KRAKOWSKA AKADEMIA IM. ANDRZEJA FRYCZA MODRZEWSKIEGO
ANDRZEJ FRYCZ MODRZEWSKI KRAKOW UNIVERSITY

BEZPIECZEŃSTWO
TEORIA I PRAKTYKA

SECURITY
THEORY AND PRACTICE

SECURITY MANAGEMENT MECHANISMS
IN THE FACE OF CONTEMPORARY THREATS

edited by
Andrzej Chodyński

e-ISSN 2451-0718
ISSN 1899-6264

Kraków 2022
No. 2 (XLVII)

KRAKOWSKA AKADEMIA IM. ANDRZEJA FRYCZA MODRZEWSKIEGO
ANDRZEJ FRYCZ MODRZEWSKI KRAKOW UNIVERSITY

BEZPIECZEŃSTWO
TEORIA I PRAKTYKA

SECURITY
THEORY AND PRACTICE

SECURITY MANAGEMENT MECHANISMS
IN THE FACE OF CONTEMPORARY THREATS

edited by
Andrzej Chodyński

Kraków 2022
No. 2 (XLVII)

BEZPIECZEŃSTWO TEORIA I PRAKTYKA
SECURITY THEORY AND PRACTICE
e-ISSN 2451-0718
ISSN 1899-6264
2022
No. 2 (XLVII)

Redakcja/Office:
ul. Gustawa Herlinga-Grudzińskiego 1A, pok. 215
30-705 Kraków
tel. (12) 25 24 665
btip.ka.edu.pl

Czasopismo punktowane w rankingu Ministerstwa Edukacji i Nauki oraz indeksowane w następujących bazach / The journal is ranked by the Ministry of Education and Science and indexed in the following bases:
Repozytorium eRIKA. Repozytorium Instytucjonalne Krakowskiej Akademii im. Andrzeja Frycza Modrzewskiego;
PBN. Polska Bibliografia Naukowa; Index Copernicus; CEJSH. The Central European Journal of Social Sciences; CEEOL. Central and Eastern European Online Library; BazHum

e-ISSN 2451-0718
ISSN 1899-6264

Na zlecenie / Commissioned by:
Krakowska Akademia im. Andrzeja Frycza Modrzewskiego
www.ka.edu.pl

Wydawca / Publisher: Oficyna Wydawnicza KAAFM

BEZPIECZEŃSTWO TEORIA I PRAKTYKA
SECURITY THEORY AND PRACTICE
e-ISSN 2451-0718
ISSN 1899-6264
2022
No. 2 (XLVII)

Contents

ARTICLES

VARIA

BULLETINS, REPORTS

BEZPIECZEŃSTWO TEORIA I PRAKTYKA
SECURITY THEORY AND PRACTICE
e-ISSN 2451-0718
ISSN 1899-6264
2022
No. 2 (XLVII)
DOI: 10.48269/2451-0718-btip-2022-2-000

Andrzej Chodyński

Professor, Andrzej Frycz Modrzewski Krakow University
https://orcid.org/0000-0003-4962-5143

Security management mechanisms in the face of contemporary threats: Introduction

The level of security of an organisation depends on a variety of factors, including the ability to identify risks and the implementation of security management, including governance mechanisms. The following criteria are considered in the typology of security threats:

1) objective – this includes political, military, and economic, as well as social and environmental security;
2) sources of threats – described as natural, technical, systemic, demographic, ideological, economic, educational, psychological, cultural, and other;
3) environmental – different environments are taken into account: natural, social, political, economic, scientific, and technological;
4) coverage – from global, through continental and regional, to local; and
5) scale of the threats – from the global level, through the international and state levels, to the administrative unit level.[1]

A threat is a situation involving the possibility of sudden, unpleasant, and unexpected events causing negative consequences. Threats can be potential, real, subjective or objective, external or internal, military or non-military, as well as accidental (random) or intentional.[2] A threat is a situation where an unsafe condition is likely to

[1] Ł. Roman, "Istota współczesnych wyzwań i zagrożeń bezpieczeństwa", *Journal of Modern Science*, vol. 27, no. 4, 2015, pp. 209–226, https://bibliotekanauki.pl/articles/451938 [accessed: 3 August 2022].

[2] P. Daniluk, H. Wyligała, *Analiza zagrożeń sektorowych dla bezpieczeństwa*, Warszawa: Difin, 2021, pp. 10–11.

occur for both the external and the internal environments. Threats are also analysed in the context of a crisis. The most important non-military threats are natural hazards. In the context of threats, much attention is paid to disasters due to both natural and civilisational causes.[3]

With regard to national security (within the national security governance system), the importance of monitoring the sources and scale of threats, as well as their types and directions, together with the prevention of the emergence of threats within and outside the national territory are emphasised. The importance of prevention of the effects of these threats, their elimination, and taking action with regard to the management of the defence of the state is pointed out.[4]

In the systemic approach, organisational security is the feature of an object that concerns its resistance to hazardous situations. The security of an organisation can also be considered as its ability to protect its values (sensitive assets) from threats, which can be related to systemic characteristics such as quality, reliability, stability, as well as sustainability and viability. The desired level of security for an organisation is provided by the organisation's security system. Disruptions affecting the security level of an organisation can be of various types – natural (e.g. floods), civilisational, technical failures – and can relate to equipment and systems, the specific regional characteristics, and the location, or to disruptive human actions. The factors affecting the level of security of an organisation also include the mechanisms for countering threats.[5]

The security of an economic organisation is mainly analysed from the point of view of prevention with regard to its potential for loss.[6] The security of a business is considered as a dynamic state. It is present when the entity is ensured access to the most important values (goods), with no deterioration of this access in the future, which involves effectively pushing away or eliminating interferences.[7] Security management, on the other hand, refers to the minimisation or elimination of threats

---

3 F. Mroczko, *Zarządzanie kryzysowe w sytuacji zagrożeń niemilitarnych. Zarys problemów regionu dolnośląskiego*, "Zarządzanie" Series, no. 32, Wałbrzych: Wałbrzyska Wyższa Szkoła Zarządzania i Przedsiębiorczości, 2012, pp. 63–70.

4 W. Kitler, "System bezpieczeństwa narodowego RP – aspekty prawno-organizacyjne", *Wiedza Obronna*, vol. 268, no. 3, 2019, pp. 5–33, http://wiedzaobronna.edu.pl/index.php/wo/article/view/3/48 [accessed: 14 February 2022].

5 J. Stanik, R. Hoffmann, J. Napiórkowski, "Zarządzanie ryzykiem w systemie zarządzania bezpieczeństwem organizacji", *Ekonomiczne Problemy Usług*, no. 123, 2016, pp. 321–336.

6 J. Konieczny, "Bezpieczeństwo państwa a bezpieczeństwo biznesu. Studium metodologiczne", *Bezpieczeństwo. Teoria i Praktyka*, no. 4, 2015, p. 17.

7 M. Kwieciński, Zarządzanie bezpieczeństwem działalności przedsiębiorstwa – zarys problematyki, [in:] *Zarządzanie w sektorach prywatnym oraz publicznym*, ed. P. Lenik, "Prace naukowo-dydaktyczne Państwowej Wyższej Szkoły Zawodowej im. Stanisława Pigonia w Krośnie" no. 70, Krosno: Państwowa Wyższa Szkoła Zawodowa im. Stanisława Pigonia w Krośnie, 2016, p. 150.

through deliberate regulatory action by people. It can be considered from the standpoint of risk management, crisis management, disaster (accident) management, and value management.[8] Security management refers to the protection against threats to different types of resources (assets): people, buildings, machines, and information resources, considering the risk and taking into account the vulnerabilities.

It is interesting to see organisations from the standpoint of security as agile, smart, or learning.[9] Consideration is given to the possibility of using the intellectual capital of individual organisations, including those operating in a network that promotes security and social capital.[10]

Cluster-like links present a model of cooperation between companies, universities, and public administration (a *triple helix*), which takes the form of a quadruple helix when social media and civil society are included. The evolution is highlighted of cooperation within clusters related to synergistic impacts of the following nature: 1) modular, based on pooling the resources of partners who manage resources independently, 2) sequential, based on the division of tasks between partners who adapt the resources to the cooperation, and 3) reciprocal, based on the pooling of companies' resources and knowledge sharing, which leads to mergers or acquisitions. Coopetitive behaviour and its types are also considered. The role of open innovation is also highlighted.[11]

This issue of *Security: Theory and Practice* addresses the issue of mechanisms for security management. The literature on this subject describes various mechanisms. The renewal mechanism is considered within the framework of the issue of company management in crises affecting specific industries. It can take the form of a spatial or temporal separation mechanism. The former mechanism, which relates to large organisations, involves renewal processes initially taking place in specific entities, as well as in departments or at functional levels of organisations. It is associated with the implementation of a learning loop and involves rearranging the structure and renewing key

---

[8] L. Korzeniowski, *Podstawy nauk o bezpieczeństwie*, "Zarządzanie Bezpieczeństwem" Series, Warszawa: Difin, 2012, p. 58.

[9] The concept of a Smart City (also in the context of a sustainable city) is presented in: A. Chodyński, "Wykorzystanie dorobku nauk o zarządzaniu na rzecz podnoszenia bezpieczeństwa miast. Koncepcja smart", *Bezpieczeństwo. Teoria i Praktyka*, no. 4, 2019, pp. 39–62, and the concept of learning organizations that use experience from emergency situations is presented in: idem, "Uczenie się i wpływ społeczny a bezpieczeństwo na poziomie lokalnym – zarządzanie w sytuacji awarii zagrażającej środowisku naturalnemu", *Bezpieczeństwo. Teoria i Praktyka*, no. 4, 2021, pp. 61–80.

[10] Idem, Sieciowość w koncepcjach biznesu – aspekty społeczne i ekologiczne, [w:] *Zarządzanie odpowiedzialnym rozwojem przedsiębiorstwa*, Kraków: Oficyna Wydawnicza KAAFM, 2012, p. 83–110.

[11] M. Klimczuk-Kochańska, Relacje międzyorganizacyjne, [in:] *Zarządzanie, organizacje i organizowanie – przegląd perspektyw teoretycznych*, ed. K. Klincewicz, Warszawa: Wydawnictwo Naukowe Wydziału Zarzadzania Uniwersytetu Warszawskiego, 2016, pp. 343–354.

competences with a limited risk. The temporal separation mechanism, which often applies to small and medium-sized companies, means that changes are implemented sequentially throughout the organisation. As a form of strategic entrepreneurship that is associated with innovation, it involves the introduction of new products and services, and the acquisition of new customers and new markets.[12] Strategic management considers the mechanisms of coordination and allocation of corporate resources related to the creation of transaction costs: price-based (market-based), hierarchical (characteristic of bureaucracy), and the later one, relational (social, based on trust).[13]

When considering an organisation as a system, the notion of an adjustment mechanism, which is a dynamic element of the management system, is discussed. It is responsible for the ability to shape new equilibrium conditions. Particularly important is its role in the mutual adjustment of three groups of stabilising components: values and goals, regulation and structures, and management methods and practices.[14] The concept of a mechanism is referred to various areas and activities within an organisation: corporate renewal,[15] knowledge management (refers to solutions, tools, and methods),[16] and mechanisms for managing inter-organisational networks.[17]

The mechanism of organisational learning and the use of effective learning instruments and techniques were analysed using the example of activities carried out in government administration. The mechanisms of organisational learning were considered in the context of the processes of knowledge creation and the factors that support them. Practices that enhance organisational learning were identified.[18] Technological entrepreneurship is cited as a mechanism for organisational development.[19] The key mechanisms are also discussed at the level of management paradigms.[20] The term

---

[12] B. Hajdasz, *Wybory strategiczne podczas odnowy przedsiębiorstwa indukowanej kryzysem branży*, doctoral thesis, Uniwersytet Ekonomiczny w Poznaniu, Wydział Zarzadzania, 2017, p. 74.

[13] W. Czakon, "Obrazy sieci w zarządzaniu strategicznym", *Zeszyty Naukowe Wydziału Zamiejscowego w Chorzowie Wyższej Szkoły Bankowej w Poznaniu*, no. 19, *Strategie przedsiębiorstw w sieci*, 2017, pp. 71–81.

[14] J. Skalik, A. Barabasz, G. Bełz, "Systemowe uwarunkowania rozwoju metod zarządzania. Przykład modelu Triady", *Acta Universitatis Lodziensis. Folia Oeconomica*, vol. 234, 2010, pp. 71–83.

[15] J. Karpacz, Swoboda działania jako determinanta odnowy strategicznej przedsiębiorstwa, [in:] *Strategie rozwoju organizacji*, eds. A. Stabryła, T. Małkus, Kraków: Fundacja UE w Krakowie, 2012, pp. 45–55.

[16] B. Mierzejewska, "Mechanizmy wspierające zarządzanie wiedzą w organizacji", *E-mentor*, no. 3(10), 2005, pp. 55–59.

[17] P. Kordel, *Zarządzanie sieciami międzyorganizacyjnymi*, Gliwice: Wydawnictwo Politechniki Śląskiej, 2010, p. 67.

[18] *Jak wzmacniać organizacyjne uczenie się w administracji rządowej*, eds. B. Ledzion, K. Olejniczak, J. Rok, Warszawa: Wydawnictwo Naukowe SCHOLAR, 2014, pp. 12–14.

