CAPiD).

- The Media Education programme implemented by the Modern Poland Foundation.
- Foundation "Counteracting Disinformation".
- Kremlin Watchers Movement.
- Fact-Checking Academy run by the Demagog Association.

Topic 5—Combating disinformation at the individual level

- Developing good habits (including skilful checking of sources, verifying URLs and names of websites, a critical approach).
- Building cyber-awareness and resilience to disinformation.
- Self-identification and disclosure of disinformation campaigns.
- Creation of your own initiatives to combat disinformation.

Literature for Module III:

Atlantic Council Digital Forensic Research Lab, www.atlanticcouncil.org/programs/digital-forensic-research-lab (accessed 9.12.2022).

Bay S., Fredheim R., *Falling Behind: How Social Media Companies are Failing to Combat Inauthentic Behaviour Online*, NATO StratCom CoE, Riga 2019.

Bellingcat, www.bellingcat.com (accessed 4.12.2022).

Bodine-Baron E., *Countering Russian Social Media Influence*, RAND Corporation, Santa Monica 2018, www.rand.org/pubs/research_reports/RR2740.html (accessed 30.11.2022).

Bryjka F., "Tracing the Development of EU Capabilities to Counter Hybrid Threats," *PISM Strategic File*, No. 9, 2022.

Centrum Analiz Propagandy i Dezinformacji, www.capd.pl/pl (accessed 4.12.2022).

CounterDisInfo Online Toolkit, www.counterdisinfo.org (accessed 4.12.2022).

Countering Disinformation, www.eeas.europa.eu/topics/countering-disinformation_en?page=1 (accessed 4.12.2022).
Demagog, www.demagog.org.pl (accessed 9.12.2022).
East Stratcom Task Force, www.euvsdisinfo.eu/disinformation-cases (accessed 30.11.2022).
Edukacja medialna, www.edukacjamedialna.edu.pl (accessed 9.12.2022).
European Centre of Excellence for Countering Hybrid Threats, www.hybridcoe.fi (accessed 4.12.2022).
Fundacja Przeciwdziałamy Dezinformacji, www.fakenews.pl (accessed 9.12.2022).
GMFUS Alliance for Securing Democracy, www.securingdemocracy.gmfus.org (accessed 9.12.2022).
INFOOPS Polska, www.infoops.pl (accessed 4.12.2022).
InformNapalm, www.informnapalm.org (accessed 4.12.2022).
Janda J., Víchová V. (eds.), *Kremlin Watch Strategy for Countering Hostile Russian Interference*, Kremlin Watch Program 2019.
Kremlin Watch, www.kremlinwatch.eu (accessed 4.12.2022).
McDougall J., Zezulkova M., Van Driel B., Sternadel D., *Teaching Media Literacy in Europe: Evidence of Effective School Practices in Primary and Secondary Education*, NESET II, www.eprints.bournemouth.ac.uk/31574/1/AR2_Teaching%20Media%20Literacy_NESET.pdf (accessed 9.12.2022).
Milo D., Klingová K., *Countering Information War: Lessons Learned from NATO and Partner Countries*, GLOBSEC Policy Institute, Bratislava 2016.
Milo D., Klingová K., *Vulnerability Index: Subversive Russian Influence in Central Europe*, GLOBSEC Policy Institute 2017.
NATO StratCom Centre of Excellence, www.stratcomcoe.org (accessed 4.12.2022).

NATO's approach to countering disinformation: a focus on COVID-19, www.nato.int/cps/en/natohq/177273.htm (accessed 4.12.2022).
Obserwatorzy Kremla, www.facebook.com/ObserwatorzyKremla (accessed 4.12.2022).
Raport: zjawisko dezinformacji w dobie rewolucji cyfrowej, NASK CyberPolicy, www.cyberpolicy.nask.pl/raport-zjawisko-dezinformacji-w-dobie-rewolucji-cyfrowej-panstwo-spoleczenstwo-polityka-bisnes (accessed 9.12.2022).
RESIST Disinformation: a toolkit, UK Government Communication Service, www.fundacioncarolina.es/wp-content/uploads/2020/11/Toolkit-UK.pdf (accessed 4.12.2022).
Smoleňová I., Chrzová B. (eds.), *United We Stand, Divided We Fall: The Kremlin's Leverage in the Visegrad Countries*, Prague Security Studies Institute, 2017.
StopFake, www.stopfake.org (accessed 4.12.2022).
Šuplata M., Nič M., *Russia's Information War in Central Europe: New Trends and Counter-Measures*, GLOBSEC Policy Institute, 2016.
Víchová V., Janda J. (eds.*),"* The Prague Manual. How to Tailor National Strategy Using Lessons Learned from Countering Kremlin's Hostile Subversive Operations in Central and Eastern Europe," *Kremlin Watch Report*, European Values, 30.04.2018.
Wenerski Ł., Kacewicz M., *Russian Soft Power in Poland The Kremlin and pro-Russian Organisations*, Political Capital, April 2017.
Wenerski Ł., "The Visegrad Countries and 'Post-Truth' Who is Responsible for Delivering the Kremlin's Narrative to the Czech Republic, Hungary, Slovakia and Poland?, *Policy Brief*, June 2017.

Useful Websites/Databases:

Atlantic Council Digital Forensic Research Lab, www.atlanticcouncil.org/programs/digital-forensic-research-lab
Balkan Insight, www.balkaninsight.com
BBC Reality Check, www.bbc.com/news/reality_check
Bellingcat, www.bellingcat.com
Brookings, www.brookings.edu
BUZZFEED NEWS, www.buzzfeednews.com
CNN, www.edition.cnn.com
Carnegie Europe, www.carnegieeurope.eu
Center for European Policy Analysis (CEPA), www.cepa.org
Center for Security and Emerging Technology (specialised), www.global.georgetown.edu/georgetown_units/center-for-security-and-emerging-technology
Center for Strategic International Studies, www.csis.org
Chatham House, www.chathamhouse.org
Clingendael, Netherlands, Institute of International Relations, www.clingendael.org
Council on Foreign Relations, www.cfr.org
EU DisinfoLab, www.disinfo.eu
Euractiv, www.euractiv.com
European Values Think Tank (Prague), www.europeanvalues.net
Foreign Policy, www.foreignpolicy.com
Foreign Policy Research Institute, www.fpri.org
German Council on Foreign Relations, www.dgap.org/en
German Marshall Fund (GMF), www.gmfus.org
Global Disinformation Index, www.disinformationindex.org
Global Engagement Center (USA) and Disinfo Cloud, www.state.gov/disinfo-cloud-launch
Globsec, www.globsec.org
Google, www.google.pl

Graphika, www.graphika.com
Harvard Kennedy School of Misinformation Review, www.misinforeview.hks.harvard.edu
Institute for Strategic Dialogue, www.isdglobal.org
International Strategic Action Network for Security (ISANS), www.isans.org/en
NATO and Partner Media, www.nato.int/cps/en/natohq/news_room.htm
NATO Defence College, www.ndc.nato.int
NATO's Strategic Communications Centre of Excellence, www.stratcomcoe.org
Ośrodek Studiów Wschodnich, www.osw.waw.pl/pl
Oxford Internet Institute, www.oii.ox.ac.uk
Pew Research Center, www.pewresearch.org
PISM- Polish Institute of International Affairs, www.pism.pl
Polish government website, www.premier.gov.pl/en.html
Politico, www.politico.com, www.politico.eu
RAND Corporation, www.rand.org
Reuter, www.reuters.com
Reuters Institute, www.reutersinstitute.politics.ox.ac.uk
Royal United Services Institute (RUSI), www.rusi.org
Stanford Internet Observatory, www.cyber.fsi.stanford.edu/io/io
The Jamestown Foundation, www.jamestown.org
The Times, www.thetimes.co.uk
Twitter, www.twitter.com
United Nations Department of Global Communications, www.un.org/en/sections/departments/department-global-communications
Visegrad Insight, www.visegradinsight.eu
Woodrow Wilson Center, www.wilsoncenter.org

FILIP BRYJKA
Polish Institute of International Affairs
Institute of Political Studies, Polish Academy of Sciences
ORCID: 0000-0002-8613-1030

Notes on Detecting and Countering Disinformation

General Characteristics of the Phenomenon, Goals, and Tools

Disinformation is a specific, developed type of message based on falsehood "whose purpose is to evoke a view, decision, action or lack thereof in the recipient, in accordance with the premise of the centre that planned the process of misleading the recipient".[1] As Vladimir Volkoff notes, this process is an indispensable element of interpersonal communication.[2] By providing information,

[1] K. Basaj, "Dezinformacja, czyli sztuka manipulacji," www.rcb.gov.pl/dezinformacja-czyli-sztuka-manipulacji (accessed 4.12.2022).

[2] V. Volkoff, "La désinformation: Arme de guerre," *L'Age d'Homme*, Lozanna 1992, p. 5.

a person, intentionally or unconsciously, may mislead the recipient by adding to the "pure information" his own interpretation, assessment, comment, or subjective opinion. Taking into account the criterion of intentionality of the entity being the source or distributor of false information, we can distinguish three types:

1) misinformation—information that does not correspond to reality. It can be spread both intentionally (purposefully) and unintentionally (by mistake);
2) disinformation—deliberately created and/or reproduced false and/or manipulated information, the intention of which is to mislead the recipient for the implementation of specific political, economic, or military goals;
3) malign information (malinformation)—misuse of information, for example, to stigmatise specific social groups, such as "hate speech".

In the second case, we are dealing with a kind of trick, the intention of which is to influence the recipients of the information, consisting of changing the perception of a specific phenomenon in the direction planned by the entity performing the operation. In this approach, disinformation should be seen as an element of information warfare, defined as "actions aimed at protecting, using, damaging, destroying information or information resources, or contradicting information in order to achieve significant benefits, some goal or victory over an opponent."[3] We can see, therefore, that disinformation is or may become a component of a wider phenomenon, including operations conducted by intelligence services and specialised military units.

Entities involved in carrying out information activities (which does not preclude them from acting as objects of disinformation) include:

[3] For more, see: W. Schwartau, *Information Warfare*, Thunder's Mouth Press, New York 1996.

