Information Security Policy

Conditions, Threats and Implementation in the International Environment

EDITED BY

PIOTR BAJOR

INFORMATION SECURITY POLICY

INFORMATION SECURITY POLICY

Conditions, Threats and Implementation in the International Environment

edited by

PIOTR BAJOR

Piotr Bajor
Jagiellonian University in Kraków, Poland
ⓘD https://orcid.org/0000-0003-2569-2552
✉ piotr.bajor@uj.edu.pl

Review: Marek Delong

Language editor:
Cover design: Marta Jaszczuk

The opinions expressed in this publication are those of the authors and do not reflect the views of the official positions of the Ministry of Foreign Affairs of the Republic of Poland.

Ministry
of Foreign Affairs
Republic of Poland

centrum badań nad
współczesnym
środowiskiem
bezpieczeństwa
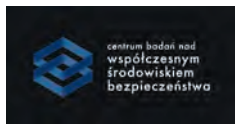
The project was implemented by the Foundation Center for Research on the Contemporary Security Environment, in cooperation with a research team from the Jagiellonian University in Kraków.

Table of contents

Introduction

This publication discusses issues related to information security, analysed through the lens of considerations, threats and implementation policies. The publication is the result of studies done by the research team implementing a project related to information security as part of the "Public Diplomacy 2022" competition organised by the Polish Ministry of Foreign affairs; according to rules of the competition, papers published as part of the contest constitute results of original research and do not reflect the official stance of the Ministry.

Information security is one the key aspects of modern security and its importance has been significantly increasing in contemporary international relations. This publication presents the results of studies on several key aspects related to this issue. The publication contains results of research on considerations related to information security, related threats and its implementation, as well as research on social media, analysed through the lens of the object and subject of disinformation activities. This aspect includes an analysis of communication strategies adopted in respect of the Russian aggression and the ongoing war between Russia and Ukraine, as well as mechanisms implemented as part of information security policies to shape public opinion. The publication also presents results of research directly concerning Ukraine's information security policy, analysed from the point of view of its tenets and implementation in successive years, EU's policy aimed at combating Russian disinformation, and presents an analysis of Russian narratives on Ukraine against the backdrop of wider geopolitical and international considerations.

The perspective presented in the publication concerns selected aspects that make up the concept of security, analysed from the point of view of theoretical assumption, as well as their importance for contemporary analysis of information security and related considerations and threats. The objective of this publication was therefore to present the latest results of research into the issues mentioned above, as well as to deepen the discussion on both theoretical and practical aspects of information security which has become an extremely significant issue in today's world.

Piotr Bajor

Magdalena Danek iD
Jagiellonian University in Kraków

Social Media as a Recipient and Creator of Political Actions in the Context of the Security Crisis

Abstract: Social media is not only an increasingly popular communication channel or business tool, but also one of the arsenals of information warfare. The next phase of Russia's war against Ukraine, launched on February 24, 2022, showed once again that the content disseminated through it is used not only to provide actual information or to improve the organisation of assistance to refugees, but also to spread disinformation and propaganda.

The aim of the article is to analyse the current status of social media platforms as tools of influence and power – particularly during the war in Ukraine – as well as activities aimed at combating disinformation, especially in the context of the activities of the EU, selected state actors and the owners of these platforms themselves (in this aspect, the analysis will include the activities of Meta and Twitter). The research hypothesis is based on the assumption that social media is, in the scope of the present issue, not only the recipient of political decisions made by legitimised actors, but – by virtue of their power over the flow of a significant amount of information – it become an important actor in these activities in terms of influencing political processes and decision-making centres (e.g., by

arbitrarily deciding on the visibility of hate speech content in situations
of armed conflict).

Keywords: social media, disinformation, Ukraine, power, influence, hybrid war

Introduction

With the emergence and development of the internet and the applications based on
it, including social media, expectations could be seen in both public and academic
discourse about the opportunity to make them tools to strengthen democratic pro-
cesses and political engagement of citizens. Thus, television, which Robert Putnam
saw as one of the main causes of generating civic passivity and the erosion of social
capital,[1] was to give way to an egalitarian and interactive space based on free access
to information and free expression of opinion. Jan van Dijk concludes that hopes for
the impact of ICT on politics were linked primarily to increasing the acquisition and
exchange of information between government and administrative representatives and
citizens, enhancing public debate, deliberation, the formation of communities and
citizen participation in decisions of public importance.[2] These approaches were based
on the belief that increasing citizens' access to information benefits both society itself
and democratic procedures.

The massive proliferation of false content on social media, including the notorious
disinformation campaigns accompanying events of particular significance – such as
the 2016 US presidential election, the campaign for Britain's exit from the European
Union (EU), the COVID-19 pandemic or the next round of the war in Ukraine
launched on February 24, 2022 – are shifting the focus towards seeing the internet
and the applications that function within it as a space not primarily for debate, but
information warfare.[3]

---

[1] R. Putnam, *Samotna gra w kręgle. Upadek i odrodzenie wspólnot lokalnych w Stanach Zjednoc-
zonych*, transl. P. Sadura, S. Szymański, Wydawnictwo Akademickie i Profesjonalne, Warszawa
2008, p. 384.

[2] J. van Dijk, *Społeczne aspekty nowych mediów*, transl. J. Konieczny, Wydawnictwo Naukowe
PWN, Warszawa 2010, p. 150.