[19] P. Kordel, *Przedsiębiorczość technologiczna*, Gliwice: Wydawnictwo Politechniki Śląskiej, 2018, pp. 13–14.

[20] A. Jaki, "Mechanizmy rozwoju paradygmatów zarządzania", *Przegląd Organizacji*, no. 2, 2014, pp. 8–13.

mechanism is often defined as coordination concerning direct managerial supervision, as well as the alignment of contractors. Using the role of the organisational structure for the integration activities of the different parts of an organisation, a system standardisation – coordination system is considered.[21] A mechanism is also seen as a key metaphor for organisational reality (e.g. as a network or a metaphor of a technological nature).[22] Resilience mechanisms related to the sustainability of an organisation are also considered.[23] The literature on this subject emphasises that resilience draws attention to a culture of preparedness. It uses mechanisms of a central or local (bottom-up) nature that result not only in the absorption of shocks, but also in opportunities concerning the adaptation of vulnerable (weakest) elements of different types of systems: social, economic, and political. The importance of the ability to restore resources in systems, as well as to restore functionality, is emphasized. Attention is drawn to the role of the autonomous capacities of individual links in the system – both resilient (robust) and adaptive.[24]

A critical infrastructure protection mechanism based on an ongoing exchange of information is described.[25]

According to the author of this text, the mechanisms presented can play a significant role as a response to existing or possible threats. The concept of a mechanism is described in detail in this issue of *Security: Theory and Practice* in the publication relating to the issue of *ambidexterity* (an article by Andrzej Chodyński).

The issue addresses a number of questions related to the opinions presented. At the national level, reference was made to enhancing security with distributed energy resources based on renewable energy sources, particularly in situations of war threats (an article by Krzysztof Waśniewski). In showing the prospects for creating hydrogen valleys, reference was made to the concept of clusters (an article by Anna Bałamut). Different viewpoints related to security management at organizations were presented. Hazards related to occupational safety are pointed at by Janusz Ziarko. New innovative solutions concern the use of blockchain technology (an article by Katarzyna Sienkiewicz-Małyjurek). The issues of management mechanisms appear in articles on information management (articles by Marta du Vall and Marta Majorek) and in articles on railway safety. The topic of safety culture in relation to the concept

---

[21] *Nowe kierunki w organizacji i zarządzaniu. Organizacje, konteksty, procesy zarządzania*, eds. B. Glinka, M. Kostera, Warszawa: Oficyna a Wolters Kluwer business, 2012, p. 269.

[22] G. Gliszczyński, L. Panasiewicz, "Koncepcja modelu metasystemu jako kierunek rozwoju teorii systemów zarządzania", *Przegląd Organizacji*, no. 1, 2018, pp. 21–29.

[23] S.T.A. Pickett, B. McGrath, M.L. Cadenasso, A.J. Felson, "Ecological resilience and resilient cities", *Building Research & Information*, vol. 42, issue 2, 2014, pp. 143–157.

[24] M. Stępka, "Rezyliencja jako paradygmat bezpieczeństwa w czasach przewlekłych kryzysów", *Przegląd Politologiczny*, no. 2, 2021, pp. 105–117.

[25] Narodowy Program Ochrony Infrastruktury Krytycznej – tekst jednolity, 2020, p. 38, https://www.konin.pl/files/dokumenty_na_strone_2021/Narodowy-Program-Ochrony-Infrastruktury-Krytycznej-2020-tekst-jednolity.pdf [accessed: 11 August 2022].

of intellectual capital is addressed (an article by Agnieszka Giszterowicz), as well as the role of the manager in shaping the safety culture of an organisation (an article by Michał Adam Leśniewski).

The articles respond to the recommended topics specified in the call for papers sent to the authors, which states:

> A manifestation of the resilience of organisations (including towns/cities, and various types of business entities) is to maintain the continuity of their operations. To achieve this, it is necessary to implement a system of appropriate coordination of activities, also in emergency situations. Coordination of activities is associated with the implementation of security management mechanisms.[26]
>
> Adequate management mechanisms should ensure business continuity also in unexpected situations, i.e. those that take place on an ad hoc basis, and within an operational perspective. At the same time, the role of mechanisms in the strategic perspective should be emphasised, as a major part of appropriate resilience strategies. People will play an important role in the implementation of these mechanisms: on the one hand, employees, and on the other hand, managers of commercial and non-commercial organisations, using various instruments to maintain the continuity of the organisation's operations in emergency situations.

With reference to the issue of rail safety in the European Union, including the role of cluster-like links, the views of representatives of the European Railway Clusters Initiative (ERCI) were presented, as well as a report from a workshop on the subject held in Italy. Attention was also given to the need to build security in organisations, with emphasis on the role of audits (a report from the 21st International Congress on Internal Control, Internal Audit, Anti-Corruption, and Anti-Fraud). Current security issues at the state and business levels are presented in a report from Mirosław Kwieciński's original seminar. Highlights from the Krynica Forum 2022 were presented by Krzysztof Waśniewski and Anna Bałamut.

[26] The European Commission adopted a set of legislative conclusions aimed at limiting the emission of greenhouse gases by 2030, thus adjusting the climate, energy, transport and tax policy, European Commission, Brussels, 14 July 2021, COM(2020) 562 final: Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and The Committee of the Regions ,"Fit for 55": delivering the EU's 2030 Climate Target on the way to climate neutrality.

BEZPIECZEŃSTWO TEORIA I PRAKTYKA
SECURITY THEORY AND PRACTICE
e-ISSN 2451-0718
ISSN 1899-6264
2022
No. 2 (XLVII)
DOI: 10.48269/2451-0718-btip-2022-2-Con

Conversation on and presentation of opinions about safety management in railway traffic of the European Union

Moderated by Professor Andrzej Chodyński,
Andrzej Frycz Modrzewski Krakow University

Dirk-Ulrich Krüger

President of ERCI – European Railway Clusters Initiative ASBL

Veronica Elena Bocci

Vice President of ERCI – European Railway Clusters Initiative ASBL

1. The state of railway safety in Europe

a) What factors currently determine the development of rail transport safety in Europe?

Rail transport safety is presently shaped by migrating (new) digital technologies into railway operations. This coincides with a societal demand towards rail to increase its transport capacities. While digital technologies enable a much higher productive output in rail operations, they create also new threats – mainly in relation to cybersecurity. Especially in the context of the aggressive war against Ukraine, it will be major consideration for European countries to prevent cyberattacks against critical infrastructures such as the railway system. We must bear in mind that not only can core safety processes can be targeted, but also weaker systems like passenger information or ticketing might be attacked and create enough damage to force the system to break down.

b) What is the impact of the requirements of the 4th Railway Package on safety, especially in the context of the functioning of the single railway market?

Our expectation is that unified standards and processes for homologation may speed up the migration of innovative solutions into the sector. Also, this provides an excellent commercial perspective to innovative companies to target the huge EU market with just one homologation process. This is a major step in the development of the industry.

c) How is knowledge transferred within the ERCI in the field of railway traffic safety?

The ERCI offers an international conference event at least twice a year as part of its Cybersecurity Taskforce. With representatives from industry, science and politics, current topics, challenges and solutions in the field of cybersecurity in railway technology are discussed. In addition, the ERCI webinar series is on twice a month. Here, institutions can present innovative products or services. The webinars are open to all topics and thus are also accessible to the field of railway security.

2. The development of innovations in rail transport and their levels of implementation in Europe

a) What is the status of innovation development and the degree of innovation implementation in Europe today?

In general, railway transport has more of a migration problem than an innovation problem. There are many innovative solutions on the market for many challenges that the sector faces. However, it generally takes too long to implement them into operations, especially when compared to other modes of transport such as automotive or aviation and the military sector.

b) What is the average implementation time for technical innovations in Europe?

This takes a comparatively long time, often 10–15 years or longer. The problem is inflexible and strict regulation, which used to be different in every country. Also, the long durability of the technical systems compared to other sectors leads to long implementation times for innovations.

c) What does the development of innovations in Europe's rail transport mainly concern?

All major areas of innovation should centre around the key challenge of the sector – to deliver more transport volumes at a better quality with enhanced capacity utilisation and a greener footprint. Thus, areas of innovation or digitalisation of operational and sales processes, interoperability of European railway systems, predictive maintenance of rolling stock and infrastructure, alternative propulsion technologies and lightweight concepts.

d) How can the ERCI support railway companies in the context of implementing innovative solutions?

The ERCI connects 16 countries and over 2,000 institutions from industry and science across Europe. In the past funding period of Shift2Rail, 18 successful consortia were supported. In addition, the ERCI Innovation Awards take place annually, where innovative products and services are rewarded. So, in a nutshell – we bring together the right players from across the continent to develop solutions and products for the railways of tomorrow.

3. Problems of ecology in EU rail transport

a) How are the principles of the Green Deal changing the development of rail transport in Europe?

The Green Deal is a major shift in strategy and will have a huge impact on transport in general. Don't forget – this is the major political framework in Europe on how to address climate change. The transport sector is a focus area, as it gives quite a lot of leverage for CO_2 reduction. The rail sector is expected to deliver a much higher share of the modal split over the next decade or so, as compared to today. That means more investments in infrastructure and rolling stock, but also better capacity utilisation and therefore solutions for safe and timely operation of more dense traffic on the network. Also, rail transport will need to be better aligned to logistical transport chains and personal trip planning. Intermodality and easy access to rail from other modes of transport will become increasingly important.

b) How is the climate and energy transformation influencing the development of rail transport in Europe?

A major influence is seen in propulsion technology. The shift away from diesel to the use of alternative propulsion technologies such as hydrogen or batteries is evident throughout Europe. In addition, the topic of secure and reliable energy supply is coming into focus. But the key will probably be more electrification of the network. This will provide the best efficiency and provide the grounds for freight transport and high-speed connections in areas that do not have attractive connections today.

c) What are the benefits and risks of striving for change to cause positive climate change in the rail transport sector?

The benefits for the rail sector are a) a greater relevance of rail in the modal split, b) the strengthening of the rail industry along the entire value chain, and c) the perception as the transport mode of the future and therefore a higher attractiveness as an employing industry.

The risks relate to the fact that rail could fail to deliver on expectations as overly ambitious planning will increase the unreliability of and possibility of errors in the overall system. Also, the high costs of creating the additional capacities in infrastructure and rolling stock might hinder achievement of the ambitious targets.

d) How does the development of renewable energy sources, including hydrogen technologies, influence the development of rail transport in Europe, based on the experience of the ERCI?

Again, more electrification will be a good means to use renewable and sustainable energy sources, as it allows management of the grid and distribution of energy that would be centrally generated. In combining the high efficiency of power distribution with the high efficiency of electric drives and the possibility of energy recuperation from vehicles, no other mode of transport can deliver nearly as green a travel option.

Battery storage and hydrogen concepts will both provide the option to store sustainably generated energy for propulsion. Both concepts have limitations in terms of energy density, therefore their main use case will be in replacing passenger trains, currently powered by diesel in more rural areas. I expect that both propulsion concepts will be successful in the market. Which concept is to be chosen will depend on specific characteristics of the operational conditions and also on the infrastructural conditions for refuelling and recharging.

Finally, in markets like the USA, with large non-electrified networks and heavy-haul diesel traction, the most likely solution will be synthetic fuels. These markets will probably continue to operate on the basis of diesel for longer than we will in Europe, and shift to synthetic fuels once they are more broadly available at more commercially attractive price points.

Adam Jabłoński

Associate Professor PhD, President of the Board of the Southern Railway Cluster

Marek Jabłoński

Associate Professor PhD, Vice President of the Board of the Southern Railway Cluster

Referring to the words of Dirk-Ulrich Krüger and Veronica Elena Bocci, the ERCI Management Board, of key importance is to define the place and role of the functioning rail transport in Polish conditions against the backdrop of the applicable EU requirements.

It is important from the point of view of the requirements of the 4th Railway Package applicable throughout the EU, in particular with regard to rail safety, rail interoperability and shaping innovation in rail transport. With this adopted logic, it is worth asking the founders and creators as well as the current management board of the first railway cluster in Poland, founded in 2011. This cluster is also the only cluster from Poland, and at the same time a founding member of the ERCI network of railway clusters unique in Europe. The President of the board of the Southern Railway Cluster is an Associate Professor PhD Adam Jabłoński, the Vice President of the Management Board is an Associate Professor PhD Marek Jabłoński.

Adam Jabłoński says that in Poland, rail transport is safe compared to other EU countries. Nevertheless, it should be overlaid with an individual dimension of the local specificity of individual EU countries. This is due to the fact that each country has a different density of railway infrastructure, as well as average travel speed in the process of passenger and freight transport. In this context, we are faced with a situation of increasing speed in the Polish railway infrastructure, which may generate new threats to the safety of railway traffic in the context of both the replaced infrastructure and rolling stock.

Marek Jabłoński points out that an important element is also the implementation of investment processes, especially in Poland. Currently, the peak of the works being carried out can be observed, which significantly reduces railway traffic capacity. This generates changes in the organisation of railway traffic, which may result in a number of threats to the safety of railway traffic. Unfamiliarity with the operation of equipment, lack of the expected level of training and experience of the staff, and failure to ensure safe cooperation of new and old equipment are the key threats faced by experts in the railway industry. The widespread implementation of the new ETCS rail traffic control system, not yet used in Poland, is a key challenge for rail operators and infrastructure managers.