- politicians, businesspeople, government officials;
- special forces;
- specialised military units;
- state institutions (e.g., Ministry of Information, Ministry of Foreign Affairs);
- traditional media (media platforms and press agencies);
- journalists, bloggers, vloggers;
- commentators, "experts", pseudo-authorities;
- social media users (Facebook, Twitter, YouTube, vKontakte, Telegram);
- fake social media accounts, trolls, and bots.

The basic forms and means of disinformation include:

- **Fabrication**—fabricating, manipulating the content of a message, for example, by including a forged document or modified image;
- **Identity**—concealing or stealing an identity, such as using fake social media accounts or pretending to be other people;
- **Rhetoric**—using in the rhetoric argumentation based on false information or offensive attacks, such as the activity of trolls commenting on posts in social media or on internet forums;
- **Symbolism**—inadequate use of symbolism to strengthen the communication message, for example, comparing a politician to a controversial historical figure;
- **Technology**—profiting from a technological advantage, such as bots, which automatically produce false messages on a mass scale.[4]

[4] "RESIST Disinformation: a toolkit," UK Government Communication Service, p. 9, www.fundacioncarolina.es/wp-content/uploads/2020/11/Toolkit-UK.pdf (accessed 12.12.2022).

Basic disinformation techniques include:
- **Astroturfing**—presenting top-down agitation campaigns as civic initiatives; falsely assigning a given message to other entities in order to authenticate them;
- **Bandwagon effect**—a cognitive effect in which a specific opinion or belief grows stronger because it is shared by others, for example, on social media where users are more likely to share articles already shared by a large number of other users than those less popular (regardless of their content);
- **False connection**—a situation in which the title, lead, photos, or graphics do not correspond with the content of the message;
- **False context**—when the content is based on facts, but it is placed in a manipulated informational context;
- **Filter bubble**—is the personalised access to information developed by filtering algorithms based on the user's search history and social media activity, which leads to a situation in which the user first sees the content corresponding to the user's previous activity on the internet;
- **Leaking**—Deliberate dissemination of information obtained unlawfully, such as the publication of classified documents, theft, and publication of private or business correspondence from government officials;
- **Malign rhetoric**—using offensive language, slander, and false accusations to disrupt public debate;
- **Manipulation**—modification of the content of information to change its meaning;
- **Misappropriation**—falsely assigning someone an argument, statement, or position;
- **Satire and parody**—making fun of people (e.g., with memes), narratives, or opinions in order to undermine their importance (position);

- **Sock puppets**—creating a fictional debate between two (or more) entities using new technologies, for example, creating fake social media accounts and conducting discussions between them;
- **Trolling**—deliberately provoking the aggravation of discussions on online forums or on social media by posting controversial, offensive, or emotional comments in order to outrage recipients and draw them into the discussion.[5]

The group of recipients (targets) of information influence includes politicians, diplomats, soldiers, businesspeople, experts, analysts, journalists, commentators, academics, and even entire societies (or specific social environments within them). The measure of the success of the impact of disinformation is the recognition of "truth" by the recipients of the prepared information message. The effect is not only a change in their perception of a given phenomenon but also its duplication (consciously or not) and the perpetuation of disinformation in a wider group of recipients. Manipulated persons, often enjoying authority in society, spreading false information not only increase the scope of the destructive influence of disinformation but also legitimise its "truthfulness" in the information space.

The main goals of disinformation activities include:

- sowing doubts and manipulating public opinion;
- influencing social and political attitudes;
- distracting public debate;
- polarisation of the political climate;
- weakening the cohesion of the state (group of states) being the target of information influence;
- undermining trust in public institutions and media;

[5] For more, see: *ibidem*; I. Brodnig, "Misinformation didn't change the outcome of the Bundestag election, but it still made headlines," *First Draft News*, www.firstdraftnews.org/latest/7-types-german-election (accessed 12.12. 2022).

- spreading one's own ideology and discrediting the adversary's ideology;
- inspiring chaos, divisions, and conflicts;
- destabilisation of the society and the state;
- undermining the integrity of government, constitutional principles, and political (decision-making) processes.

Attention should be paid to the disturbing tendency in the era of "post-truth" in which the credibility of scientific research and the opinion of experts or authorities in a given field are questioned by bloggers, vloggers, celebrities, and self-proclaimed pseudo-authorities who, despite the lack of the necessary knowledge, competences, and qualifications, enjoy popularity in social media. With thousands of followers on Facebook, Instagram, YouTube, or Twitter, they are able to have a much greater impact on society than reliable and credible institutions. Targeting the impact of disinformation on these groups will be most effective in the case of ideological subversion directed against society. Its aim is to destroy the foundations of society, such as trust in the government and state institutions, media, and the education system.[6] Due to these conditions, in the 21st century, disinformation may be perceived as a "weapon of mass destruction".

This is evidenced by the fact that in 2017, Collins Dictionary recognised the term "fake news" as the word of the year.[7] Fake news is false information (often of a sensational nature) published in media with the intention of misleading the recipient, in order to achieve financial, political or prestigious benefits.[8] The researchers of the Reuters Institute for the Study of Journalism distinguish

[6] For more on ideological subversion, see: T.D. Schuman (J. Bezmienov), "Love Letter to America," NATA, Los Angeles 1984.

[7] "'Fakenews' is Collins Dictionary's word of the year 2017," www.apnews.com/article/47466c5e260149b1a23641b9e319fda6 (accessed 14.12.2022).

[8] B. McNair, *Fake News: False-hood, Fabrication and Fantasy in Journalism (Disruptions)*, Routledge, London, New York 2017.

a number of categories of information that can be classified as "fake news":

1) consciously distorted in order to achieve a specific result;
2) invented from scratch to achieve a political or business (financial) goal;
3) resulting from a low level of journalistic professionalism, poor technique, factual errors, messages with misleading headlines, with titles that are clickbait, i.e., announcements with sensational, intriguing content, only partially related to the actual content of the information, which is attempting to achieve clicking on the link;
4) situations when the term "fake news" is misused (e.g., by politicians) to discredit the source or the information itself in order to achieve political goals;
5) information that looks like reliable journalistic material, but is in fact advertising material;
6) information invented from scratch, the purpose of which is to make the audience laugh (satire).[9]

A separate category of disinformation or "fake news", but related to this phenomenon, is propaganda, defined as a one-way media message designed to manipulate public opinion. In terms of the degree of confidentiality of the conducted activities, it is divided into:

– **white—open (public)** provision of information that is to shape a positive image of a given entity (e.g., state, political party, company, etc.). It is based on real information that is selectively used. Any unfavourable, inconvenient or compromising facts are omitted in the message;

[9] N. Newman, R. Fletcher, A. Schulz, S.Andı, R.K. Nielsen, "Reuters Institute Digital News Report 2020," Reuters Institute for the Study of Journalism, www.reutersinstitute.politics.ox.ac.uk/sites/default/files/2020-06/DNR_2020_FINAL.pdf (accessed 14.12.2022).

- **grey—covert (concealed source)** transmission of specially prepared information by intermediary institutions, which, to a greater or lesser extent, officially or semi-officially, are related to the institutions of the state conducting propaganda activities;
- **black—covert** transmission of manipulated, falsified (partially or fully) information with the use of intermediary institutions, for which it is difficult to prove affiliation with the institutions of the state conducting the propaganda activities.

In addition to disinformation, "fake news", and propaganda, there are a number of other categories related to information warfare, such as Public Affairs, Public Diplomacy, strategic communication (StratCom), information operations (InfoOps), and psychological operations (PsyOps). The above concepts may be defined differently depending on the strategic culture of a state or state entity. The following set of definitions is based on the terminology used by NATO.[10]

Public Affairs

- **civilian**—timely, accurate, active, and reactive involvement of NATO's civilian sector in reporting through media about Alliance policy and the activities and operations resulting from it;
- **military**—a function related to the responsibility for promoting the military objectives of activities undertaken by NATO among the objects. They are intended to raise the level of awareness and increase understanding of the military aspects of the functioning of the Alliance.

[10] See: "NATO Military Policy on Strategic Communications," 2017, www.stratcom.nuou.org.ua/wp-content/uploads/2020/01/NATO-MILITARY-POLICY-ON-STRATEGIC-COMMUNICATIONS.pdf (accessed 15.12.2022).

This activity includes planning and implementation of assumptions adopted for proper relations with the media, internal communication, and relations with the community (communities).

Public Diplomacy—NATO civil communication projects, complemented by supporting activities and tools that promote awareness and build understanding and support for the policies adopted by NATO, as well as for the short-, medium-, and long-term activities and operations conducted by the Alliance.

Strategic Communication *(StratCom)*—the coordinated and tailored application of NATO's communications and communications capabilities—Public Diplomacy, Civilian and Military Public Affairs activities, Information Operations, and Psychological Operations—in support of Allied policies, activities, and operations to achieve NATO goals.

Information Operations (*InfoOps*)—a functional element, the main task of which is to advise and coordinate activities carried out in the information sphere, in order to achieve the desired results in terms of the will to act, understanding, and capabilities of the opponent, potential enemy, and other objects of influence, approved by the North Atlantic Council as part of supporting operations, and tasks and goals set by the Alliance.

Psychological Operations (*PsyOps*)—planned psychological activities using communication methods and other means aimed at approved audiences to shape the perceptions, attitudes, and behaviours that determine the achievement of political and military goals.

The above definitions largely reflect the way of thinking about the elements of information warfare in Western countries. However, they are not the same as their interpretation and practical application by entities with an undemocratic system of

government. Russian information warfare theorists distinguish between its two components: information-technical and information-psychological. The first component is understood as an integrated operation, blocking the entire ICT infrastructure of a hostile state: communication channels, radio-electronic means and the command-and-control system (C2) of its armed forces.[11] In turn, information and psychological operations are understood as a complex set of activities including support, counteraction, and information defence, carried out according to a uniform concept and plan, in order to gain and maintain an information advantage over the enemy during military operations. The purpose of conducting information and psychological operations is to disrupt the functioning of the enemy's information infrastructure and, as a consequence, to block the functioning of the state structure. The condition for the successful outcome of the operation is continuous pressure on the opponent and the maintenance of psychological initiative, implemented as part of informational and propaganda support for the military operation. It should be emphasised that Russian theorists do not distinguish between the military and non-military, technological (cyberspace), and social (information space) order, or the time of peace and war.[12]

The Russians (as opposed to the West) do not treat cyberspace as a separate strategic theatre of military operations (next to air, sea, land, or outer space). Instead of the word "cyberspace" they use the term "information space". For Russia, its cyber abilities are

[11] T.L. Thomas, "Russian Information Warfare Theory: The Consequences of August 2008," [in:] S.J. Blank, R. Weitz, *The Russian Military Today and Tomorrow. Essays in Memory of Mary Fisgerald*, Strategic Studies Institute, July 2010.