[3] A. Guess, B. Nyhan, J. Reifler, *Selective Exposure to Misinformation: Evidence from the Con-
sumption of Fake News during the 2016 US Presidential Campaign*, 9.01.2018, [on-line:] https://
about.fb.com/wp-content/uploads/2018/01/fake-news-2016.pdf, 20 November 2022; M.T. Bastos,
D. Mercea, "The Brexit Botnet and User-generated Hyperpartisan News", *Social Science Computer
Review*, vol. 37, no. 1 (2019), pp. 38–54; Y.M. Rocha et al., "The Impact of Fake News on Social
Media and Its Influence on Health during the COVID-19 Pandemic: A Systematic Review", *Journal
of Public Health* (2021), pp. 1–10.

The information space has, since ancient times, been seen as a vital pillar of security and, at the same time, a tool for confrontational action. This is expressed in the words of Sun Tzu, who – in his treatises – indicated that *war is about being misled*.[4] Coherent management of the information space, especially in its digital dimension, is one of the key elements of state security.

The approach to war as not only a kinetic clash, but a whole range of diverse actions – including a special role for the information sphere – has been particularly popularised in the context of the notion of hybrid warfare. The clearest emanation of this phenomenon was Russia's actions towards Ukraine with the annexation of Crimea and the start of fighting in the Donbas region in 2014. The Russian Federation's point of view on the modern battlefield can be reconstructed from an article by the Chief of the General Staff of the Russian Armed Forces (Valery Gerasimov), where he states that nowadays, the fundamental principles of war have changed, and the role of non-military means of achieving political and strategic goals has significantly increased – often exceeding the power and effectiveness of kinetic weapons.[5]

In this sense, hybrid warfare, also referred to as *a war of controlled chaos*, encompasses the entire range of actions implemented to destabilise the economic and political situation, disintegrate and limit sovereignty, and consequently change political power to that controlled by the aggressor.[6] Although the concept of hybrid warfare does not have a clearly defined scope of meaning – and, thus, faces accusations of blurring the boundaries between times of war and times of peace, lowering preparedness for an appropriate response – it is noted that it points to key current and future security and defence challenges.[7]

Russia's ongoing war against Ukraine, which has been continuing since February 24, 2022, despite being – in its significant dimension – an example of a kinetic type of clash, is also marked by a meaningful potential for other acts with the hallmarks of a hybrid impact. It should be emphasized that, they are targeted not only at Ukraine,

---

[4] S u n T z u, *Sztuka wojny*, transl. J. Z a w a d z k i, Hachette, Warszawa 2009, p. 31.
[5] V. G e r a s i m o w, "The Value of Science Is in the Foresight New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations", *Military Review* (2016), [on-line:] https://www.armyupress.army.mil/portals/7/military-review/archives/english/militaryreview_20160228_art008.pdf, 22 November 2022.
[6] O. W a s i u t a, "Geneza pojęcia i zmiany podejścia do wojny hybrydowej w zachodnim dyskursie politycznym i wojskowym", *Przegląd Geopolityczny*, no. 17 (2016), p. 28.
[7] A. B i l a l, "Hybrid Warfare – New Threats, Complexity, and 'Trust' as the Antidote", *NATO Review* 2021, [on-line:] https://www.nato.int/docu/review/articles/2021/11/30/hybrid-warfare-new-threats-complexity-and-trust-as-the-antidote/index.htm (20.11.2022).

but also at Western countries. They manifest themselves, among other means, in large-scale propaganda actions or economic blackmail related to access to energy resources.

The aim of the article is to analyse the current status of social media platforms as tools of influence and the space of power making, in particular during the war in Ukraine, as well as activities aimed at combating disinformation – especially in the context of the activity of the EU, selected state actors and the owners of these platforms themselves (in this aspect, the analysis will include Meta and Twitter activities). The theoretical framework for the undertaken research will be the concept of the network society, and power understood as an influence on the management of communication processes by Manuel Castells. The research hypothesis is based on the assumption that in the scope of this issue, social media is not only the recipient of political decisions made by legitimate actors, but thanks to their control over the flow of a significant amount of information, they become an important actor of these activities in terms of influencing political processes.

In the course of the analysis carried out, three key reference levels were distinguished. The first relates to using social media as a new and increasingly crucial war arsenal in information warfare. The second one concerns regulatory action and the pressure exerted by political actors such as states and international organisations on social media platforms, which resultantly become the object of political action – especially in the context of the fight against disinformation. The last, but extremely important, dimension covers actions taken in relation to the conflict by the managers of social platforms, making them important actors of decision and political impact.

Information management in cyberspace as an emanation of power

Manuel Castells, analysing the contemporary transformations of social, economic and political structures in the era of dynamic ICT development, introduces the concept of a network society (i.e., social structure) whose main features are the presence of digital network communication technologies, as well as the reproduction and insti-tutionalisation of the connections created thanks to them through society itself. In this way, according to the researcher, a *new social morphology* is being created.[8] One of the essential dimensions of this emerging social structure are the power relationships

---

[8]   M. Castells, *Społeczeństwo sieci*, crowd. M. Marody et al., transl. M. Marody, Wydawnictwo Naukowe PWN, Warszawa 2011, p. 491.

Information security is one the key aspects of modern security and its importance has been significantly increasing in contemporary international relations. This publication presents the results of studies on several key aspects related to this issue. The publication contains results of research on considerations related to information security and its implementation, as well as research on social media, analysed through the lens of the object and subject of disinformation activities.

WYDAWNICTWO
KSIĘGARNIA
AKADEMICKA
Sp. z o.o.   Kraków

https://akademicka.pl