In the context of the safe operation of rail transport in Poland, **Adam Jabłoński** refers to the war between Russia and Ukraine taking place directly on our borders. This is of particular importance for the safety of the railway system in Poland. Threats can range from cybersecurity factors to physical terrorist attacks. In this dimension, it is important to understand the issues and distinguish two areas required for modern management: digital safety and cybersecurity. Activities in Poland should follow these two key directions in the development of rail transport in Poland.

According to **Marek Jabłoński**, the adaptation of operational processes in the context of the implementation of new technical solutions, such as ETCS Level 2 and GSM-R digital communication is a key task for rail traffic operators in Poland. Everyone is learning this, especially in the context of ensuring the safe operation of these systems. Therefore, the biggest challenge will be to ensure safe integration of new systems with solutions already in use. This is where the greatest risks can arise.

In conclusion, **Adam Jabłoński** points out that against the backdrop of the above-mentioned issues, the strength and potential for participation of the Southern Railway Cluster in the European Cluster Network is emerging. Thanks to it, we have access to the best innovative solutions in rail transport, which we can adapt, present and explore for individual domestic users of rail transport in Poland. This is also confirmed by the fact that both Adam and Marek Jabłoński have been members of the ERCI Innovation Award Jury for many years, a competition aimed at selecting entities that offer and deliver highly innovative products and services for rail transport to the market, both in the context of technological solutions and operational conditions.

Dirk-Ulrich Krüger is the President of the ERCI – European Railway Clusters Initiative ASBL, Brussels, Belgium. The ERCI is an association that unites 15 innovation-driven European railway clusters, that cover 16 countries and have a consolidated membership of over 2,000 businesses and research institutes. The ERCI's mission is to bring customers, suppliers and supply chain opportunities together. Mr Krüger is also the Managing Director of Rail.S – the East German railway industry cluster that is a founding member of ERCI. Besides his long experience in that position, he has a strong background in strategic and financial advice for the transport and infrastructure sector. Former positions in that field include PwC (PricewaterhouseCoopers). Mr Krüger holds a degree in business studies from HTW – Dresden University of Applied Sciences. He is also a charterholder of CFA Institute, Charlottesville, Virginia, USA.

Veronica Elena Bocci is the Vice President of the ERCI – European Railway Clusters Initiative ASBL, Brussels, Belgium and Coordinator of DITECFER District for Rail Technologies, High Speed, Network's Safety and Security Consortium.
She is a graduate of the University of Pisa and several other faculties including the University of Fribourg, 24ORE Business School and DiploFoundation.

Adam Jabłoński, PhD is an Associate Professor at WSB University in Poznań, Poland, and Head of the Institute of Management and Quality. He is also President of the Board of a reputable management and technology consulting company "OTTIMA plus" Ltd. Katowice and President of the Association of the "Southern Railway Cluster" Katowice, which supports development in railway transport and innovation transfer, also working towards cooperation with the European Railway Clusters Initiative ASBL, Brussels, Belgium. For many years, he has also been a member of the jury for the ERCI Innovation Awards in railway transport. He holds a postdoctoral degree in economic sciences, specialising in management science.

Working as a management and technical consultant since 1997, his experience and expertise have grown through his contact with a number of leading companies in Poland and abroad. He is the author of a variety of studies and business analyses in the fields of business models, digital and sustainable business models, strategic management, safety and digital safety, railway transport, value-based management and risk management. Additionally, he has written and co-written several monographs and over 100 scientific articles in the fields of management and railway safety management, published both in Poland and abroad.

Marek Jabłoński, PhD is an Associate Professor at WSB University in Poznań, Poland. He is also Vice President of the Board of "OTTIMA plus" Ltd. Katowice, and Vice President of the Association "Southern Railway Cluster" Katowice. He holds a postdoctoral degree in economic sciences, specialising in management science.

Working as a management and technical consultant since 1997, his experience and expertise have grown through his contact with a number of leading companies in Poland and abroad. He is the author of a variety of studies and business analyses in the fields of business model concept, value-based management, performance management, value creation and project management, and particularly in railway safety management. He has also written and

co-written several monographs and over 100 scientific articles in the fields of management, railway safety management, published both in Poland and abroad. Marek's scientific interests focus on the issues of modern and efficient business model design, including sustainable business models, innovative business models, value creation, railway safety management and the technical aspects of safety rules.

Adam Jabłoński and **Marek Jabłoński** are the co-authors of a series of books. In their monographs, they introduced, developed and promoted the concept of *mechanisms* of effective safety and maintenance management in rail transport, mechanisms for effective management of sidings in rail transport, mechanisms for shaping safety culture in rail transport, mechanisms for ensuring technical and safe compliance integration, and management mechanisms for the safe operation and maintenance of railway vehicles.

In 2022, they co-wrote a book *Digital Safety in Railway Transport – Aspects of Management and Technology* for the Springer Series in Reliability Engineering.

Articles

BEZPIECZEŃSTWO TEORIA I PRAKTYKA
SECURITY THEORY AND PRACTICE
e-ISSN 2451-0718
ISSN 1899-6264
2022
No. 2 (XLVII)
DOI: 10.48269/2451-0718-btip-2022-2-001
Received: 8.06.2022
Accepted: 21.07.2022

Katarzyna Sienkiewicz-Małyjurek
Associate Professor, Silesian University of Technology
https://orcid.org/0000-0002-0915-5776

Benefits, challenges, and perspectives of using the blockchain technology in emergency management

Introduction

Blockchain is a decentralized technology based on distributed ledger information in a peer-to-peer network, in which each node includes a copy of a given chain and has access to the complete transaction history without the need for intermediaries.[1] As a result, this technology facilitates the acquisition, storage and transmission of information and ensures its transparency and integrity. It creates new opportunities for joint activities and sharing resources, increasing the possibility of providing public services. For this reason, it is considered one of the most significant technological trends, a global revolution and innovation changing organizational structures and methods of implementing activities.[2] It is not a new technology but a new way of using other advanced technologies.

1 S. Ølnes, J. Ubacht, M. Janssen, "Blockchain in government: Benefits and implications of distributed ledger technology for information sharing", *Government Information Quarterly*, vol. 34, no. 3, 2017, p. 356; C. L'Hermitte, N.-K.C. Nair, "A blockchain-enabled framework for sharing logistics resources during emergency operations", *Disasters*, vol. 45, no. 3, 2021, p. 534.

2 M. Janssen, V. Weerakkody, E. Ismagilova, U. Sivarajah, Z. Irani, "A framework for analysing blockchain technology adoption: Integrating institutional, market and technical factors", *International Journal of Information Management*, vol. 50, 2020, p. 303; F. Lumineau, W. Wang, O. Schilke, "Blockchain governance – A new way of organizing collaborations?", *Organization Science*, vol. 32, no. 2, 2021, p. 500.

Nowadays, blockchain is gaining more and more followers. Researchers and practitioners point to the potential of this technology not only in banking and finance but also in trade, healthcare, insurance, transport, supply chain management, data management, education, voting, public procurement, social assistance, administrative processes and energy market.[3] Increasingly, researchers claim that blockchain can transform public policy and public service activities.[4] However, research on the subject is limited, and blockchain's usefulness is still debatable.[5] The current research on the blockchain is primarily conceptual, focusing on the technical aspects of using this technology.

As a result, more and more attention is being paid to the disadvantages and limitations of blockchain technology. Possible problems result from, among others, the lack of legal regulations defining the scope and manner of using this technology, the lack of specialist knowledge, and limited scalability and compatibility with other systems.[6] Ølnes et al.[7] and Jansen et al.[8] also noted that – as with any other technology – blockchain, in terms of technology, is insufficient to guarantee an increase in the efficiency of operations. Because blockchain is an emerging technology in public governance, there are extensive research needs both in terms of the possibilities and principles of its implementation, as well as its positive and negative effects.

Considering the potential benefits of blockchain implementation, researchers in the field of emergency management are calling for more research on this topic.[9] This technology could have particular importance in this area due to the complex and dispersed nature of emergency management and the growing scale of contemporary threats.[10] It could facilitate decentralized management of activities and thus improve

---

3 F. Lumineau, W. Wang, O. Schilke, "Blockchain governance ..., *op. cit.,* pp. 501–502; E. Tan, S. Mahula, J. Crompvoets, "Blockchain governance in the public sector: A conceptual framework for public management", *Government Information Quarterly*, vol. 39, no. 1, 2022, 101625, p. 1.

4 D. Tapscott, A. Tapscott, *Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money Business and the World*, New York: Portfolio-Penguin, 2016; D. Cagigas, J. Clifton, D. Diaz-Fuentes, M. Fernández-Gutiérrez, "Blockchain for Public Services: A systematic literature review", *IEEE Access*, vol. 9, 2021, p. 13904.

5 M. Janssen, V. Weerakkody, E. Ismagilova, U. Sivarajah, Z. Irani, *op. cit.*, p. 303; E. Tan, S. Mahula, J. Crompvoets, *op. cit.*, p. 9.

6 D. Cagigas, J. Clifton, D. Diaz-Fuentes, M. Fernández-Gutiérrez, *op. cit.*, p. 13912; E. Toufaily, T. Zalan, S. Ben Dhaou, "A framework of blockchain technology adoption: An investigation of challenges and expected value", *Information and Management*, vol. 58, no. 3, 2021, 103444, pp. 10–11.

7 S. Ølnes, J. Ubacht, M. Janssen, *op. cit.*, p. 356.

8 M. Janssen, V. Weerakkody, E. Ismagilova, U. Sivarajah, Z. Irani, *op. cit.*, p. 308.

9 Y. Wang, H. Chen, "Blockchain: A potential technology to improve the performance of collaborative emergency management with multi-agent participation", *International Journal of Disaster Risk Reduction*, vol. 72, 2022, 102867, pp. 3–5.

10 D. Marciniak, "The supportive role of non-governmental organisations in sustainable emergency management: The case of Poland", *International Journal of Emergency Management* [forthcom-

direct response to threats. However, there is still a lack of conceptual research and results from the practical implementations of this technology.[11] Therefore, this article aim is to understand blockchain technology's benefits, challenges, and usefulness in emergency management based on previous research and experience in this field.

Research methodology

Although there are examples of blockchain's use in public governance, they are limited, and they were implemented in a short period. Primarily, it is not a well-established research area in emergency management. For this reason, it was decided to use the critical review method in this article.

Generally, "literature reviews are essential to advance the knowledge and understand the breadth of the research on a topic of interest, synthesize the empirical evidence, develop theories or provide a conceptual background for subsequent research, and identify the topics or research domains that require more investigation".[12] Critical reviews are beneficial for analyzing emerging research areas. Although they are interpretative and the selection of sources is often discretionary, their role is to inform and initially outline specific initial research problems.[13] Moreover, critical reviews are not only a synthesis of the existing knowledge, but they analyze it leading to the establishment of propositions or models, which are the starting point for further research.[14]

In the case of this article, the research problem is the question: What are the benefits, challenges, and usefulness of blockchain technology in emergency management processes? Searching for an answer to this research question, a critical review of the characteristics of blockchain technology in emergency management was conducted (Figure 1).

The first step of the research process involves identifying the reasons for implementing blockchain technology in emergency management. Next, analyses of the benefits and challenges of this technology based on the critical review of emergency management theory and blockchain characteristics are conducted. In line with the adopted methodology, propositions and recommendations for theory and practice are established from the conducted critical review.

---

ing]; K. Sienkiewicz-Małyjurek, "Specyfika łańcucha dostaw w procesie zarządzania kryzysowego", *Zeszyty Naukowe Politechniki Śląskiej. Organizacja i Zarządzanie*, vol. 70, 2014, p. 427.

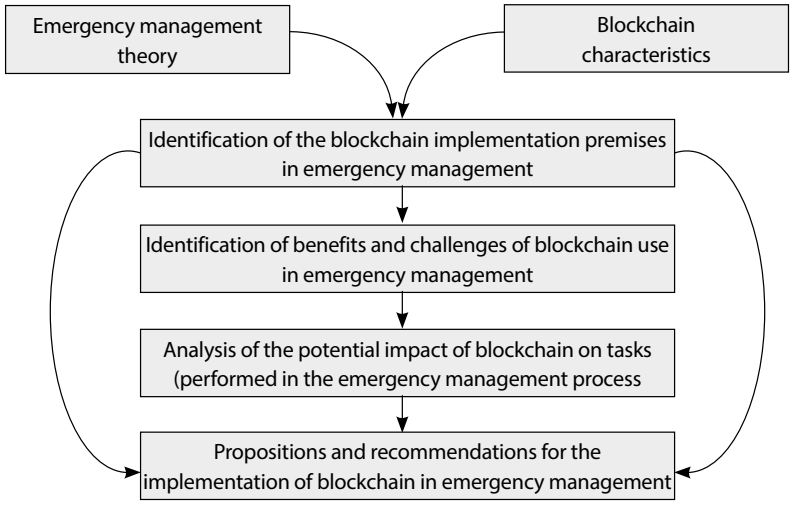
[11] C. L'Hermitte, N.-K.C. Nair, *op. cit*., p. 546; Y. Wang, H. Chen, *op. cit.*, p. 3.