[12] J. Darczewska, "The anatomy of Russian information warfare. The Crimean operation, a case study," *Point of View*, no 42, www.osw.waw.pl/en/publikacje/point-view/2014-05-22/anatomy-russian-information-warfare-crimean-operation-a-case-study (accessed 12.12.2022).

a new tool for activities in the framework of information warfare (intelligence, counterintelligence, disinformation, propaganda), electronic warfare, disrupting communication and navigation, exerting psychological pressure, and destroying the enemy's IT resources.

Militarisation of Information in Russian Strategic Culture

Disinformation has almost always been a key element of Russia's imperial strategy. In tsarist times, Ochrana, the secret police whose main goal was to eliminate the political opposition, subversive groups, anarchism, and terrorism, was responsible for conducting information and psychological operations. The methods of disinformation were developed to perfection in the times of Soviet Russia, as exemplified by the operation "MOCR Trust" conducted in the 1920s by the GPU (State Political Authority). By creating a fictitious opposition organisation (*Monarchiczieskoje Objedinienije Central'noj Rossii*, MOCR), the Soviet secret services developed the possibility of eliminating "white emigration" and disinforming the foreign intelligence services supporting it (including Poland, Estonia, Latvia, Finland, and Great Britain).[13]

Since 1954, the First Main Directorate of the State Security Committee (KGB) was responsible for disinformation activities in the external dimension.[14] Operations of this type were carried out by Service A, which was responsible for the use of "active measures". This category included offensive disinformation,

[13] M. Świerczek, "The internal sources of the defeat of the Second Department of Polish General Staff in the confrontation with the State Political Directorate under the People's Commissariat of interior affairs of the Russian Soviet Federative Socialist Republic during the disinformation operation of the Soviet counterintelligence known as the 'MOCR-Trust affair'," *Przegląd Bezpieczeństwa Wewnętrznego*, 2018, no 10, pp. 352–378.

[14] W. Mitrochin, *KGB Lexicon: The Soviet Intelligence Officer's Handbook*, London 2002.

subversive, destabilising, and agent-based activities, resulting from Russia's foreign policy priorities, the purpose of which was to force the enemy to act in the direction desired by Moscow. The term combines various techniques used in operations to influence Russia's international environment and operations supporting the Kremlin's policy.[15] The instruments of "active measures" include: informational and psychological activities, disinformation, *maskirovka*, special propaganda, provocations, subversion, and sabotage. They make it possible to influence the political environment, public mood, and thus the internal security of other countries, in a way that enables Moscow to pursue its strategic interests.

During the Cold War, "active measures" were used primarily to "export" the communist revolution, promote Marxist-Leninist ideology, destabilise the political systems of adversaries, or discredit oppositionists. The most famous examples of disinformation campaigns carried out by the Soviets include:

- crediting the United States with the invention of the HIV/AIDS virus in the course of research on biological weapons;
- the Golitsyn-Nosenko affair, which paralysed the counterintelligence activities of the CIA and the FBI in the 1960s;
- an attempt to discredit U.S. President Ronald Reagan and connected with blocking the accession of Spain to NATO (1982).

The end of the bipolar rivalry and the collapse of the Soviet Union meant that the offensive information activity in the external dimension was severely limited. At that time, the main focus was on internal problems, especially the war in Chechnya. After the

[15] J. Darczewska, P. Żochowski, "Active measures. Russia's key export," *Point of View*, no 64, pp. 12–14, www.osw.waw.pl/en/publikacje/point-view/2017-05-30/active-measures-russias-key-export (accessed 12.12.2022).

former KGB officer Vladimir Putin came to power in 1999, the use of "active measures" regained momentum. This is evidenced by, among others the doctrine of "information security" developed since 2000, as well as its practical (offensive) application as a support instrument for armed operations in Georgia (2008) and Ukraine (since 2014).[16] Proof of Russia's attribution of the strategic role of "information militarisation" is the concept of "new generation wars", often also referred to as "hybrid war", "non-linear war" or the "Gerasimov doctrine".[17] Its main assumption is that due to the change in the contemporary conditions of warfare (there is no clear difference between peace and a state of war), Russia's strategic interests are pursued by means of non-military means and indirect methods, such as:

- disinformation of the political elite, military commanders, and the public by manipulating information, fabricating information, falsifying reality, and distracting attention from Russia's real actions and goals (*maskirovka*)[18];
- intoxication, control, and social manoeuvring, i.e., intentionally influencing society to achieve specific benefits;
- discreditation, corruption, and blackmail of political and military elites;

[16] See: J. Darczewska, "The anatomy of...," *op. cit.*; J. Darczewska, "The devil is in the details. Information warfare in the light of Russia's military doctrine," *Point of View*, no 50, www.osw.waw.pl/en/publikacje/point-view/2015-05-19/devil-details-information-warfare-light-russias-military-doctrine (accessed 12.12.2020); J. Darczewska, "Russia's armed forces on the information war front. Strategic documents," *Point of View*, no 57, www.osw.waw.pl/en/publikacje/osw-studies/2016-06-27/russias-armed-forces-information-war-front-strategic-documents (accessed 12.12.2022).

[17] *Russian New Generation Warfare Handbook*, U.S. Army Asymmetric Warfare Group, Fort Meade, December 2016.

[18] On differences between disinformation and *maskirovka*, see: W. Martynowicz, "O maskirowce w dezinformacji," www.fundacjapoint.pl/2016/09/o-maskirowce-w-dezinformacji (accessed 14.12.2022).

- fuelling internal and international tensions and disputes, supporting separatist tendencies and ethnic and religious conflicts;
- organising provocations and demonstrations (using the "protest potential");
- supporting opposition groups, resistance movements and extremist circles; creation of institutions, associations, foundations, organisations, and armed paramilitary groups controlled by special services;
- inspiring events that destabilise the internal situation; conducting subversive activities, including sabotage and terrorist activities, the purpose of which is to create a feeling of insecurity and danger in the society.[19]

Their common denominator is causing "controlled chaos".[20] This makes it possible to shape the socio-political situation outside Russia by inspiring crises, and then imposing a solution favourable to the Kremlin. The development of information technologies has made cyberspace one of the key tools for conducting this type of operation.[21] The virtual world is a key element of influencing public opinion, due to its availability, openness, lifting communication barriers, etc. The effect of this is a significant expansion of the scale of action by means of "active measures". In the information and psychological space, the essential role is played by propaganda outlets in the form of:

- traditional media and news agencies (e.g., RT, Sputnik);

[19] F. Bryjka, "Rosyjskie 'środki aktywne' w przestrzeni euroatlantyckiej," [in]: T. Grabińska, Z. Kuźniar (eds.), *Bezpieczeństwo personalne a bezpieczeństwo strukturalne VI*, AWL, Wrocław 2018, pp. 168-180.

[20] M. Galeotti, "Controlling Chaos: How Russia Manages Its Political War in Europe," European Council on Foreign Relations, 2017, no. 228.

[21] See : B. Lilly, J. Cheravitch, "The Past, Present, and Future of Russia's Cyber Strategy and Force," in: *2020 12th International Conference on Cyber Conflict (CyCon),* Estonia, 2020, pp. 129–155, DOI: 10.23919/CyCon49761.2020.9131723.

- unmasking portals (such as WikiLeaks[22], DCLeaks);
- "troll farms" (Internet Research Agency);
- "alternative media";
- think-tanks, including the Russian Institute for Strategic Research (RISI), Council for Foreign and defence Policy (SVOP), Russian Council for International Affairs (RIAC), Centre for Strategy and Technology Analysis (CAST), Centre for Energy and Security Research (CENESS), Strategic Research Centre (CSR), or websites belonging to pro-Russian organisations, associations, and foundations (e.g., Russkij Mir, Valdai Club).

The pro-Russian narrative is distributed in the information space by various kinds of intermediaries acting on behalf of the Kremlin, including journalists, bloggers, commentators, "experts", academics, and even local politicians spreading (knowingly or not) false information compiled by Russian disinformation strategists. We can classify them into several categories: "agents of influence", "useful idiots", "trolls". A separate (non-human) category is "bots", which are computer programmes or algorithms that automatically create and duplicate false information, posts, comments, etc.[23]

[22] For more about WikiLeaks, see: F. Bryjka, "Whistleblowing jako zagrożenie dla bezpieczeństwa informacyjnego państwa. Kazus WikiLeaks i Edwarda Snowdena," [in:] T. Grabińska, H. Spustek, *Bezpieczeństwo personalne a bezpieczeństwo strukturalne II. Terroryzm i inne zagrożenia*, WSO WL, Wrocław 2014, pp. 95–119.

[23] According to research by the NATO Centre of Excellence for Strategic Communications in Riga, 70% of tweets written in Russian and 28% in English, negatively regarding the presence of Alliance forces on the Eastern Flank were created from "bot" (robot) accounts. In total, they account for 84% of Russian-language and 46% of English-language content on this topic. This demonstrates the growing role of information technology used for automated social engineering, see: R. Fredheim (ed.), *Robotrolling*, NATO StratCom CoE, Riga 2017.

"Agents of influence" are persons recruited by foreign intelligence. They consciously act on its behalf by following instructions, for which they may accept specific benefits (e.g., financial). Their goal is to disseminate specially crafted information in order to change the perception of a specific issue (e.g. assessment of the political situation) by the recipient (society, political elite, etc.).

The term "useful idiots", in turn, is defined as people who perform a similar role, but in an unconscious way, i.e., their actions are not the result of an order by a foreign intelligence officer, but their personal views. The term "useful idiot" (Russian: *poleznyj idiot*) was used for the first time by Vladimir Lenin, who used to call Western journalists who wrote enthusiastically about the Bolshevik Revolution and concealed its failures.[24]

"Trolls", on the other hand, are usually people who work on commission and are paid for the work they do, i.e., generating posts and comments that show relevant people and events in a positive light. For this purpose, they use modified facts, recalled in an appropriate context. The most famous Russian "troll factory" is the Internet Research Agency (IRA), based in St. Petersburg and owned by Yevgeny Prigozhin, a close associate of Putin. In operation since 2013, this "troll factory" has a monthly budget of €1 million and employs around 80 people. Their task is, among others, to duplicate the Russian narrative, spread false information (fake news), provoke extreme social and political attitudes, and disinform foreign public opinion. Thus, this institution is one of the main tools used by Russia to conduct hybrid operations.[25]

[24] M. Charen, *Useful Idiots: How Liberals Got It Wrong in the Cold War and Still Blame America First*, Lahnam 2003, p. 10.

[25] A. Legucka, "Countering Russian Disinformation in the European Union," *Bulletin PISM*, no 111(1357), 6 August 2019, www.pism.pl/publications/Countering_Russian_Disinformation_in_the_European_Union (accessed 12.12.2022).

Conducting informational (info-ops) and psychological (psyops) activities is presently the domain of intelligence services. In the case of Russia, the dominant role is played by:

- The Federal Security Service (FSB)—responsible not only for counterintelligence or combating internal threats such as terrorism but also for so-called "tactical intelligence", conducted mainly in the neighbouring countries of Russia;
- The Foreign Intelligence Service (SVR)—carrying out intelligence activities outside the borders of Russia;
- The Main Intelligence Directorate of the General Staff (GRU) —Russian military intelligence.

The civilian special services (FSB and SVR), established after the collapse of the USSR, are the heirs of the KGB. Although in their nomenclature "active measures" has been replaced by the term "support measures" (Russian: *meropriyatiya sodeistviya*), the *modus operandi* has remained unchanged. Of course, their use has been expanded to include new technological capabilities (especially the internet and social media). The world learned about the SVR's activity in the field of information warfare thanks to Sergei Tretiak, a former Russian intelligence officer, deputy chief of a spy "station" in New York, who in 2000 defected to the Americans and began cooperating with the CIA.

We have much less knowledge about disinformation activities carried out by the Russian military intelligence (GRU). Based on the information available, it is possible to get the impression that disinformation was only the domain of "civilian" services. However, thanks to the publications of investigative journalist Michael Weiss, working for the non-governmental organisation Free Russia Foundation, we know that this was not the case. In his report, *Aquarium leaks. Inside the GRU's psychological warfare*

program, he reveals the background of the GRU's psychological operations during and after the Cold War.[26]

In the report, we meet Col. Alexandr Victorovich Goliyev, a propaganda and psychological warfare specialist who entered service in the early 1980s. His main task was to fight anti-communist movements in the Warsaw Pact countries. While serving in the Special Propaganda Directorate of the Main Political Directorate of the Soviet Army and the Russian Navy (GLAVPUR), Col. Goliyev was sent to Poland in the 1980s, where he was involved in combating the Solidarity movement. Then (in the early 1990s) he was sent to Lithuania where, after the storming of the Vilnius TV centre, he founded the newspaper *Soviet Lithuania*, loyal to the regime and printed in Minsk. His last mission abroad was the German Democratic Republic (GDR) where he oversaw the withdrawal of Soviet troops.

From the memoirs of Col. Goliyev, we learn that in the 1970s the Soviets established propaganda training centres at the Military Institute of Foreign Languages and at the Faculty of Journalism at Moscow State University (MGU). Specialists in propaganda and psychological warfare were trained there, constituting a reserve of personnel in the event of war mobilisation. One of the tasks of the graduates of the special propaganda courses was the indoctrination of Soviet soldiers. At the end of the 1980s, there were 20,000 political departments in military structures supported by 80,000 employees.

During the First Chechen War (1994-1996), Goliyev was assigned to the newly created secret GRU unit no. 54777, specialised in information and psychological activities. The colonel took part, among others, in the production of the anti-Chechen films "Dogs

[26] See: M. Weiss, "Aquarium leaks. Inside the GRU's psychological warfare program," *4FreeRussia*, www.4freerussia.org/aquarium-leaks-inside-the-gru-s-psychological-warfare-program (accessed 15.12.2022).

of War" and "Werewolves". Interestingly, in 2018, Putin brought GLAVPUR back to life, most likely to maintain the morale of the soldiers and their loyalty to the Kremlin's policy. At the same time, unit no. 54777 functions within the structures of the GRU and conducts information and psychological activities both where there are Russian military operations (especially Ukraine and Syria) and against the countries of the transatlantic community (NATO and the EU).

Critical Thinking, Fact-Checking, and Open-Source Interview

The ability to separate fact from opinion, truth from lie, or to recognise manipulated or completely false content, is a particularly important skill in times of "post-truth". These competences can be acquired, developed, and improved thanks to critical thinking, which should not be equated with criticism in the common sense. Its aim is not to spot errors (criticism) maliciously, but to skilfully analyse information, assess the accuracy of argumentation or the logic of argumentation. By tradition, critical thinking goes back to the ancient school of Greek philosophers. The term "critical" is derived from two Greek words: *kritikos* ("luminous judgment" or "understanding judgment") and *kriterion* ("standards", "criteria").[27] Richard Paul and Linda Elder believe that "critical thinking is thinking directly aimed at reaching a well-founded opinion, using adequate standards of judgment to determine the true meaning

[27] P. Henzler, "Jak świadomie korzystać z informacji," Fundacja Rozwoju Społeczeństwa Informacyjnego, Warszawa 2018, pp. 7, 8, www.goethe.de/resources/files/pdf168/poradnik_kliknij_sprawdz_zrozum.pdf (accessed 12.12.2022).

or value of something."[28] Edward Glaser, in turn, distinguishes its three components:

1) an attitude expressed in the readiness to consider in a thoughtful way the problems and objects that are within the scope of experience;
2) competence in logical methods of reasoning and inquiry;
3) relative skill in using these methods.[29]

Critical thinking is therefore constructive, useful, and necessary thinking. It is a conscious, thoughtful, and planned process. In practice, critical thinking is a set of skills including:

– collecting the necessary information;
– analysing them;
– determining their significance (materiality) and credibility;
– putting them into practice (processing and drawing conclusions).

Thanks to the development of critical thinking skills, we understand the reality around us better, we deal with problems better, we see cause-and-effect relationships occurring in various phenomena and processes more easily, we are able to assess the importance and usefulness of specific information, and we use better arguments to defend our position.[30]

Fact-checking is a method of confirming or disproving statements that appear in media or on the internet in order to correct errors and allow the text to be distributed or rejected if questionable content cannot be verified.[31] This is done by fact-

[28] R. Paul, L. Elder, *Critical Thinking: Tools for Taking Charge of Your Learning and Your Life*, Pearson Education Limited 2014.

[29] "Czym jest krytyczne myślenie", www.criticalthinking.pl/czym-jest-krytyczne-myslenie (accessed 12.12.2022).

[30] P. Henzler, "Jak świadomie korzystać...," *op. cit*.

[31] M. Wójcik (ed.), *Mały leksykon post-prawdy*, Fundacja Wolność i Demokracja, p. 27, www.wid.org.pl/wp-content/uploads/E_wydanie-Ma%C5%82y-Leksykon-Postprawdy.pdf (accessed 12.12.2022).

checking organisations, such as FactCheck.org, PolitiFact, The Washington Post Fact-Checker, Full Fact, Demagog, and AllSides.

Fact-checking organisations verify information using unified standards and similar work patterns. The overriding principle is the issue of operational transparency, consisting of the full availability of recipients to the methodology and information on the activities of a given entity. Organisations thus undertake to follow the standards and procedures common to fact-checkers. The basic principles are contained in the International Fact-Checking Network (IFCN) Code of fact-checking organisations. Their foundation consists of three elements:

1) impartiality;
2) transparency of action;
3) intention to improve the quality of public debate.[32]

While competences and skills in the field of critical thinking and fact-checking allow, above all, to identify disinformation, a thorough analysis of the content of the message, its source, methods and scope of distribution, as well as defining the objectives of a given operation, requires efficient use of tools included in the practice of what is called white intelligence (Open Source Intelligence, OSINT).

OSINT is one of the methods of the work of intelligence services, which, in addition to obtaining information in an operational manner, as part of Human Intelligence (HUMINT), also uses technical Measurement and Signatures Intelligence (MASINT), signals intelligence (SIGINT), Imagery Intelligence (IMINT), or Communication Intelligence (COMINT). It is estimated that during the Cold War, only 20% of intelligence came from classified sources, while as much as 80% was obtained through the analysis

[32] "International Fact-Checking Network fact-checkers' code of principles," Poynter, www.poynter.org/ifcn-fact-checkers-code-of-principles (accessed 12.12.2022).

of open-source content.[33] Jarosław Stróżyk, former deputy director of the Intelligence Board at NATO Headquarters, while recalling historical research, pointed out that intelligence agencies often overestimate the importance of information obtained through operations, ignoring the conclusions that can be drawn from a careful analysis of open sources.[34]

These sources include information from media, publicly available documents, reports, analyses and other publications, as well as all kinds of information available online (on websites, forums and social media). The NATO Open Source Intelligence Handbook distinguishes the following categories of information from open sources:

1) Open Source Data, (OSD)—i.e., raw data;
2) Open Source Information, (OSIF)—information consisting of data usually aggregated as a result of an editing, filtering, checking, and presentation process;
3) Open Source Intelligence (OSINT)—information processed, analysed, and disseminated to recipients in order to answer a specific question;
4) Validated OSINT—Information that can be assigned a high degree of certainty. It can be produced by an intelligence analyst who also has access to information obtained with operational methods.[35]

All of the above elements (OSINT, HUMINT, MASINT, SIGINT, IMINT, COMINT) are used within the intelligence (analytical)

[33] H.J. Williams, I. Blum, "Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise," RAND Corporation, Santa Monica 2018, p. 5, www.rand.org/pubs/research_reports/RR1964.html (accessed 15.12.2022).

[34] J. Stróżyk, *Wybrane problemy międzynarodowej współpracy wywiadowcze. Czy NATO ma wywiad?,* Wydawnictwo Uniwersytetu Warszawskiego, Warszawa 2020, pp. 18, 19.