[12] G. Paré, M.-C. Trudel, M. Jaana, S. Kitsiou, "Synthesizing information systems knowledge: A typology of literature reviews" *Information and Management*, vol. 52, no. 2, 2015, p. 183.

[13] M.J. Grant, A. Booth, "A typology of reviews: An analysis of 14 review types and associated methodologies", *Health Information and Libraries Journal*, vol. 26, no. 2, 2009, p. 93; H.M. Cooper, "Organizing knowledge syntheses: A taxonomy of literature reviews", *Knowledge in Society*, vol. 1 no. 1, 1988, pp. 120–121.

[14] G. Paré, M.-C. Trudel, M. Jaana, S. Kitsiou, *op. cit*., p. 189; M.J. Grant, A. Booth, *op. cit.*, p. 93.

Figure 1. Research framework



Source: author's own elaboration.

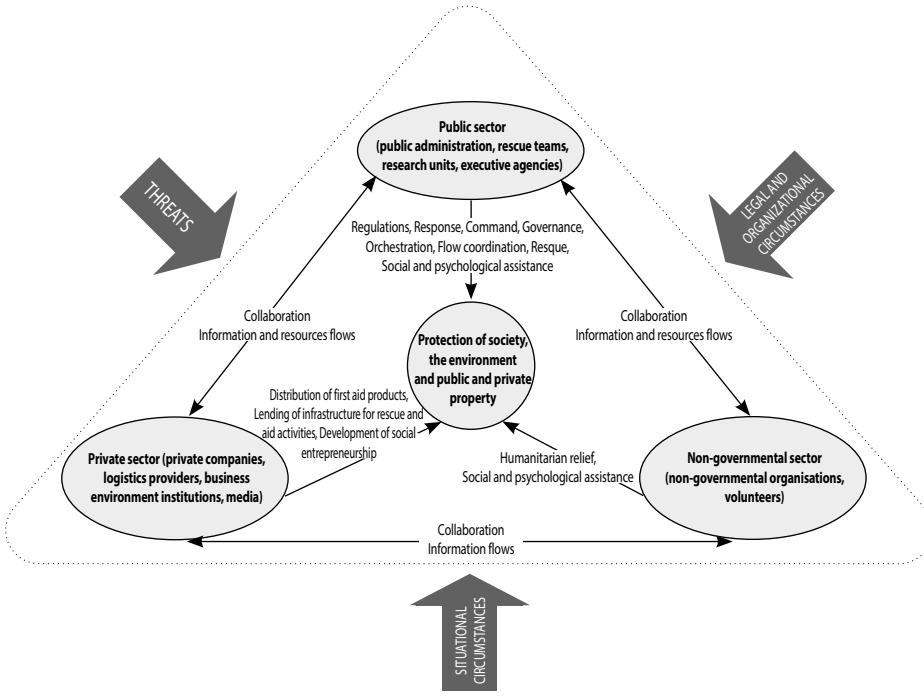
Complexity of emergency management

The nature of emergency management is complex. Activities in this field are implemented by many autonomous actors from all sectors and take place at all state levels. Tasks between public units have been divided according to the statutory competencies of individual organizations in order to ensure collaboration and complementarity of activities.[15] The orchestrators are the relevant public administration bodies, but blue light organizations (police, fire brigade, emergency medical services) play a key role in direct response. Their activities are complemented by other organizations, crucial in a given situation, such as the Building Supervision Inspection, Border Guard, Epidemiological Station, and Gas Emergency. Although public administration bodies are responsible for the entirety of emergency management activities, the participation of organizations from other sectors is also necessary, e.g. to provide a fleet of vehicles for evacuation purposes and other infrastructure to provide temporary accommodation for victims, inform the public about threats and interventions taken, or to obtain additional necessities, e.g. food, clothing, hygiene products. For this reason, actors such as private companies, the media or Red Cross

[15] A. Chodyński, "Sieciowość w zarządzaniu bezpieczeństwem na poziomie regionalnym i lokalnym", *Bezpieczeństwo. Teoria i Praktyka*, vol. 14, no. 1, 2014, p. 19; B. Kożuch, K. Sienkiewicz-Małyjurek, "Mapowanie procesów współpracy międzyorganizacyjnej na przykładzie działań realizowanych w bezpieczeństwie publicznym", *Zarządzanie Publiczne*, no. (3) 31, 2015, pp. 242–243.

and Caritas play an essential role.[16] Therefore, emergency management is collaboration-based, depending on the type of emergency. In each case, even when the same threat occurs, the actions are different because a given emergency occurs in a different place and time, and other people and entities are at risk. As a result, each emergency requires an individual approach. Additionally, threats can accumulate and cascade. The complexity of emergency management is illustrated in Figure 2.

Figure 2. The complexity of emergency management



Source: author's own elaboration.

The structure and flows in emergency management, presented in Figure 2, illustrate its interoperable nature. Protection of society, environment and property requires combining the competencies of organizations from various sectors, reliable and up-to-date information and effective flow of resources. Moreover, emergency management covers both activities before, during and after an emergency. During stabilization, even before the symptoms of an emergency appear, it is possible to plan and prepare activities and resources appropriately. At this time, it is possible to conclude partnership agreements and contracts with private organizations. Actions taken at

[16] D. Marciniak, "Podstawowe problemy wpływające na logistyczne uwarunkowania zarządzania kryzysowego", *Bezpieczeństwo. Teoria i Praktyka*, no. 4, 2020, pp. 111–112; K. Sienkiewicz-Małyjurek, "Specyfika łańcucha dostaw...", *op. cit.*, p. 428.

this time aim to mitigate and prepare for possible threats. The entities participating in actions must mobilize quickly and flexibly react to changes. After the end of an emergency, in the reconstruction phase, there is a gathering of resources to bounce back and even obtain a higher level of resilience and preparation for future threats. This complexity pushes researchers to search for ways to increase the effectiveness of emergency management, and many researchers have high hopes for blockchain.[17]

Benefits and challenges of blockchain technology in emergency management

Blockchain is a "secure public ledger platform shared by all parties through the Internet or an alternative distributed network of computers".[18] It consists of a series of encrypted blocks based on distributed ledger technology, in which data is stored along with the date and links to related blocks.[19] New data, after being entered into the distributed ledger, and all modifications are subject to verification and approval by the entities in the chain. Unconfirmed data is blocked, thus minimizing the risk of introducing false data, unwanted changes, hacking or phishing. All activities in blockchain are also easy to trace for its participants. In addition, the verification and approval of transactions that meet the requirements occur through smart contracts, which are self-executing computer codes that force blockchain users to behave according to the arrangements because different behaviours are not confirmed and accepted.[20] Key blockchain-specific features relevant to emergency management include:[21]

- data security resulting from immutability or verified modification of stored data and transaction sharing; only authorized participants can add, modify, and approve data; in emergency management, this feature replaces the need for inter-organizational trust with data verification and interaction mechanisms;
- transparency on the ability to store and share information with all authorized parties on an open-access basis, where each participant is responsible for their actions and all transactions are digitally signed; this is beneficial for joint decision-making and setting up operational procedures in emergency management;
- decentralization equalizing rights and obligations in the chain and eliminating domination in decision-making processes and central coordination; this

[17] Y. Wang, H. Chen, *op. cit.*, p. 4.

[18] M. Pilkington, Blockchain technology: Principles and applications, [in:] *Research handbook on digital transformations*, eds. F.X. Olleros, M. Zhegu, Cheltenham: Edward Elgar Publishing, 2016, p. 231.

[19] Y. Wang, H. Chen, *op. cit.*, p. 3; E. Tan, S. Mahula, J. Crompvoets, *op. cit.*, p. 2; E. Toufaily, T. Zalan, S. Ben Dhaou, *op. cit.*, pp. 1–2.

[20] F. Lumineau, W. Wang, O. Schilke*, op. cit.*, p. 2.

[21] E. Toufaily, T. Zalan, S. Ben Dhaou, *op. cit.*, p. 3; Y. Wang, H. Chen, *op. cit.*, pp. 7–8*;* F. Lumineau, W. Wang, O. Schilke, *op. cit.*, p. 2.

possibility builds the adaptability of the emergency management network thanks to the spontaneous and quick reaction of individual blocks to threats.

In addition, there are three types of blockchain: public, alliance, and private.[22] The entire society has access to the public blockchain and only a narrow group of participants to the private. By contrast, the alliance blockchain is mixed and seems to be the best solution for multi-agent, joint emergency management from an interoperability perspective. In the case of focusing strictly on communication with the public and co-creation of public value, public blockchain should be more applicable. As a result, the choice of the type of blockchain depends on the purpose of its implementation. Nevertheless, each type is assumed to create conditions for effective inter-organizational and intersectoral collaboration. The main benefits of blockchain and their potential impact on emergency management contains:[23]

1. Collaboration reliability: reducing opportunities for opportunistic behaviour and limited rationality in elections and decision-making, leading to the implementation of actions as agreed; activities are carried out after approval by authorized participants;
2. Facilitating coordination: improving the division of rights, tasks and roles thanks to standard administrative documents and the direct possibility of implementing processes; using blockchain means accepting the established rules and automating them;
3. Communication improvement: equal access to transparent and verified information in real-time thanks to decentralization, openness and collective supervision of this information; the consensus mechanism improves credibility and reduces the dissemination of false information;
4. Ensuring trust: limiting the traditional approach to inter-organizational trust thanks to consensus and sequential recording of information; in blockchain, each participant has equal access to information that is located in secure, shared transaction records, where changes cannot be made without the approval of other authorized participants;
5. Safety of data: the need to verify new data and the changes introduced in it reduces the risk of manipulation of this data; decentralization, the use of multiple databases and authorization of access to them guarantee the integrity of information, reducing the likelihood of security breaches;

---

22 Y. Wang, H. Chen, *op. cit.*, p. 9.

23 D. Cagigas, J. Clifton, D. Diaz-Fuentes, M. Fernández-Gutiérrez, *op. cit.*, pp. 13912–13914; V. Chamola, V. Hassija, V. Gupta, M. Guizani, "A comprehensive review of the COVID-19 pandemic and the role of IoT, drones, AI, blockchain, and 5G in managing its impact", *IEEE Access*, vol. 8, 2020, p. 90245; C. L'Hermitte, N.-K.C. Nair, *op. cit*., p. 536; Y. Wang, H. Chen, *op. cit.*, p. 9*;* F. Lumineau, W. Wang, O. Schilke, *op. cit*., p. 508; S. Ølnes, J. Ubacht, M. Janssen, *op. cit.*, pp. 359–360*;* E. Tan, S. Mahula, J. Crompvoets, *op. cit*., pp. 4–8.

6. Task automation: automated contract execution as agreed simplifies processes and reduces bureaucracy and flaws;
7. Transaction transparency: access to data and transaction history tracking open to participants allows for identification of all necessary information for participants at a given moment and creates responsibility for tasks.

Blockchain can affect the effectiveness of collaborative emergency management by facilitating the management of joint activities and optimizing the technical aspects of collaboration. The possibilities offered by this technology may be of significant importance in emergency management, as they may allow to improve the division of tasks, ensure equal access to current information, and simplify ongoing processes. However, blockchain is new technology if we consider its use in emergency management. The experience with the use of this technology shows that thanks to decentralization, operational transparency and data security, it has the potential to effectively manage complex situations in which many independent entities from various sectors are involved. For this reason, it is assumed that using blockchain on a large scale will be a breakthrough in collaboration. However, this assumption is still not fully empirically verified, and it has not been verified whether the expectations for blockchain are overstated.[24] It is also not recognized what the nature of the changes caused by blockchain implementation will be. However, it was noted that trust depends on the institutional solutions used and not on the blockchain technology itself, which only supports the proper course of processes and their control but does not guarantee the reliability of the information entered.[25] As a result, implementing and adequately using blockchain will be easier for countries with higher-quality institutional and legal solutions and highly qualified staff. Such challenges mean that more and more researchers pay attention to the problems and limitations related to the use of this technology. They include:[26]

1. No legal regulations: Problems may be related to the scope of blockchain use in emergency management and the information that can be made available as part of this technology. Without appropriate policies and procedures, participants of collaborative emergency management will not know the transparent rules of using blockchain and will not fully use it, or vice versa – they may exceed applicable regulations.
2. The potential concentration of power in the hands of a small group of people: Specialized knowledge is required to manage blockchain processes, and people supervising this technology can dictate how it is used and modify codes and rules.

---

[24] F. Lumineau, W. Wang, O. Schilke, *op. cit*., p. 514; Y. Wang, H. Chen, *op. cit.*, p. 11.

[25] S. Ølnes, J. Ubacht, M. Janssen, *op. cit.*, p. 362*;* D. Cagigas, J. Clifton, D. Diaz-Fuentes, M. Fernández-Gutiérrez, *op. cit.*, p. 13915.

[26] D. Cagigas, J. Clifton, D. Diaz-Fuentes, M. Fernández-Gutiérrez, *op. cit.*, pp. 13912–13915; M. Janssen, V. Weerakkody, E. Ismagilova, U. Sivarajah, Z. Irani, *op. cit.*, p. 306*;*. F. Lumineau, W. Wang, O. Schilke*, op. cit*., pp. 509–511; E. Tan, S. Mahula, J. Crompvoets, *op. cit*., pp. 4–8.