[35] "NATO Open Source ...," *op. cit.*, pp. 2, 3.

cycle, defined as a repetitive process, consisting of (depending on the organisational culture) of 4-6 elements (see table below).

Examples of Intelligence Cycle Models

	Classic model	CIA	NATO
1)	Identification of needs	Planning and management	Management
2)	Planning and management	Information acquisition	Information acquisition
3)	Gathering	Information processing	Information processing
4)	Processing	Analysis and development	Information dissemination
5)	Analysis	Distribution	
6)	Dissemination		

Own work based on R.M. Clarke, *Intelligence Analysis: a Target-Centric Approach*, Waszyngton 2010, pp. 17-27; R. Johnston, *Analytic Culture in the U.S. Intelligence Community. An Ethographic Study*, CIA Center for the Study of Intelligence, Washington 2005, p. 45 and following.

In simple terms, the process of identifying and analysing disinformation may consist of the following steps:

1) evaluation of the information source;
2) evaluation of information;
3) the circumstances of obtaining (making public) information;
4) possible purpose of the disinformation;
5) the consequences of disinformation;
6) assessing our vulnerability to disinformation.

Among the numerous models, methods, and tools for verifying the accuracy of information, one of the most popular and effective

is CRAAP analysis, developed by Meriam Library at California State University in Chico.[36] This model consists of 5 elements:

1) Currency (up-to-date information)
   – when was the information published?
   – has the information (if it is not new) been updated?
   – does the matter for which you are reading this information require up-to-date data or can you rely on older materials?
   – do the links in the information (if any) work?
2) Relevance (the relevance of the information to your needs)
   – does the information relate to the topic you are dealing with at all, or does it answer a question that is important to you?
   – for whom was the information prepared? For some target group?
   – is the information adequate to your needs? Is it too vague or too advanced, detailed?
   – did you check other sources before making the decision to use this information?
   – will you feel okay and comfortable stating publicly that you are using this source of information?
3) Authority (origin of information)
   – who is the author, publisher, source, or sponsor of the information?
   – what are the credentials of the author of the information? With which organisation, institution or other entity is it related?
   – is the author qualified to write on this topic?
   – whether contact details, for example, the publisher name and/or address can be found with the information, e-mail, etc?

[36] See: "Evaluating Information—Applying the CRAAP Test," Meriam Library, California State University, Chico, https://library.csuchico.edu/sites/default/files/craap-test.pdf (accessed 15.12.2022).

– does the address of the website where the information appeared say something about the author or the sender (for example, the URL ends with .com, .edu, .gov)?

4) Accuracy (credibility, truthfulness, and correctness of information)

– where does the information come from?
– is the information provided supported by evidence?
– has the information been reviewed or cited? (concerns mainly scientific works)
– are you able to confirm at least some of the given messages in another source or using your own knowledge?
– does the language or pronunciation of all information indicate impartiality and is not emotional?
– does the information contain spelling, grammatical or stylistic errors?

5) Purpose (the purpose of the information; the reason it was created)

– what was the information created for? Is it supposed to educate, inform, entertain, persuade?
– has the author or the person financing the information clearly defined its purpose?
– is the information quoting or describing facts, presenting an opinion, or is it propaganda?
– does the point of view presented in the information appear objective?
– do you see any elements in the information that indicate partiality and taking a specific position on issues related to politics, religion, beliefs or, for example, presenting the perspective of only one institution or person?

The answers to the above questions will allow us to determine not only the truthfulness of the information itself but also the reliability of its preparation and the credibility of the source. If

false or manipulated information is detected, we can use several tools to further verify and analyse it by using:

- internet search engines (including Google, DuckDuckGo, Bing, Entireweb;
- tools for collecting statistical data, tracking trends, and distributing information on the internet (including Google Trends);
- social media analysis tools (including Netlytic, Socialbearing, Follow The Hashtag, TweetDeck);
- tools for advanced image search and analysis (including Google Images, TinEye, FotoForensics);
- tools for analysing video materials (including YouTube Data Viewer);
- searching for information about changed or deleted websites (including The Internet Archive Wayback Machine);
- a tool for obtaining and verifying information about people and other entities (including Email Checker, PIPL, Facebook Graph Search).

The results of the investigation should be processed and presented in the form of an analysis or commentary and then published on the website of centres dealing with detecting, analysis, and combating disinformation. You do not have to be an expert in a think-tank to engage in the fight against the manipulation of the information space on an individual level. With basic knowledge and skills, each of us can independently unmask examples of fake news using free online platforms or social media.

Bibliography:

Basaj K., *Dezinformacja, czyli sztuka manipulacji*, www.rcb.gov.pl/dezinformacja-czyli-sztuka-manipulacji (accessed 4.12.2020).

Brodnig I., *Misinformation didn't change the outcome of the Bundestag election, but it still made headlines*, www.firstdraftnews.org/latest/7-types-german-election (accessed 12.12.2020).
Bryjka F., "Rosyjskie "środki aktywne" w przestrzeni euroatlantyckiej," [in:] T. Grabińska, Z. Kuźniar (eds.), *Bezpieczeństwo personalne a bezpieczeństwo strukturalne VI*, AWL, Wrocław 2018, p. 168-180.
Bryjka F., *Whistleblowing jako zagrożenie dla bezpieczeństwa informacyjnego państwa. Kazus WikiLeaks i Edwarda Snowdena*, [in]: T. Grabińska, H. Spustek, "Bezpieczeństwo personalne a bezpieczeństwo strukturalne II. Terroryzm i inne zagrożenia", WSO WL, Wrocław 2014, p. 95-119.
Charen M., *Useful Idiots: How Liberals Got It Wrong in the Cold War and Still Blame America First*, Lahnam 2003.
Clarke R.M., *Intelligence Analysis: a Target-Centric Approach*, SAGE Publishing/CQ Press, London-New Delhi-Singapore 2020.
Czym jest krytyczne myślenie, www.criticalthinking.pl/czym-jest-krytyczne-myslenie (accessed 12.12.2022).
Darczewska J., "Russia's armed forces on the information war front. Strategic documents," *Point of View*, no 57, www.osw.waw.pl/en/publikacje/osw-studies/2016-06-27/russias-armed-forces-information-war-front-strategic-documents (accessed 12.12.2022)
Darczewska J., "The anatomy of Russian information warfare. The Crimean operation, a case study," *Point of View*, no 42, https://www.osw.waw.pl/en/publikacje/point-view/2014-05-22/anatomy-russian-information-warfare-crimean-operation-a-case-study (accessed 12.12.2022).
Darczewska J., "The devil is in the details. Information warfare in the light of Russia's military doctrine," *Point of View*, no 50, Warsaw 2015, www.osw.waw.pl/

en/publikacje/point-view/2015-05-19/devil-details-information-warfare-light-russias-military-doctrine (accessed 12.12.2022).
Darczewska J., Żochowski P., "Active measures. Russia's key export," *Point of View*, no 64), pp. 12–14, https://www.osw.waw.pl/en/publikacje/point-view/2017-05-30/active-measures-russias-key-export (accessed 12.12.2022).
Evaluating Information—Applying the CRAAP Test, Meriam Library, California State University, Chico, www.library.csuchico.edu/sites/default/files/craap-test.pdf (accessed 15.12.2022).
'Fake news' is Collins Dictionary's word of the year 2017, www.apnews.com/article/47466c5e260149b1a23641b9e319fda6 (accessed 14.12.2022).
Fredheim R. (ed.), *Robotrolling*, NATO StratCom CoE, Ryga 2017.
Galeotti M., *Controlling Chaos: How Russia Manages Its Political War in Europe*, European Council on Foreign Relations, 2017, no. 228.
Henzler P., *Jak świadomie korzystać z informacji*, Fundacja Rozwoju Społeczeństwa Informacyjnego, Warszawa 2018, p. 7-8, www.goethe.de/resources/files/pdf168/poradnik_kliknij_sprawdz_zrozum.pdf (accessed 12.12.2022).
International Fact-Checking Network fact-checkers' code of principles, [online] https://www.poynter.org/ifcn-fact-checkers-code-of-principles (accessed 12.12.2022).
Johnston R., *Analytic Culture in the U.S. Intelligence Community. An Ethographic Study*, Washington D.C. 2005.
Kupiecki R., "Mit założycielski" polityki zagranicznej Rosji, *Sprawy Międzynarodowe*, 2019, no 4, pp. 77–105, DOI: 0.35757/SM.2019.72.4.03, www.researchgate.net/publication/344069207_ROBERT_KUPIECKI_Mit_zalozycielski_polityki_zagranicznej_Rosji (accessed 18.12.2022).

Kupiecki R., Menkiszak M. (eds.), *Documents Talk. NATO-Russia Relations after the Cold War*, Polski Instytut Spraw Międzynarodowych, Warszawa 2020.
Legucka A., "Countering Russian Disinformation in the European Union," *Bulletin PISM*, no 111(1357), 6 August 2019, www.pism.pl/publications/Countering_Russian_Disinformation_in_the_European_Union (accessed 12.12.2022).
McNair B., *Fake News: False-hood, Fabrication and Fantasy in Journalism (Disruptions)*, Routledge, London-New York 2017.
Mitrochin W., *KGB Lexicon: The Soviet Intelligence Officer's Handbook*, London 2002.
NATO Military Policy on Strategic Communications, 2017, www.stratcom.nuou.org.ua/wp-content/uploads/2020/01/NATO-MILITARY-POLICY-ON-STRATEGIC-COMMUNICATIONS.pdf (accessed 15.12.2022).
NATO Open Source Intelligence Handbook, www.academia.edu/4037348/NATO_Open_Source_Intelligence_Handbook (accessed 15.12.2022).
Newman N., Fletcher R., Schulz A., Andı S., Nielsen R.K., *Reuters Institute Digital News Report 2020*, Reuters Institute for the Study of Journalism www.reutersinstitute.politics.ox.ac.uk/sites/default/files/2020-06/DNR_2020_FINAL.pdf (accessed 14.12.2022).
Paul R., Elder L., *Critical Thinking: Tools for Taking Charge of Your Learning and Your Life*, Pearson Education Limited 2014.
RESIST Disinformation: a toolkit, UK Government Communication Service, www.fundacioncarolina.es/wp-content/uploads/2020/11/Toolkit-UK.pdf (accessed 12.12.2022).
Russian New Generation Warfare Handbook, U.S. Army Asymmetric Warfare Group, Fort Meade, December 2016
Schuman T.D. (Bezmienov J.), *Love Letter to America*, NATA, Los Angeles 1984.
Schwartau W., *Information Warfare*, Thunder's Mouth Press, New York 1996.