Therefore, there is a risk of limiting decentralization in operations and decision-making, which may result in top-down control.

3. Lack of awareness and knowledge: Many people still associate blockchain with only Bitcoin and criminal activities. In addition, few people know how to use it. In emergency management, implementing blockchain would require the involvement of decision-makers and users and their appropriate training; it is related to economic and social limitations.
4. Economic and social costs: Like any technology, blockchain requires investment in technical measures and the integration of distributed systems, as well as training the people who will use it. In emergency management, collaboration is not only inter-institutional, as private sector organizations and non-governmental organizations, the media, and the public also participate in the activities. The solution could be to implement blockchain in the first place in order to facilitate inter-institutional collaboration (private chain) and then its gradual extension to other sectors (alliance chain). Another solution could be to implement a public chain for communicating with the public and building social responsibility in emergency management in the first place.
5. Replacing people's work with automated processes: There is a view that easy and repetitive work will be automated thanks to blockchain implementation. However, the specificity of emergency management makes each situation unique and requires an individual approach. Moreover, actions taken in this area require continuous, ongoing decision-making, adequate to the situation. Therefore, at present, this threat does not seem to be significant. It is possible that after integrating blockchain with artificial intelligence, there will be prospects of replacing human work with machines, which in dangerous conditions may have a positive meaning.
6. It is not possible to verify the authenticity of the entered information: The quality of the data entered into the blockchain depends on the participants of that chain. The technology itself only facilitates the flow of processes based on existing information. If the entered data is inaccurate, incomplete or false, it will have a critical impact on the course of emergency management activities. This threat also makes people realize that it is impossible to replace trust with blockchain technology completely. Parties must trust the information entered into the chain, its nodes, and those who manage this technology.
7. Inability to codify tacit knowledge: Along with the increase in the tacitness of data, the possibility of its codification decreases. This limitation is a significant challenge in emergency management because a large part of the activities in this area is based on experience and is tacit knowledge. The situational uniqueness of emergency management also limits the possibility of codifying knowledge because there are many factors influencing decision-making in a given situation, and not all of them can be codified.

8. Not fully resilience to attacks: It is not possible to eliminate the vulnerability to attacks completely. In addition, decentralization may lead to additional weak links in the chain. In emergency management, such problems can limit the interoperability between participants in a private blockchain. In a public blockchain, attacks can cause information chaos.
9. Scalability limitation: Blockchain is limited by the scale and speed at which it can process transactions. It takes time to place data and verify it between nodes, which increases as the number of validating links increases. Additionally, their propagation speed decreases as the blocks' size increases. In the response phase of emergency management, units need to process a huge amount of information per second.
10. Limited possibilities of blockchain integration with legacy technologies: An interoperable infrastructure is needed for blockchain functionality. Technologies implemented in an earlier period may not be compatible and may need to be adjusted accordingly to ensure their interoperability. In emergency management, each unit uses its own operating system, and not all of these systems are always compatible. However, it is also possible to implement blockchain with incomplete functionality, to perform specific functions, e.g. communication with the society and co-creation of public value in the form of a public chain or in the form of an alliance or private chain for joint decision-making, communication and information transfer.

Although blockchain can significantly improve inter-organizational activities in emergency management, the problems that may arise during its use force units to think about its effectiveness. The benefits listed earlier indicate that blockchain can improve operations and reduce problems resulting from the complexity of emergency management. On the other hand, many challenges may limit potential benefits. For this reason, it is worth noting that blockchain requires appropriate management by competent people and institutional and social embedding.[27]

Blockchain in the emergency management process

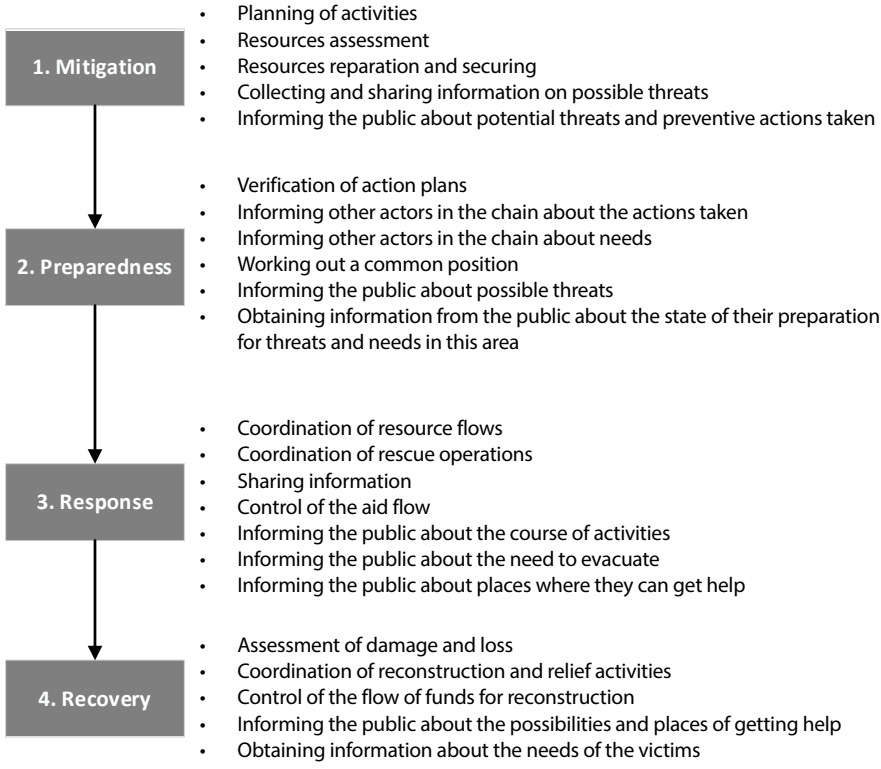
The possibilities of using blockchain in emergency management are broad, ranging from sharing information to planning and supporting the implementation of complex projects. Wang and Chen[28] believe this system can be helpful in communication and emergency resource management. For example, the World Food Program (WFP) used blockchain to deliver coupons to Syrian refugees.[29] The technology has also found application in tracking and obtaining reliable real-time informa-

[27] S. Ølnes, J. Ubacht, M. Janssen, *op. cit.*, p. 360.
[28] Wang, H. Chen, *op. cit.*, p. 10.
[29] F. Lumineau, W. Wang, O. Schilke, *op. cit*., p. 515.

tion on the spread of the COVID-19 virus, coordinating clinical trials for vaccines and drugs, and raising funds for research and the fight against the virus.[30] Ølnes et al.[31] also indicate the usefulness of blockchain in managing mass events that require the cooperation of event organizers with city authorities, blue light organizations, private security companies, building managers, etc. Due to the significant utility of blockchain in managing distributed data, this technology can also be used to manage critical infrastructure. It can help track changes in protecting this infrastructure and spread information about emerging threats.

As seen from the above examples, there are many possibilities for using blockchain, but they depend on the phase of emergency management and the specificity of a given threat. Examples of blockchain technology's usefulness in the emergency management process are presented in Figure 3.

Figure 3. Examples of blockchain technology's usefulness in the emergency management process



Source: author's own elaboration.

[30] H. Wang, "Public health emergency decision-making and management system sound research using rough set attribute reduction and blockchain", *Scientific Reports*, vol. 12, no. 1, 2022, 3600, p. 10.

[31] S. Ølnes, J. Ubacht, M. Janssen, *op. cit.*, p. 357.

In the mitigation phase, thanks to obtaining reliable data from many dispersed sources, blockchain can facilitate the preparation of actions adequate to real threats. It can also favour the creation of decentralized working teams enabling direct and immediate reaction to emerging threats. Blockchain is also significant in the preparedness phase in improving communication, mobilizing resources, and alerting society. Thanks to its use, local societies can not only prepare for threats but also mobilize to participate, e.g. in the form of volunteering. In the response phase, thanks to the automation and simplification of procedures, blockchain can create opportunities to eliminate duplication of activities and allow access to information about currently performed tasks, thus facilitating their coordination. However, due to the dynamics of changes and time pressure, blockchain limitations related to scalability must also be considered. This bottleneck may be important because lack of time is the norm in the response phase. Waiting for data to be sent and verified may further delay decision-making and action implementation processes. In the recovery phase, blockchain can facilitate coordination and control of resource flows. It is the longest phase of emergency management, carried out under less time pressure than the response phase. For this reason, the limitation of scalability will not have such a significant impact on the actions taken. The key utility of blockchain in the recovery phase may include gathering and managing information and resources from multiple dispersed sources to ensure adequate recovery, as well as helping the society to obtain aid.

Conclusion

Blockchain still requires intensive research. It offers great benefits in emergency management but also brings challenges that need to be solved. Moreover, the readiness of the government to reduce its role and decentralize emergency management has great importance. The technical ability to guarantee safe transactions cannot be overestimated either. These parameters are essential because, after deciding to implement blockchain, the government should choose the type of blockchain and to what extent it should be implemented. This technology will not have the expected functionality if central control is maintained. Analyses conducted in this article lead to three main propositions requiring empirical verification:

1. Blockchain can significantly improve communication processes in emergency management, both between organizations involved in conducting activities and with the society, if its full functionality is ensured.
2. By ensuring transparency and decentralization of decision-making processes, blockchain can increase the efficiency of operational processes, including managing mass events and critical infrastructure, as well as conducting rescue, evacuation and humanitarian aid activities.

3. In the longer term, public blockchain may also contribute to increasing the effectiveness of the process of co-creating public value in emergency management by increasing the level of public involvement in activities in this area.

In addition, the analysis carried out allows the following recommendations to be formulated:

1. There is a need to create a legal basis enabling the use and governance of blockchain in emergency management.
2. It is advisable to carry out an analysis of case studies of the use of blockchain in emergency management in order to identify good practices.
3. It is necessary to develop human resources in the use and management of blockchain.
4. It is advisable to prepare projects for the implementation and use of blockchain in individual phases of emergency management and even in the entire process.
5. It is necessary to develop reliable technical solutions to minimize the risk of introducing false information and data loss and increase the scalability and the possibility of blockchain integration with other systems.

The above recommendations result from the fact that blockchain needs appropriate management, adapted to the context in which it will be used. Adequate knowledge about the functionality of this technology and how to use it is necessary to ensure this requirement. Otherwise, the blockchain may not be used at all. The threats are also related to using the blockchain, including the possibility of failure occurrence, management of sensitive data, and technological alienation. For this reason, it is necessary to ensure appropriate legal regulations and organizational framework allowing full and transparent implementation of processes. Blockchain is a very prospective technology that can significantly improve emergency management processes; however, in the first place, it requires appropriate organization and embedding in the existing conditions.

References

Cagigas D., Clifton J., Diaz-Fuentes D., Fernández-Gutiérrez M., "Blockchain for Public Services: A systematic literature review", *IEEE Access*, vol. 9, 2021, pp. 13904–13921.

Chamola V., Hassija V., Gupta V., Guizani M., "A comprehensive review of the COVID-19 pandemic and the role of IoT, drones, AI, blockchain, and 5G in managing its impact", *IEEE Access*, vol. 8, 2020, pp. 90225–90265.

Chodyński A., "Sieciowość w zarządzaniu bezpieczeństwem na poziomie regionalnym i lokalnym", *Bezpieczeństwo. Teoria i Praktyka*, vol. 14, no. 1, 2014, pp. 13–27.

Cooper H.M., "Organizing knowledge syntheses: A taxonomy of literature reviews", *Knowledge in Society*, vol. 1, no. 1, 1988, pp. 104–126.

Grant M.J., Booth A., "A typology of reviews: An analysis of 14 review types and associated methodologies", *Health Information and Libraries Journal,* vol. 26, no. 2, 2009, pp. 91–108.

Janssen M., Weerakkody V., Ismagilova E., Sivarajah U., Irani Z., "A framework for analysing blockchain technology adoption: Integrating institutional, market and technical factors", *International Journal of Information Management*, vol. 50, 2020, pp. 302–309.

Kożuch B., Sienkiewicz-Małyjurek K., "Mapowanie procesów współpracy międzyorganizacyjnej na przykładzie działań realizowanych w bezpieczeństwie publicznym", *Zarządzanie Publiczne*, no. (3) 31, 2015, pp. 237–253.

L'Hermitte C., Nair N.-K.C., "A blockchain-enabled framework for sharing logistics resources during emergency operations", *Disasters*, vol. 45, no. 3, 2021, pp. 527–554.

Lumineau F., Wang W., Schilke O., "Blockchain governance – A new way of organizing collaborations?", *Organization Science*, vol. 32, no. 2, 2021, pp. 500–521.

Marciniak D., "Podstawowe problemy wpływające na logistyczne uwarunkowania zarządzania kryzysowego", *Bezpieczeństwo. Teoria i Praktyka*, no. 4, 2020, pp. 109–124.

Marciniak D., "The supportive role of non-governmental organisations in sustainable emergency management: The case of Poland", *International Journal of Emergency Management* [forthcoming].

Ølnes S., Ubacht J., Janssen M., "Blockchain in government: Benefits and implications of distributed ledger technology for information sharing", *Government Information Quarterly*, vol. 34, no. 3, 2017, pp. 355–364.