Stróżyk J., *Wybrane problemy międzynarodowej współpracy wywiadowcze. Czy NATO ma wywiad?*, Wydawnictwo Uniwersytetu Warszawskiego, Warszawa 2020.
Świerczek M., *The internal sources of the defeat of the Second Department of Polish General Staff in the confrontation with the State Political Directorate under the People's Commissariat of interior affairs of the Russian Soviet Federative Socialist Republic during the disinformation operation of the Soviet counterintelligence known as the "MOCR-Trust affair"*, *Przegląd Bezpieczeństwa Wewnętrznego*, 2018, no. 10, pp. 352–378.
Thomas T.L., *Russian Information Warfare Theory: The Consequences of August 2008*, [w]: Blank S.J., Weitz R., "The Russian Military Today and Tomorrow. Essays in Memory of Mary Fisgerald", Strategic Studies Institute, July 2010.
Volkoff V., *La désinformation : Arme de guerre*, L'Age d'Homme, Lozanna 1999.
Weiss M., *Aquarium leaks. Inside the GRU's psychological warfare program, 4FreeRussia*, www.4freerussia.org/aquarium-leaks-inside-the-gru-s-psychological-warfare-program (accessed 15.12.2022).
Williams H.J., Blum I., *Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise*, RAND Corporation, Santa Monica 2018, www.rand.org/pubs/research_reports/RR1964.html (accessed 15.12.2022).
Wojnowski M., *Koncepcja "wojny nowej generacji" w ujęciu strategów Sztabu Generalnego Sił Zbrojnych Federacji Rosyjskiej*, "Przegląd Bezpieczeństwa Wewnętrznego", 2005, no. 13, p. 13-39.
Wójcik M. (ed.), *Mały leksykon postprawdy*, Fundacja Wolność i Demokracja, www.wid.org.pl/wp-content/uploads/E_wydanie-Ma%C5%82y-Leksykon-Postprawdy.pdf (accessed 12.12.2022).

JUSTYNA PODEMSKA

PIOTR PODEMSKI
Faculty of Applied Linguistics, University of Warsaw
ORCID: 0000-0002-1525-7867

Protect Yourself Against Disinformation

The following is a presentation of lesson plans for students on disinformation and information warfare.

LESSON 1
LOOK! DISINFORMATION: WHAT IS THAT?

Lesson Objectives

1. To raise students' awareness of DISINFORMATION as a phenomenon they encounter in their everyday lives.
2. To promote a critical attitude towards the content conveyed, i.e., understanding that not everything that is written or said is necessarily true.
3. To familiarise students with definitions and types of DISINFORMATION.

Lesson Outline

1. WARM-UP PHASE (PRACTICAL)

Warm-up activities are meant to inspire students' interest by pushing them out of their everyday comfort zone, to make them aware of a problem that they may not have been aware of before.

With this intention in mind, and without explaining the purpose or topic of the lesson to the students, we invite them to watch two videos, in the following order:

1. "Battle of Warsaw 1920. Medal for every Pole" (Polish: "Bitwa Warszawska 1920. Medal dla każdego Polaka").
www.youtube.com/watch?v=yh_YhhDRPzQ (duration: less than one minute)

2. "Urgent news November, 5 7528 in Radio Sławenia" (Polish: "Aktualności Pilne 05.11.7528 r. w Radio Sławenia"
www.youtube.com/watch?v=RO_XjTQBaso&feature=youtu.be

Warning! The entire length of the second video lasts approximately 45 minutes and includes language inappropriate for secondary school students. We leave it to the discretion of the teachers whether to allow students to view the initial fragment (~5 minutes) of the recording in the original version, or to use the shortened version prepared by us instead (~5 minutes long, censored).

We expect the footage will stimulate students to various comments, both hilarious and serious, which will allow them to smoothly move on to our planned classroom discussion.

1. "Battle of Warsaw 1920. Medal for every Pole"

Suggested questions for students (asked one by one as the discussion proceeds):

- Would you like to receive such a medal?
- Is this a fair offer? Who pays for it?
- What measures did the advertisers use to attract customers?

– What is the National Treasury (Skarbnica Narodowa)?
– Does the material contain lies?

The aim of this discussion will be to make students aware of the following facts:

– The Medal, in the material referred to as a "free commemorative medal" and "Free. A medal for every Pole", is actually a commercial offer.
– In the material, next to the words "Price PLN 0", an attentive observer may find the information "+ PLN 9.95 - packing and shipping" in small print. Therefore, ordering a medal entails the payment of PLN 9.95, thus it is not entirely free.
– In order to gain customers, the authors of the material (advertisement) refer to patriotic feelings. Solemn language ("we Poles defended independence", "a great victory", "the brilliant strategy of Marshal Józef Piłsudski", "the courage of the whole nation") serves to inspire positive emotions and to hinder critical thinking. The general public normally does not expect noble slogans related to national history to be used to persuade one to spend money on a "free medal".
– The National Treasury is not—as many will probably think—an institution of the Polish state, but a private company with international connections (www.skarbnicanarodowa.pl/o-firmie).

The material does not contain lies: it is a presentation of a private company's commercial offer, designed to convince as many people as possible to order a free medal. However, this implies the obligation to cover the costs of packaging and shipping, which will constitute the company's profit.

2. "Urgent news 05/11/7528 in Radio Sławenia"

Suggested questions for students (asked one by one as the discussion proceeds):

- If you had watched this video from 5 November 2020, would you have believed that "next Thursday" Russian troops would enter Poland?
- What facts and sources does the author of the broadcast refer to?
- What elements reduce the message's credibility?
- What is Radio Sławenia? Who is the host?
- With what purpose in mind was this recording made?
- In your opinion, was the broadcast author discredited in the eyes of the audience since there was no Russian invasion of Poland in November 2020?

The aim of this discussion will be to make students aware of the following facts:

1. A Russian military invasion of Poland on 12 November 2020 ("next Thursday"), as predicted in the broadcast, did not materialise
2. The broadcast author does not cite any facts directly confirming his predictions, while he only makes reference to various current events in Poland and around the world in a general and imprecise way ("look, there were siren exercises", "this Maidan in Ukraine", "Trump is held right there, there will be a fight for every vote until January", "Czechia, Slovakia closed"). At times, he offers opinions that are remotely related to some aspects of our reality but are not confirmed by any facts ("lands to which Germany claims rights"; "there are plans to divide Belarus"; "we have a civil war in the United States"; "French cities are abandoned"; "Fighting in Spain"; "fighting terrorists in Austria").
3. The author does not refer to any specific, verifiable sources, informing only in general terms that he draws his information "from Polish sources", "from Western sources", "from certain other sources", from "people who live on the coast", from what "all economists say".

4. The speaker's credibility is impaired by linguistic mistakes, such as "a continent of a thousand soldiers" (instead of "contingent"); "Anarchies are happening" (he means "riots"); "That everything is Ofair" (instead of "OK").
5. If the audience believes in the author's message, they will probably feel threatened ("war has just been declared on Russia", "as long as the internet is still working", "stock up", "something for your own defence will also prove useful"). It is debatable whether or not this is the author's genuine intention.
6. As one can read in the video description at youtube.com, Radio Sławenia is a private website and bookstore (with a rather strange and only partially visible www address) and a YouTube channel, run by "Edward Sławianin Leh". The recording description says: "We are the first Radio for Slavs, independent of corporations and business, and above all Censorship-free!!!, so Poles and all Slavs!!! Here you will hear what other stations are even afraid to think!! Fame and Glory!". Therefore, one can presume there are pro-Russian or directly Russian inspirations behind the broadcast.
   www.youtube.com/watch?v=RO_XjTQBaso&feature=youtu.be
7. In the description, the author also gives a bank account for payments for the maintenance of the radio outlet under the name of Edward Świętosławski. On the web one can find a Polish presidential election campaign flyer of a candidate with the same name, promoting slogans such as "Leaving the European Union" and "unity with the Slavic nations".
   www.1polska.pl/img/2020/EDWARD_SWIETOSLAWSKI_ULOTKA.pdf
8. Therefore, it can be assumed that the author's aim is to obtain financial benefits (payments to the account from

listeners) and to influence Polish public opinion in an anti-EU and pro-Russian direction.

9. It can be assumed that, in the eyes of many of his listeners, the author was not discredited as a result of the Russian invasion predicted for November failing to materialise, since the predicted date was based on "the feelings of people from the coast", so it is easy to explain that—for any reason and based on any unspecified sources—the timing of the Russian invasion of Poland was postponed.

1. FOLLOW-UP PHASE (THEORETICAL)

Follow-up are activities aimed at building a solid, theoretically grounded knowledge based on the experiences gathered during the first part of the lesson. In this section, we will introduce students to the definitions of information warfare and disinformation as well as the types of the latter.

THE CONCEPTS OF "INFORMATION WAR" AND "DISINFORMATION"

We inform students—or remind them, if they knew about it before—that they are participating in a project entitled "Protect Yourself Against Disinformation", now specifically in a lesson entitled "Look! Disinformation: What is That?". The film materials, presented and discussed, were intended to illustrate this phenomenon.

We ask students to share their understanding of the concepts of INFORMATION WAR and DISINFORMATION (write them on the board or display them on the slide).

We expect that in the course of the discussion students will independently come to the conclusion that, generally speaking, INFORMATION WAR is a conflict (not necessarily between countries) in which information is a tool and a weapon.