Paré G., Trudel M.-C., Jaana M., Kitsiou S., "Synthesizing information systems knowledge: A typology of literature reviews", *Information and Management*, vol. 52, no. 2, 2015, pp. 183–199.

Pilkington M., Blockchain technology: Principles and applications, [in:] *Research handbook on digital transformations*, eds. F.X. Olleros, M. Zhegu, Cheltenham: Edward Elgar Publishing, 2016, pp. 225–253.

Samir E., Azab M., Jung Y., "Blockchain Guided Trustworthy Interactions for Distributed Disaster Management", *IEEE 10th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*, 2019, pp. 241–245, https://ieeexplore.ieee.org/document/8936147 [accessed: 31 October 2022].

Sienkiewicz-Małyjurek K., "Specyfika łańcucha dostaw w procesie zarządzania kryzysowego", *Zeszyty Naukowe Politechniki Śląskiej. Organizacja i Zarządzanie*, vol. 70, 2014, pp. 425–436.

Tan E., Mahula S., Crompvoets J., "Blockchain governance in the public sector: A conceptual framework for public management", *Government Information Quarterly*, vol. 39, no. 1, 2022, 101625.

Tapscott D., Tapscott A., *Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money Business and the World*, New York: Portfolio-Penguin, 2016.

Toufaily E., Zalan T., Ben Dhaou S., "A framework of blockchain technology adoption: An investigation of challenges and expected value", *Information and Management*, vol. 58, no. 3, 2021, 103444.

Wang H., "Public health emergency decision-making and management system sound research using rough set attribute reduction and blockchain", *Scientific Reports*, vol. 12, no. 1, 2022, 3600.

Wang Y., Chen H., "Blockchain: A potential technology to improve the performance of collaborative emergency management with multi-agent participation", *International Journal of Disaster Risk Reduction*, vol. 72, 2022, 102867.

Benefits, challenges, and perspectives of using the blockchain technology in emergency management

Abstract

The potential of blockchain causes more researchers to postulate this technology's use in public governance. Due to the specificity and complexity of emergency management, blockchain may have particular importance in this area. On the other hand, there are many challenges related to the implementation and use of this technology. Therefore, this article aim is to understand blockchain technology's benefits, challenges, and usefulness in emergency management based on previous research and experience in this field. The perspectives and challenges of using blockchain were analyzed based on the complexity of emergency management. As a result, this article presents how blockchain can contribute to the improvement of emergency management processes.

Key words: blockchain, emergency management, complexity, threats, technology

BEZPIECZEŃSTWO TEORIA I PRAKTYKA SECURITY THEORY AND PRACTICE
e-ISSN 2451-0718
ISSN 1899-6264
2022
No. 2 (XLVII)
DOI: 10.48269/2451-0718-btip-2022-2-002
Received: 23.05.2022
Accepted: 20.07.2022

Krzysztof Waśniewski
PhD, Andrzej Frycz Modrzewski Krakow University
https://orcid.org/0000-0003-0076-4804

The management of distributed energy resources for national security

Introduction

Today, just as it used to be in the past, innovation and technological change are key issues for national security.[1] As a civilization, we seem to be experiencing, right now, an episode of technological breakthrough and social discontinuity. New technologies become new targets, new weapons, and new fields of vulnerability, which is reflected, among others, in the concept of systemic war.[2]

National energy systems can be targets and are vulnerable. When the critical infrastructure of energy systems is under imminent threat of systemic failure due to the projection of military force, managing energy security means finding ways of assuring maximum resilience. Different spatial distributions of power-generating and energy-storing facilities are conducive to different exposures of the national energy system to exogenous risks such as war. That kept in mind, technological advancements as regards energy resources have been creating new areas of international conflict since at least 2014; e.g. new geotechnologies bring the discovery of new offshore oil and gas fields, which, in turn, brings new international tensions as regards the actual control over those reserves.[3]

---

1 V. Levchenko, A. Boiko, T. Savchenko *et al.*, "State regulation of the economic security by applying the innovative approach to its assessment", *Marketing and Management of Innovations*, vol. 10, no. 4, 2019, pp. 364–372.

2 E.A. Colby, *The Strategy of Denial: American Defense in An Age of Great Power Conflict*, New Haven: Yale University Press, 2021, pp. 23–26.

3 R. Dannreuther, *Energy security*, Hoboken, NJ: John Wiley & Sons, 2017, pp. 101–122; N. Mazzucchi, *Énergie: Ressources, Technologies et Enjeux de Pouvoir*, Paris: Armand Colin, 2017, pp. 55–134.

Assuring energy security is one of the most basic missions of national governments.[4] Still, it remains the weak spot of most countries. Less than 25% of countries on the planet have national energy systems endowed with high resilience to exogenous shocks and change in that domain is slow because of significant hysteresis.[5] Distributed energy resources (DER) are one of the ways to make the national energy system more resilient. Small power installations distributed across local communities, are unlikely to be all incapacitated at the same moment, whilst one big power plant can be shut down at once, e.g. by an adversary attack.[6]

The purpose of this article is to pass in review the principal angles of scientific approach to the deployment of DER, and therefore to assess the way that scientific research is being done on that topic. Review of literature and meta-analysis are the main conceptual tools used. The expected outcome of that analysis is to define fields, which either require further research or raise doubts as for the practical utility of the research done so far.

The technological state of the art in distributed energy resources

All the essential technologies for DER seem to be available and tested at the industrial scale. DER systems prove to be workable solutions in very different conditions of physical geography.[7] Technological progress goes even as far as allowing self-charging in local power installations by harvesting surpluses of energy.[8] DER systems are complex technologies. Two basic models can be distinguished in literature as for modelling that complexity: the remote island and the virtual power plant. The model of remote island[9] studies DER systems in hypothetical situations, when country-wide disruptions in power supply turn specific areas into de-facto islands, i.e. places either completely cut from external supplies or exposed to severe uncertainty in that respect, both isolation and uncertainty determined essentially by exogenous factors. In such an island-like case, a power system is based on one

4 E. Bompard, A. Carpignano, M. Erriquez *et al.*, "National energy security assessment in a geopolitical perspective", *Energy*, vol. 130, 2017, pp. 144–154.

5 Q. Wang, K. Zhou, "A framework for evaluating global national energy security", *Applied Energy*, vol. 188, 2017, pp. 19–31.

6 P. Kivimaa, M.H. Sivonen, "Interplay between low-carbon energy transitions and national security: An analysis of policy integration and coherence in Estonia, Finland and Scotland", *Energy Research & Social Science*, vol. 75, 2021, 102024.

7 N. McIlwaine, A.M. Foley, D.J. Morrow *et al.*, "A state-of-the-art techno-economic review of distributed and embedded energy storage for energy systems", *Energy*, vol. 229, 2021, 120461.

8 X. Pu, Z.L. Wang, "Self-charging power system for distributed energy: Beyond the energy storage unit", *Chemical Science*, vol. 12, no. 1, 2021, pp. 34–49.

9 L. Feng, X. Zhang, X. Li *et al.*, "Performance analysis of hybrid energy storage integrated with distributed renewable energy", *Energy Reports*, vol. 8, 2022, pp. 1829–1838.

or more microgrids. Distributed installations of renewable energy (mostly photovoltaic and wind) are combined with hybrid energy storage. The latter comprises lithium-ion batteries, super capacitors, and compressed air energy storage (CAES). Adding storage technologies other than just batteries seems to: a) lower the cost of energy for end-users b) improve stability in the system.

The model of virtual power plant (VPP) was brought forth in the late 1990s,[10] and takes a tangent opposite to that of the remote island paradigm: flexible, market-based cooperation between many independent agents with local installations of generation and storage can be studied as one big power plant with many component parts in it. Sikorski et al. demonstrate the working of the VPP framework in a network of 1 MW hydro-electric turbines, coupled with 0,5 MW battery-based energy storage.[11] An interesting finding of that study is that distributed energy systems can be a burden for larger power grids, as they generate rapid changes in voltage. Combining local generation of energy from renewable sources with the technologies of energy storage seems to use the best of both. Local energy storage allows curtailing the inherent volatility of supply in energy from renewable sources, whilst using renewable sources to charge those energy-storage devices solves the problem of secondary load put on a typical power grid when end users start storing energy.[12]

The economics of distributed energy resources

Apparently, distributed networks of energy resources can lead to solutions which are economically far from optimal; e.g., distributed energy storage facilities can destabilize the high-voltage power grid instead of stabilizing it, as individual owners of such installations start arbitering in the market of energy.[13] Market-based solutions, where intelligent devices installed at the level of individual installations, coordinate with each other using monetary value as the baseline semantics for communication, seem promising to optimize economic efficiency of distributed energy systems.[14]

---

[10] *The Virtual Utility: Accounting, technology & competitive aspects of the emerging industry*, eds. S. Awerbuch, A. Preston, Boston, MA Springer, 1997.

[11] T. Sikorski, M. Jasiński, E. Ropuszyńska-Surma *et al.*, "A case study on distributed energy resources and energy-storage systems in a virtual power plant concept: Technical aspects", *Energies*, vol. 13, no. 12, 2020, 3086.

[12] W. Zheng, B. Zou, "Evaluation of intermittent-distributed-generation hosting capability of a distribution system with integrated energy-storage systems", *Global Energy Interconnection*, vol. 4, no. 4, 2021, pp. 415–424; C. Silva, P. Faria, A. Fernandes, Z. Vale, "Clustering distributed Energy Storage units for the aggregation of optimized local solar energy", *Energy Reports*, vol. 8, suppl. 3, 2022, pp. 405–410.

[13] B. Zakeri, G.C. Gissey, P.E. Dodds, D. Subkhankulova, "Centralized vs. distributed energy storage: Benefits for residential users", *Energy*, vol. 236, 2021, 121443.

[14] P. Hou, G. Yang, J. Hu *et al.*, "A distributed transactive energy mechanism for integrating PV and storage prosumers in market operation", *Engineering*, vol. 12, 2022, pp. 171–182.

Distributed systems of power installations can be studied as intelligent structures and therefore simulate their collective behaviour with artificial intelligence. There is substantial evidence that DER systems display intelligent learning with reinforcement, which, in turn, allows assuming the importance of market-based incentives in the deployment and current management of such systems.[15]

Intelligent collective learning is a valuable cognitive perspective for understanding the behaviour of DER systems, yet there remains the issue of their linear predictability. We need to predict accurately the aggregate need for investment in capacity of generation and storage. Xia et al.[16] argue that such a system becomes linearly predictable only in the presence of both the positive and the negative behavioural reinforcement: there needs to be a system of rewards for playing fair in the network, and punishments for opportunistic behaviour. On the other hand, Sidnell et al.[17] provide evidence that linear predictability of distributed energy systems is strongly sensitive to the catalogue of technologies on both the demand and the supply side of the local energy market, such as inter-house connections through pipes with hot water, or air conditioning in households. Somewhere between the approach based on intelligent collective learning and that referring to linear prediction one can find stochastic methods based on alternative scenarios. Those scenarios include both short-term flexibility and long-term uncertainty, for a given catalogue of technologies used in a distributed energy system, which allows using weak, non-deterministic assumptions and thus insulating the resulting predictions from the impact of false assumptions.[18] Interestingly, this methodology is consistent with much earlier ones, which makes it familiar for many practitioners of the energy industry.[19]

---

15 S. Touzani, A.K. Prakash, Z. Wang *et al.*, "Controlling distributed energy resources via deep reinforcement learning for load flexibility and energy efficiency", *Applied Energy*, vol. 304, 2021, 117733; R. Haider, D. D'Achiardi, V. Venkataramanan *et al.*, "Reinventing the utility for distributed energy resources: A proposal for retail electricity markets", *Advances in Applied Energy*, vol. 2, 2021, 100026; S. Zhang, D. May, M. Gül, P. Musilek, "Reinforcement learning-driven local transactive energy market for distributed energy resources", *Energy and AI*, vol. 8, 2022, 100150.

16 Y. Xia, Q. Xu, H. Qian, L. Cai, "Peer-to-Peer energy trading considering the output uncertainty of distributed energy resources", *Energy Reports*, vol. 8, suppl. 1, 2022, pp. 567–574.

17 T. Sidnell, F. Clarke, B. Dorneanu *et al.*, "Optimal design and operation of distributed energy resources systems for residential neighbourhoods", *Smart Energy*, vol. 4, 2021, 100049.

18 A. Flores-Quiroz, K. Strunz, "A distributed computing framework for multi-stage stochastic planning of renewable power systems with energy storage as flexibility option", *Applied Energy*, vol. 291, 2021, 116736.

19 S. Jin, S.M. Ryan, J.-P. Watson, D.L. Woodruff, "Modeling and solving a large-scale generation expansion planning problem under uncertainty", *Energy Systems*, vol. 2, no. 3, 2011, pp. 209–242; Y. Feng, S.M. Ryan, "Scenario construction and reduction applied to stochastic power generation expansion planning", *Computers & Operations Research*, vol. 40, no. 1, 2013, pp. 9–23.