We will devote more time to the definition of DISINFORMATION by dividing students into groups and assigning each of these one of the following definitions to be read and discussed:

Definition by Defence24.pl (a specialised national security website)

Disinformation—disseminating manipulated or false information in order to influence recipients and induce them to behave in a specific manner to the benefit of the disinformer.

www.defence24.pl/wojna-informacyjna-jako-effeczne-narzedzie-destabilalisacji-panstw-i-rzadow-raport

Polish government Centre for Security definition

Disinformation can be seen as an advanced form of communication, whose purpose is to evoke a view, decision, action or lack thereof in the recipient, in line with the premise of the centre that planned the process of misleading the recipient. In essence, it is an interference in the decision-making process of an object (i.e., recipient) or group of objects. This is also why disinformation is also information, not always false or manipulated

www.rcb.gov.pl/dezinformacja-czyli-sztuka-manipalisacji/

The European Commission definition

Disinformation—false or misleading information created, presented, and disseminated for financial gain or to knowingly mislead the public; distorts public debate, undermines citizens' trust in institutions and the media, and even destabilises democratic processes such as elections.

www.ec.europa.eu/commission/presscorner/detail/en/MEMO_18_6648

NATO definition

NATO views disinformation as the deliberate creation and dissemination of false and/or manipulated information with the intention of fraud and/or misleading. Disinformation deepens divisions among allied nations and undermines people's confidence in elected governments. NATO has faced these challenges since its inception.

www.nato.int/cps/en/natohq/177273.htm#case

Swedish government definition

Disinformation refers to false or manipulated information that is intentionally disseminated with the intent to mislead. It is the cornerstone of classical propaganda, but it also forms the basis of a more recent phenomenon—fake news. The deliberate use of false information to mislead is not new. However, digital platforms have fundamentally changed the nature of disinformation. Counterfeit content may appear in the form of manipulated texts, images, videos, or audio recordings. They can be used to validate untrue theories, spread confusion and discredit reliable information, organisations, or individuals.

www.msb.se/RibData/Filer/pdf/28698.pdf

After discussing individual definitions in groups, we can ask students to create a common, working list of the features of DISINFORMATION, which, once they have been determined by students in the course of their discussion, we write on the blackboard/slide/special poster.

FOUR TYPES OF DISINFORMATION

We present students—in the form of distributed printouts or a displayed slide—the definitions of the four types of DISINFORMATION proposed by the Swedish government, i.e.:

FABRICATION

Information without a factual basis, published in a form that causes the recipient to mistakenly believe that it is reliable. For example, a fake email from a politician, made available to the press, may undermine the politician's credibility.

MANIPULATION

Adding, hiding, or modifying the content of a text, photo, sound or video recording to change its pronunciation.

ABUSE

Using real content in relation to an unrelated matter to put a problem, event, or person in a false context. For example, in a false article, photos from an event unrelated to it are used to prove the truthfulness of the text.

SATIRE AND PARODY

Satire and parody are generally harmless forms of entertainment. However, humour can be used aggressively to spread false content or to criticise people, ideas, or opinions. Humour can also be a very effective tool to legitimise controversial opinions.

www.msb.se/RibData/Filer/pdf/28698.pdf

Finally, we invite students to talk about which of the four types of DISINFORMATION—according to the students—were embodied in the examples discussed in the first part of the lesson.

LESSON 2
CHECK! FACT-CHECKING: HOW DO YOU DO IT?

Lesson objectives

1. To theoretically ground students' intuitive ability to distinguish between fact and opinion.

2. To master the ability to distinguish reliable information from fake news.
3. To master the procedure of fact-checking with a specific example.

Lesson outline:

1. WARM-UP PHASE (THEORETICAL)

During our second lesson, the warm-up will be used to equip students with skills they will apply practically in the second part of the lesson.

SECONDARY RECAPITULATION
(revision of the message from the previous lesson)

We remind students that in the previous lesson we discussed the phenomenon of DISINFORMATION, as a vital element of INFORMATION WAR.

We ask students:

- if they have had any further reflections, questions or doubts since the previous lesson (if necessary, we briefly discuss them, making students aware their thoughts are respected and they are not being manipulated),
- what definition of DISINFORMATION they have developed for themselves and remembered from the previous lesson.

FACT OR OPINION—IT MAKES A HUGE DIFFERENCE!

As an element connecting the current lesson to the previous one, we state that DISINFORMATION may sometimes take the form of someone deliberately blurring the line between FACT and OPINION.

We write down on the board (or display on the slide) the terms FACT and OPINION.

We ask students to brainstorm the differences between them. We expect students will say intuitively, for example, that:

"Facts are what one knows, while opinions are what one feels."; "Facts are universal, while opinions may differ."; "Facts are true, and opinions needn't be true."

When students are finished sharing responses, we ask them to do an activity: verify whether the quoted sentences are FACT or OPINION.

We may choose from the three options below of how to carry out the exercise:

1. Distribute hand-outs with the following 10 sentences printed on them.
2. Display the following sentences (one by one or all at once) on a slide.
3. Invite students to an online quiz at kahoot.it

(Our publicly available quiz can be accessed at www.create.kahoot.it under the title "DISINFORMATION: FACT OR OPINION?")

EXERCISE MATERIAL:

1. There are too many immigrants in Italy.
2. Some people from Africa would like to live in Europe.
3. Doctors should earn more.
4. Ritual slaughter increases animal suffering.
5. You don't need television if you listen to the radio.
6. Fighting smog must be a government priority.
7. Most high school students finally obtain their diploma.
8. Blue dresses are the most beautiful.
9. Bosnians are the tallest men in the world.
10. Every war is evil.

We stop at each statement to discuss students' likely doubts as to whether it is an example of a FACT or an OPINION. In case of any ambiguities, we follow the criteria proposed by the BBC.

FACT	OPINION
WHAT I KNOW.	WHAT I FEEL
I CAN PROVE IT.	I CAN NEITHER PROVE NOR DENY IT.
YOU HAVE TO ACCEPT IT.	YOU CAN EITHER AGREE OR NOT.
FACTS MAY CHANGE OPINIONS.	OPINIONS CANNOT CHANGE FACTS.

Based on: www.bbc.co.uk/teach/skillswise/fact-or-opinion/z4r7cqt

DISINFORMATION might thus result from someone presenting their OPINIONS as FACTS.

RELIABLE INFORMATION OR FAKE NEWS?

We introduce students to the subject of FAKE NEWS, reminding them that in the course of Lesson 1, we found out that not all information we receive is true. In today's world, disinformation often takes the form of FAKE NEWS, i.e., false information produced by fabrication, manipulation, or abuse, usually with the use of modern technologies.

There is an easy procedure for verifying the reliability of information, i.e., determining whether it can be trusted or should be considered FAKE NEWS.

We divide students into two groups and assign each of these for analysis one of the English-language posters on the topic developed by:

1. the International Society for Technology in Education.
2. the International Federation of Library Associations and Institutions.

We encourage students to use the original, English-language sources available at the above-mentioned websites. Optionally, we may also hand out a translation of the content of both posters.

The students' task is to develop their own procedure (e.g., in 5 steps) of assessing whether a given piece of information should be considered reliable.

Possible answers :

INFORMATION IS RELIABLE IF:

1. It comes from a well-known and trusted source (e.g., a well-known newspaper, website).
2. The title is consistent with the content (not artificially flashy, catchy, groundless).
3. It provides the name of an author who is generally known as an expert in the field.
4. It cites specific and verifiable sources (information is derived from several sources).
5. It bears a specific date and is up-to-date (e.g., the situation may have changed since 1978).
6. It is impartial and does not serve the interests of the people or institutions that disseminate it.

2. FOLLOW-UP PHASE (PRACTICAL)

Follow-up during our second lesson will take the form of a practical exercise in FACT-CHECKING, i.e., verification of the reliability of specific statements with the use of previously learned concepts and procedures.

FACT-CHECKING—THE HAMMER FOR FAKE NEWS

If we believe in FAKE NEWS, we lose the information war, allow others to deceive us, we are naive, and we lose our money or even risk our personal safety.

A basic weapon in information warfare is FACT-CHECKING, i.e., checking whether:

- the information provided to us is objective (FACTS) or subjective (OPINIONS),
- the FACTS provided to us are reliable information or FAKE NEWS.

PRACTICAL EXERCISE

We ask students to do an exercise in groups: they will carry out FACT-CHECKING (in accordance with the procedure developed above and using devices with internet access) on one of the following statements (we assign a specific statement to be verified by each group of students):

1. Every year Poland contributes more to the European Union than it receives from it.
2. In France, Muslims already constitute the majority of the population.
3. During the last U.S. presidential election (2020) massive fraud was observed.
4. Most Poles attend weekly church service every Sunday.
5. Polish students are better at maths than students from Spain.

After the assigned time (approx. 5-10 minutes, depending on the work pace of a given group, which will be best assessed by their teachers themselves), we ask students to present:

1) their judgment on whether the statements presented above are reliable information or FAKE NEWS.
2) the procedure(s) they have applied in order to reach their judgment.

As a conclusion, we encourage students not to accept the role of victims of information warfare, but to systematically protect themselves against FAKE NEWS through FACT-CHECKING.

LESSON 3
REACT! HOW CAN YOU FIGHT DISINFORMATION?

Lesson objectives:

1. To make students aware of the need to actively respond to disinformation.
2. To develop practical ways of dealing with disinformation in its various forms.

3. To familiarise students with technological and psychological risks when fighting disinformation.

Lesson outline:

1. WARM-UP PHASE (THEORETICAL)

Our third lesson's warm-up will serve to make students aware of the need to actively respond to disinformation while a large part of our society remains passive and vulnerable.