The actual resilience of distributed energy resources

The resilience of DER systems, such as they are designed presently, seems promising, which is substantiated by studies of DER systems in areas afflicted with frequent local blackouts.[20] Still, when resilience is considered for extreme conditions, such as war, DER systems present two major weaknesses. Firstly, they are sensitive to the working of supply chains. Dispersed structures of this type generate a steady demand for maintenance services, which includes spare parts. Disturbances in supply chains are highly impactful when emergency situations last longer than the maintenance cycle.[21] Secondly, DER systems are closely connected to digital platforms that facilitate coordination between local installations.[22] The technology of digital cloud seems to be promising in that respect, especially as regards reducing peaks and valleys in demand for energy, and the underlying logic consists in mirroring a cloud of shared energy with a digital cloud, in a local network of small installations.[23] As those digital technologies allow creating country-wide platforms for smartly trading local surpluses of energy, local power installations must become partly accessible digitally from remote locations. That creates a meta-risk of systemic failure in the digital network that underpins the national power system.[24]

When distributed energy systems are based on local installations combining renewable sources of energy (photovoltaic & wind) with battery-based energy storage, they seem to change the economic role of low-voltage networks (LV) and the way they work. Wasiak et al.[25] present a controlled experimental environment for reli-

---

20 R. Wu, G. Sansavini, "Energy trilemma in active distribution network design: Balancing affordability, sustainability and security in optimization-based decision-making", *Applied Energy*, vol. 304, 2021, 117891.

21 D.M. López González, J. Garcia Rendon, "Opportunities and challenges of mainstreaming distributed energy resources towards the transition to more efficient and resilient energy markets", *Renewable and Sustainable Energy Reviews*, vol. 157, 2022, 112018; D.M. Maschio, B. Duarte, A.E. Lazzaretti *et al.*, "An event-driven approach for resources planning in distributed power generation systems", *International Journal of Electrical Power & Energy Systems*, vol. 137, 2022, 107768.

22 V. Tikka, A. Mashlakov, A. Kulmala *et al.*, "Integrated business platform of distributed energy resources – Case Finland", *Energy Procedia*, vol. 158, 2019, pp. 6637–6644.

23 T. Yan, J. Liu, Q. Niu *et al.*, "Distributed energy storage node controller and control strategy based on energy storage cloud platform architecture", *Global Energy Interconnection*, vol. 3, no. 2, 2020, pp. 166–174.

24 S. Howell, Y. Rezgui, J.-L. Hippolyte *et al.*, "Towards the next generation of smart grids: Semantic and holonic multi-agent management of distributed energy resources", *Renewable and Sustainable Energy Reviews*, vol. 77, 2017, pp. 193–214; S. Pazouki, E. Naderi, A. Asrari, "A remedial action framework against cyberattacks targeting energy hubs integrated with distributed energy resources", *Applied Energy*, vol. 304, 2021, 117895.

25 I. Wasiak, M. Szypowski, P. Kelm *et al.*, "Innovative energy management system for low-voltage networks with distributed generation based on prosumers' active participation", *Applied Energy*, vol. 312, 2022, 118705.

able testing of the above issues, where controllable devices located in prosumers' installations allow generating ancillary services with energy and minimizing the use of storage capacities for voltage regulation.

Conclusion

The management of DER systems, with a strong orientation on national security, needs to account for the collectively intelligent nature of networks that make DER systems. Individual local installations in a system of distributed energy resources, together with their local operators, form a collectively intelligent social structure. This, in turn, allows using the theory of complex systems (aka complexity theory) as conceptual framework for managing DER systems. Complexity theory can be traced back to the works of Herbert Simon, who argued that big sets of heterogenous phenomena spontaneously generate meta-structures of coordination, after reaching a critical size. It is possible to study social systems as hierarchies of emergent coordination structures, stacked upon one another.[26] In its more modern version, complexity theory forms the theoretical base for simulating alternative states of a given social system with the help of artificial intelligence. The essential assumption is that apparently random actions in component entities of the system produce, in the same system, both patterned behaviours, and meta-structures of coordination.[27]

From the perspective of management, and once we assume that DER systems are emergent structures, collective intelligence in DER works mostly by imitation and coordination between individual agents, with markets being important mediators in that coordination. Models such as the ants' colony seem particularly suitable for rigorous quantitative simulations of collectively intelligent adaptation in the population of participants in DER networks.[28]

---

[26] H.A. Simon, "The architecture of complexity", *Proceedings of the American Philosophical Society*, vol. 106, no. 6, 1962, pp. 467–482; P.W. Anderson, "More is different: Broken symmetry and the nature of the hierarchical structure of science", *Science*, vol. 177, no. 4047, 1972, pp. 393–396.

[27] P.C. Anderson, A. Meyer, Complexity theory and process organization studies, [in:] *SAGE Handbook of Process Organization Studies*, eds. A. Langley, H. Tsoukas, Thousand Oaks, CA: SAGE Publications Ltd, 2016, pp. 127–143; J. Ladyman, K. Wiesner, *What Is a Complex System?*, New Haven, CT: Yale University Press, 2020, Kindle Edition, p. 15–17.

[28] A. Gupta, S. Srivastava, "Comparative analysis of ant colony and particle swarm optimization algorithms for distance optimization", *Procedia Computer Science*, vol. 173, 2020, pp. 245–253; D. Di Caprio, A. Ebrahimnejad, H. Alrezaamiri, F.J. Santos-Arteaga, "A novel ant colony algorithm for solving shortest path problems with fuzzy arc weights", *Alexandria Engineering Journal*, vol. 61, no. 5, 2021, pp. 3403–3415.

Using complexity theory involves an essentially non-commanding approach to the management of DER systems. It is hardly conceivable to develop a viable and resilient DER system just by the fiat of the government, communicated top-down through the social structure. The deployment of distributed energy resources can be achieved only through creating market-based communities of exchange. The most critical factor to manage in DER systems seems to be the stability and viability of supply chains. Efficient, resilient supply chains of spare parts and technical services are necessary to maintain dispersed energy resources at a state-of-the-art technological advancement, and, at the same time, crucial to their economic and environmental sustainability.

There is substantial evidence that businesses exposed to supply-chain-related risks develop very risk-specific strategies to manage those contingencies. However, the strategy of the type "Control, Share and Transfer" seems to override significantly other types of risk-management strategies.[29] This, in turn, means that proper management of supply-chain-related risk relative to distributed energy systems involves, most of all, the development of proper financial instruments and markets: insurance contracts, specific types of financial securities, and workable forms of business association (partnerships and companies). That corroborates the need for approaching the management of DER systems from the perspective of complexity theory: financial markets are hardly manageable in a top-down manner.

References

Anderson P.C., Meyer A., Complexity theory and process organization studies, [in:] *SAGE Handbook of Process Organization Studies*, eds. A. Langley, H. Tsoukas, Thousand Oaks, CA: SAGE Publications Ltd, 2016, pp. 127–143.

Anderson P.W., "More is different: Broken symmetry and the nature of the hierarchical structure of science", *Science*, vol. 177, no. 4047, 1972, pp. 393–396.

Bompard E., Carpignano A., Erriquez M. *et al.*, "National energy security assessment in a geopolitical perspective", *Energy*, vol. 130, 2017, pp. 144–154, https://doi.org/10.1016/j.energy.2017.04.108.

Colby E.A., *The Strategy of Denial: American Defense in An Age of Great Power Conflict*, New Haven: Yale University Press, 2021.

Dannreuther R., *Energy security*, Hoboken, NJ: John Wiley & Sons, 2017.

Di Caprio D., Ebrahimnejad A., Alrezaamiri H., Santos-Arteaga F.J., "A novel ant colony algorithm for solving shortest path problems with fuzzy arc weights", *Alexandria Engineering Journal*, vol. 61, no. 5, 2021, pp. 3403–3415, https://doi.org/10.1016/j.aej.2021.08.058.

Feng Y., Ryan S.M., "Scenario construction and reduction applied to stochastic power generation expansion planning", *Computers & Operations Research*, vol. 40, no. 1, 2013, pp. 9–23, http://dx.doi.org/10.1016/j.cor.2012.05.005.

[29] Ç. Sofyalıoğlu, B. Kartal, "The Selection of Global Supply Chain Risk Management Strategies by Using Fuzzy Analytical Hierarchy Process – A Case from Turkey", *Procedia – Social and Behavioral Sciences*, vol. 58, 2012, pp. 1448–1457.

Feng L., Zhang X., Li X. *et al.*, "Performance analysis of hybrid energy storage integrated with distributed renewable energy", *Energy Reports*, vol. 8, 2022, pp. 1829–1838, https://doi.org/10.1016/j.egyr.2021.12.078.

Flores-Quiroz A., Strunz K., "A distributed computing framework for multi-stage stochastic planning of renewable power systems with energy storage as flexibility option", *Applied Energy*, vol. 291, 2021, 116736, https://doi.org/10.1016/j.apenergy.2021.116736.

Gupta A., Srivastava S., "Comparative analysis of ant colony and particle swarm optimization algorithms for distance optimization", *Procedia Computer Science*, vol. 173, 2020, pp. 245–253, https://doi.org/10.1016/j.procs.2020.06.029.

Haider R., D'Achiardi D., Venkataramanan V., "Reinventing the utility for distributed energy resources: A proposal for retail electricity markets", *Advances in Applied Energy*, vol. 2, 2021, 100026, https://doi.org/10.1016/j.adapen.2021.100026.

Hou P., Yang G., Hu J. *et al.*, "A distributed transactive energy mechanism for integrating PV and storage prosumers in market operation", *Engineering*, vol. 12, 2022, pp. 171–182, https://doi.org/10.1016/j.eng.2022.03.001.

Howell S., Rezgui Y., Hippolyte J.-L. *et al.*, "Towards the next generation of smart grids: Semantic and holonic multi-agent management of distributed energy resources", *Renewable and Sustainable Energy Reviews*, vol. 77, 2017, pp. 193–214, http://dx.doi.org/10.1016/j.rser.2017.03.107.

Jin S., Ryan S.M., Watson J.-P., Woodruff D.L., "Modeling and solving a large-scale generation expansion planning problem under uncertainty", *Energy Systems*, vol. 2, no. 3, 2011, pp. 209–242, http://dx.doi.org/10.1007/s12667- 011-0042-9.

Kivimaa P., Sivonen M.H., "Interplay between low-carbon energy transitions and national security: An analysis of policy integration and coherence in Estonia, Finland and Scotland", *Energy Research & Social Science*, vol. 75, 2021, 102024, https://doi.org/10.1016/j.erss.2021.102024.

Ladyman J., Wiesner K., *What Is a Complex System?*, New Haven, CT: Yale University Press, 2020, Kindle Edition.

Levchenko V., Boiko A., Savchenko T. *et al.*, "State regulation of the economic security by applying the innovative approach to its assessment", *Marketing and Management of Innovations*, vol. 10, no. 4, 2019, pp. 364–372, http://doi.org/10.21272/mmi.2019.4-28.

López González D.M., Garcia Rendon J., "Opportunities and challenges of mainstreaming distributed energy resources towards the transition to more efficient and resilient energy markets", *Renewable and Sustainable Energy Reviews*, vol. 157, 2022, 112018, https://doi.org/10.1016/j.rser.2021.112018.

Maschio D.M., Duarte B., Lazzaretti A.E. *et al.*, "An event-driven approach for resources planning in distributed power generation systems", *International Journal of Electrical Power & Energy Systems*, vol. 137, 2022, 107768, https://doi.org/10.1016/j.ijepes.2021.107768.

Mazzucchi N., *Énergie: Ressources, Technologies et Enjeux de Pouvoir*, Paris: Armand Colin, 2017.

McIlwaine N., Foley A.M., Morrow D.J. *et al.*, "A state-of-the-art techno-economic review of distributed and embedded energy storage for energy systems", *Energy*, vol. 229, 2021, 120461, https://doi.org/10.1016/j.energy.2021.120461.

Pazouki S., Naderi E., Asrari A., "A remedial action framework against cyberattacks targeting energy hubs integrated with distributed energy resources", *Applied Energy*, vol. 304, 2021, 117895, https://doi.org/10.1016/j.apenergy.2021.117895.

Pu X., Wang Z.L., "Self-charging power system for distributed energy: Beyond the energy storage unit", *Chemical Science*, vol. 12, no. 1, 2021, pp. 34–49, https://doi.org/10.1039/D0SC05145D.

Sidnell T., Clarke F., Dorneanu B. *et al.*, "Optimal design and operation of distributed energy resources systems for residential neighbourhoods", *Smart Energy*, vol. 4, 2021, 100049, https://doi.org/10.1016/j.segy.2021.100049.

Sikorski T., Jasiński M., Ropuszyńska-Surma E., "A case study on distributed energy resources and energy-storage systems in a virtual power plant concept: Technical aspects", *Energies*, vol. 13, no. 12, 2020, 3086, https://doi.org/10.3390/en13123086.

Silva C., Faria P., Fernandes A., Vale Z., "Clustering distributed Energy Storage units for the aggregation of optimized local solar energy", *Energy Reports*, vol. 8, suppl. 3, 2022, pp. 405–410, https://doi.org/10.1016/j.egyr.2022.01.043.

Simon H.A., "The architecture of complexity", *Proceedings of the American Philosophical Society*, vol. 106, no. 6, 1962, pp. 467–482.

Sofyalıoğlu Ç., Kartal B., "The Selection of Global Supply Chain Risk Management Strategies by Using Fuzzy Analytical Hierarchy Process – A Case from Turkey", *Procedia – Social and Behavioral Sciences*, vol. 58, 2012, pp. 1448–1457, https://doi.org/10.1016/j.sbspro.2012.09.1131.