SECONDARY RECAPITULATION (revision of previous lessons)

Referring to the materials and exercises from previous lessons, we ask students to estimate the percentage of Poles (their peers, parents, grandparents) who would be able to:

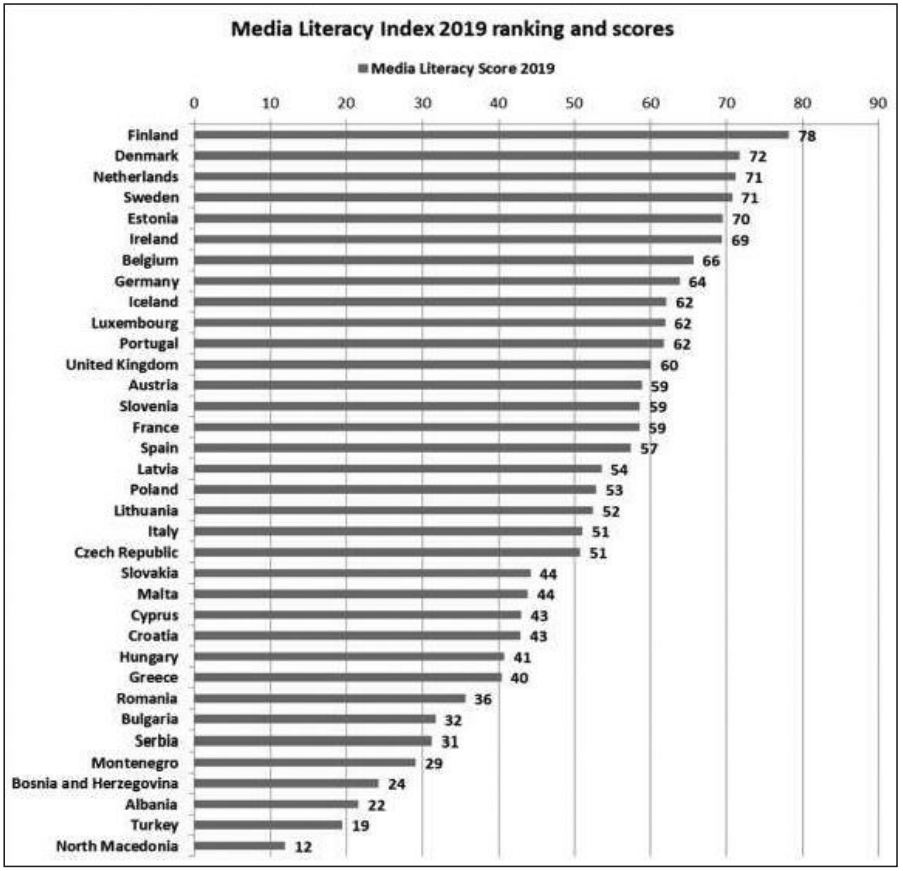
- resist DISINFORMATION in the form of video materials presented during Lesson 1;
- provide definitions of INFORMATION WARFARE and DISINFORMATION (Lesson 1);
- distinguish between various forms of DISINFORMATION such as fabricating information, manipulation, abuse, satire (Lesson 1);
- distinguish FACT from OPINION (according to the procedure proposed in Lesson 2);
- distinguish reliable information from FAKE NEWS (Lesson 2);
- carry out FACT-CHECKING (Lesson 2).

On the board, we write the resulting figure, expressed as a percentage (the percentage of Poles, who would be able to successfully resist DISINFORMATION in all the above forms, as estimated during this class discussion).

We then ask students for their opinion on how well Poles are doing in this respect compared to other European nations.

POLES' MEDIA LITERACY - ARE WE PREPARED FOR INFORMATION WARFARE?

After collecting students' answers, assessments and predictions, we provide them with the FACTS (we emphasise—as a revision—that in this way we will yet again confront OPINIONS with FACTS), i.e., the results of the Media Literacy Index 2019 survey conducted by the Open Society Institute:



www.osis.bg/wp-content/uploads/2019/11/MediaLiteracyIndex2019_-ENG.pdf, p. 5.

We briefly discuss with students to what extent the presented figures are consistent with the group's predictions.

We advise students that media literacy is a very broad concept, defined, among others, as "the ability to select, critically analyse and use information creatively. Being a conscious media user helps us to solve problems, make decisions, and participate in culture and social life."

www.edukacjamedialna.edu.pl/media/chunks/attachment/edukacja_medialna_infografika.pdf

At the end of this part, we ask students what threats to our safety are posed by poor media literacy skills, i.e., the lack of skills to resist DISINFORMATION, at the following levels:

- personal (expected responses may concern, for example, advertisements);
- social (e.g., elections);
- national (e.g., war).

We conclude this part of the lesson with a question (meant as a rhetorical question) whether students now agree that actively responding to DISINFORMATION can be considered their personal, social, and patriotic (national) duty.

1. FOLLOW-UP PHASE (practical)

We ask students to create, through brainstorming, a list of "channels of DISINFORMATION", i.e., the routes by which FAKE NEWS can reach us.

Expected responses include:

- Facebook and other social media;
- news websites;
- Television;
- Press;
- Rumours and jokes (as far as they are satire meant as DISINFORMATION);

Posters and flyers (on the streets).

PRACTICAL EXERCISE

We divide students into as many groups as there are "channels of disinformation" we have identified and we ask students to discuss within these groups how they can actively respond to FAKE NEWS coming from these sources.

When the discussion in groups ends, we ask each group to present the results of their work, and the remaining groups to evaluate the quality of the ideas submitted (e.g., after the presentation of Group 1, we ask Group 3 to indicate the ideas of Group 1 that Group 3 supports, and alternative suggestions in those cases where the ideas of Group 1 do not seem satisfactory).

Expected responses:

- DISINFORMATION on Facebook, social media, news websites: publishing critical comments about the fake news provided, with a brief explanation of what is not true as well as providing hard FACTS (e.g., numbers) and links to more complete information from a reliable source; using the "Report abuse" option; informing the administrator/moderator about the problem;
- television, press: students will probably question the idea of writing official protest letters to the appropriate editors (with a request to publish them in the pages) as pointless, so it can be expected that this topic will cause controversy; other possible solutions are, e.g., unmasking media FAKE NEWS on social networks;
- rumours and jokes: asking those spreading rumours and jokes to consider who and for what purpose may be fabricating them (Latin: *cui bono*? In whose interest?); as a response, giving indication of specific FACTS that contradict the FAKE NEWS spread in this way;
- posters and leaflets: this topic will probably trigger a discussion about whether it will be appropriate to destroy

posters and leaflets spreading FAKE NEWS (e.g., anti-vaccine). Another reaction that students may suggest is, for example, reporting such cases to the police.

The topic of "feeding trolls", i.e., the belief that reacting to FAKE NEWS only increases its visibility on the web and therefore is beneficial to its authors. It is worth discussing the arguments for and against such reasoning with students.

INFORMATION WARFARE – BE CAREFUL!

Encouraged to defend themselves, their community, and their country against information warfare, students should be warned that participation in it involves risks, including technological and psychological ones.

TECHNOLOGICAL RISKS

Information warfare is war, so do not expect your opponent to always play fairly. In modern information warfare, aggressors often use advanced technology, such as bots.

We ask students what bots are, why they are dangerous and how they can be recognised.

Bots are computer programs that perform automated tasks such as spreading content with a specific profile on social media using fake accounts.

How to recognise a bot?

- accounts operated by bots either do not have a profile picture or have stolen pictures, which can be checked, for example, with the "search with an image" service provided by Google;
- bots are extremely active in their short lifetime, e.g., in an election or advertising campaign;
- the names of accounts from which bots operate are most often created automatically, consisting of random letters and numbers;

- bot accounts are created for a given disinformation campaign, so they usually don't have a long history of previous activity;
- bots operate simultaneously in many languages, sometimes in different languages at different times of their activity (depending on the current need), often committing basic grammar mistakes, which are easy to detect;

bots usually cooperate as part of coordinated DISINFORMATION actions, and therefore often their contacts mostly include other bots whose messages they pass on.
(SOURCE: www.msb.se/RibData/Filer/pdf/28698.pdf, p. 24)

It is worth making students aware that not always one person acting on their own is able to overcome an organised DISINFORMATION campaign conducted with the support of technology and machines. First, you should take care of your own internet security (e.g., avoid malware and password theft). If necessary, ask for help from respected institutions, such as schools or the police. However, it is certainly not dangerous to warn people in your own circle about an ongoing DISINFORMATION campaign.

PSYCHOLOGICAL RISKS

Information warfare can be considered a part of a larger scheme—psychological warfare. Therefore, the psychological aspects play a key role here.

When fighting DISINFORMATION, be aware that:

- people who knowingly spread FAKE NEWS will not necessarily remain passive, rather trying to defend their own message and discredit us;
- people who unknowingly accept or distribute DISINFORMATION—if you try to explain and prove it to them—will likely fall into a psychologically uncomfortable state of "cognitive dissonance" (i.e., an internal conflict between the

previous and new state of consciousness), which may cause nervousness and aggression (verbal or even physical).

For this reason, especially in the case of people close to us, and the elderly in particular, responding to DISINFORMATION should be tactful and carried out over a period of time, rather than violent and one-off. It should be remembered that in an information war, our opponents are not people who unknowingly succumb to disinformation, but those individuals and groups that consciously spread it for their own purposes.

SUMMARY (PRIMARY RECAPITULATION)

At the end of this series of lessons, " Protect Yourself Against Disinformation", it is important to make sure students are now aware that:

- they have now been prepared to resist INFORMATION WARFARE;
- they know how to recognise various types of DISINFORMATION;
- they can distinguish FACT from OPINION and reliable information from FAKE NEWS;
- they can carry out FACT-CHECKING when faced with suspicious information;
- they understand why it is important to actively respond to DISINFORMATION on a personal, social, and national level;
- they know how to react to perceived cases of DIS-INFORMATION in its various forms, while taking care of their own technological and psychological safety.

Similar lessons have been taking place for years now and will be held in all NATO member states as an element of increasing the common allied readiness to repel attacks in the form of disinformation, in accordance with the NATO motto:

ANIMUS IN CONSULENDO LIBER

The phenomenon of disinformation is one of the critical problems of contemporary international relations and modern states. Cyberspace has become an area of international competition and a battleground for the hearts and minds of people. This book, edited by Robert Kupiecki and Agnieszka Legucka, is a welcome reflection and the choice of the book's subject is justified, topical, and interesting. The value of the reviewed book is in the combination of theoretical and practical elements and the inclusion of European and Polish perspectives. An extremely important contribution is the section with materials for teachers and lecturers to use in their classes. This is important because of the key role of these professional groups in strengthening awareness and social resilience to disinformation.

Agata Włodkowska,
an Associate Professor at the Vistula University

The Polish Institute of International Affairs (PISM) is a leading Central European think tank that positions itself between the world of politics and independent analysis. PISM provides analytical support to decision-makers and diplomats, initiates public debate and disseminates expert knowledge about contemporary international relations. The work of PISM is guided by the conviction that the decision-making process in international relations should be based on knowledge that comes from reliable and valid research.