Tikka V., Mashlakov A., Kulmala A. *et al.*, "Integrated business platform of distributed energy resources – Case Finland", *Energy Procedia*, vol. 158, 2019, pp. 6637–6644, https://doi.org/10.1016/j.egypro.2019.01.041.

Touzani S., Prakash A.K., Wang Z. *et al.*, "Controlling distributed energy resources via deep reinforcement learning for load flexibility and energy efficiency", *Applied Energy*, vol. 304, 2021, 117733, https://doi.org/10.1016/j.apenergy.2021.117733.

The Virtual Utility: Accounting, technology & competitive aspects of the emerging industry, eds. S. Awerbuch, A. Preston, Boston, MA Springer, 1997.

Wang Q., Zhou K., "A framework for evaluating global national energy security", *Applied Energy*, vol. 188, 2017, pp. 19–31, https://doi.org/10.1016/j.apenergy.2016.11.116.

Wasiak I., Szypowski M., Kelm P. *et al.*, "Innovative energy management system for low-voltage networks with distributed generation based on prosumers' active participation", *Applied Energy*, vol. 312, 2022, 118705, https://doi.org/10.1016/j.apenergy.2022.118705.

White S., Youssefi S., *Energy Storage Basics: A Study Guide for Energy Practitioners*, independently published, 2020, Kindle Edition.

Wu R., Sansavini G., "Energy trilemma in active distribution network design: Balancing affordability, sustainability and security in optimization-based decision-making", *Applied Energy*, vol. 304, 2021, 117891, https://doi.org/10.1016/j.apenergy.2021.117891.

Xia Y., Xu Q., Qian H., Cai L., "Peer-to-Peer energy trading considering the output uncertainty of distributed energy resources", *Energy Reports*, vol. 8, suppl. 1, 2022, pp. 567–574, https://doi.org/10.1016/j.egyr.2021.11.001.

Yan T., Liu J., Niu Q. *et al.*, "Distributed energy storage node controller and control strategy based on energy storage cloud platform architecture", *Global Energy Interconnection*, vol. 3, no. 2, 2020, pp. 166–174, https://doi.org/10.1016/j.gloei.2020.05.008.

Zakeri B., Gissey G.C., Dodds P.E., Subkhankulova D., "Centralized vs. distributed energy storage: Benefits for residential users", *Energy*, vol. 236, 2021, 121443, https://doi.org/10.1016/j.energy.2021.121443.

Zhang S., May D., Gül M., Musilek P., "Reinforcement learning-driven local transactive energy market for distributed energy resources", *Energy and AI*, vol. 8, 2022, 100150, https://doi.org/10.1016/j.egyai.2022.100150.

Zheng W., Zou B., "Evaluation of intermittent-distributed-generation hosting capability of a distribution system with integrated energy-storage systems", *Global Energy Interconnection*, vol. 4, no. 4, 2021, pp. 415–424, https://doi.org/10.1016/j.gloei.2021.09.003.

The management of distributed energy resources for national security
Abstract

This article investigates the possibilities of using distributed energy resources (DER) to increase the resilience of national energy systems and national security, including the case of war. A review of literature is conducted, regarding the management of DER systems. Conclusions focus on the specificities of managing such systems for national security, namely: a) the importance of complexity theory as basic framework for strategic planning in DER systems b) the management of risks relative to disruptions in supply chains and c) the role to be played by financial instruments and markets.

Key words: energy security, distributed energy resources (DER), national security, energy resilience

BEZPIECZEŃSTWO TEORIA I PRAKTYKA
SECURITY THEORY AND PRACTICE
e-ISSN 2451-0718
ISSN 1899-6264
2022
No. 2 (XLVII)
DOI: 10.48269/2451-0718-btip-2022-2-003
Received: 23.04.2022
Accepted: 13.07.2022

Andrzej Chodyński
Professor, Andrzej Frycz Modrzewski Krakow University
https://orcid.org/0000-0003-4962-5143

Using ambidexterity in the ecological security management of organisations

Introduction

The discussion on the management of organisations in the context of their security concerns problems considered simultaneously from a strategic and operational perspective (*ambidexterity*), or the appropriate behaviour of different types of organisations in the face of varying environmental turbulence. In particular, the issue of residual behaviour for organisations comprising critical infrastructure is relevant.

Questions concerning the development and adaptation of management mechanisms to the specific security threat situation of an organisation are relevant: according to a situational approach or for the implementation of *ambidexterity* behaviour. In the literature, mechanisms for crisis management are considered on the basis of the different stages (phases) of this management. Crisis management takes a process form with permanent functioning procedures, resources and mechanisms. It is noted that the effectiveness of crisis management mechanisms is influenced by good practices.[1]

The possibility of unexpected, significant (catastrophic) risks should be reflected in the organisation's *ambidexterity* behaviour (mechanisms) in the form of readiness for resilient (referred to as resistance or robustness, combining resistance with

[1] A. Nowicka, "Zarządzanie kryzysowe w ujęciu porównawczym na przykładzie Włoch i Polski", *Obronność – Zeszyty Naukowe Wydziału Zarządzania i Dowodzenia Akademii Sztuki Wojennej*, no. 4(28), 2018, pp. 193–224.

adaptability and flexibility), and resilient (stability) behaviour. The latter involve, inter alia, the use of entrepreneurship and innovation in both a strategic and current (operational) perspective, using appropriate management mechanisms.[2] This type of behaviour is described under the concept of *resilience*. Emphasising the importance of organisational resilience stems from the notion that it is currently a security paradigm, which can be applied to crisis management.[3]

In the case of extreme weather events, mechanisms of resilience based on communication, coordination (mainly of resources and self-organisation), authority of the authorities taking into account the legitimacy of decisions made and learning, including using knowledge gained through experience can be used.[4] Three mechanisms of residual behaviour have been identified in relation to crisis situations including natural disasters: 1. situation awareness (acting in a network means knowing one's position, changes in the environment and the ability to identify crises with their consequences), 2. explaining risks, 3. risk reduction with improved organisational effectiveness using planning.[5]

Hypothesis: *Ambidexterity*, using management mechanisms, can provide support to the functioning of an organisation in both a strategic and operational perspective in the face of unexpected extreme turbulence in the environment related to the ecological factor.

This means, on the one hand, preparing a strategy of resistance and stability and, on the other hand, being ready for ad hoc behaviour.

Ambidexterity and security

The ability to overcome crisis situations can be linked to an organisation's strategic approach related to the concept of *ambidexterity*. The author of this article

---

2 A. Chodyński, *Dynamika przedsiębiorczości, i zarządzania innowacjami w firmach. Odpowiedzialność –prospołeczność – ekologia – bezpieczeństwa*, Kraków: Oficyna Wydawnicza KAAFM, 2021, pp. 165–203.

3 M. Stępka, "Rezyliencja jako paradygmat bezpieczeństwa w czasach przewlekłych kryzysów", *Przegląd Politologiczny*, no. 2, 2021, pp. 105–117.

4 A. Leszczyńska, ,"Mechanisms of organisational resilience to weather extremes: an attempt of identification", *5th International Multidisciplinary Scientific Conference on Social Sciences and Arts SGEM 2018, 26 August – 01 September, 2018*, https://www.researchgate.net/publication/338038128_MECHANISMS_OF_ORGANISATIONAL_RESILIENCE_TO_WEATHER_EXTREMES_-AN_ATTEMPT_OF_IDENTIFICATION [accessed: 2 January 2022].

5 S.Y. Teoh, H.S. Zadeh, *Strategic Resilience Management Model: Complex Enterprise Systems Upgrade Implementation. Proceedings of the 17th Pacific Asia Conference on Information Systems, Illinois, 18–22 July 2013*, [as cited in:] A. Karman, *Odporność organizacji na ekstrema pogodowe*, Lublin: Wydawnictwo UMCS, 2019, p. 128. Karman presents a list of resilience mechanisms in the different phases of extremes: anticipation, response, recovery (p. 154).

proposes that this approach, in a risk situation, considers the proactive attitude of an organisation related to the implementation of a strategy using the capacity for both current and future-oriented actions. The work in this area can be used in security considerations to ensure the ongoing continuity of the organisation under predictable operating conditions and to prepare the organisation for unexpected actions. Ambidexterity refers to the balance of an organisation's exploitative and exploratory behaviour. Exploration is associated with innovation activities, change, while exploitation is associated with improvement and operational competence, among others. The importance of being able to perform these behaviours simultaneously is emphasised.[6]

Ambidexterity is also considered in terms of organisational resilience, referring to the different states of the company in relation to environmental influences. The ability of an organisation to simultaneously exploit and explore is referred to the state of adaptivity.[7]

Ambidexterity can concern structural solutions, the context of activities and leadership. Separate structures relating to exploratory and exploitative activities, linked at the top management level, are the focus of structural *ambidexterity*. Contextual ambidexterity refers to the shaping of processes and systems, taking into account the behavioural choices of employees who devote their time to activities of an exploratory or exploitative nature. Mainstream research on *ambidexterity* considers, among other things, the simultaneous implementation of single and dual learning loops, knowledge management, radical and incremental innovation, transformational leadership or organisational culture. Attention is drawn to the importance of duality concerning the organisation itself and in the context of networks or alliances.[8] With regard to knowledge, *ambidexterity* can refer to its exchange and protection.[9] *Ambidexterity* can be realised in organisations of a different nature from a security point of view, i.e. both operating in and interacting with security systems (including commercial organisations). Up to now, their involvement in security matters may have been low, but this may have increased as a result of the fact that the security of the organisation has already been compromised or is likely to be in the future. The importance of *ambidexterity* may vary and may depend on whether commercial organisations are operating

---

6 A. Zakrzewska-Bielawska, "Paradoks eksploracji i eksploatacji – ambidexterity w zarządzaniu strategicznym", *Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu*, no. 420: *Strategie. Procesy i praktyki*, 2016, pp. 435–449.

7 E.A. Mamouni Limnios, T. Mazzarol, A. Ghadouani, S.G.M. Schilizzi, "The resilience architecture framework: four organizational archetypes", *European Management Journal*, vol. 32, no. 1, 2014, pp. 104–116.

8 A. Zakrzewska-Bielawska, "Ambidexterity – światowe trendy eksploracji w naukach o zarządzaniu", *Przegląd Organizacji*, no. 1, 2016, pp. 16–23.

9 M. Stelmaszczyk, A. Jarubas, "Zastosowanie podejścia ambidexterity w odniesieniu do wymiany wiedzy i ochrony wiedzy w kontekście zdolności absorpcyjnej", *e-mentor*, no. 2(79), 2019, pp. 68–78.

in high-risk sectors, e.g. the chemical industry (in terms of environmental/ecological threats) or energy sector companies operating within critical infrastructure, for which business continuity is essential.[10] Business continuity assurance can refer to the improvement of operational capabilities (in the operational variant) or exploratory, related to the search for new solutions, including for unexpected situations. In the literature, organisational solutions are sought to ensure the security of an organisation's operations through the creation and location of security cells in organisational structures within corporations and companies, among others. The tasks of security departments and the tasks of the security *director* (including his/her role as a leader, but also as an innovator) and the tasks of the security *manager*[11] are considered. The author of this paper points out that it is important that security learning takes place under conditions of controlled business continuity or is the result of the need to react in emergency situations, e.g. the occurrence of unexpected threats and the need for resilient or resilient behaviour.[12] The simultaneous ability to respond in both situations is a manifestation of ambidextrousness. It will therefore be important to create solutions in terms of structures, processes or procedures that are useful in a situation of normal operation of the entity and in an emergency or catastrophic situation where the level of threats has exceeded an acceptable level. This is particularly important for highly reliable organisations (e.g. nuclear power plants). These types of organisations should remain resilient, which does not preclude, in the longer term, there will be changes to better adapt to the risks involved. An important question remains whether and in which areas of the organisation's operation to maintain resources at a slimmed-down level, and in which areas, e.g. related to environmental security and potential crisis situations to maintain redundant resources (strategic approach related to resource redundancy).

Ambidexterity behaviour is conditioned on the one hand by the perspective of anticipatory behaviour and on the other hand by the realities of the implementation of current operational activities. Unexpected events, including those of a catastrophic nature, occur in the reality of the company's operating conditions, in a specific place and time, with a certain degree and nature of links between different organisations. This place, going beyond a narrow understanding of this concept in purely geographical

[10] Business continuity management with regard to critical infrastructure is reflected in the unified text of the Crisis Management Act (Journal of Laws of the Republic of Poland, 2019, item 1398). For a broader commentary, see A. Jagnieża, *Promocja zarządzania ciągłością działania*, https://fibis.pl/o-potrzebie-promocji-zarzadzania-ciagloscia-dzialania [accessed: 10 November 2020].

[11] Ch. Sennewald, C. Baillie, *Effective security management*, 7th ed., Oxford: Elsevier, Butterworth-Heinemann, 2020, pp. 3–45, https://www.elsevier.com/books/effective-security-management/sennewald/978-0-12-814794-8 [accessed: 3 January 2021].

[12] A. Chodyński, Przedsiębiorstwo sprężyste – odpowiedzialność w skrajnie turbulentnym otoczeniu, [in:] *Obszary zrównoważonego zarządzania organizacjami w zmiennym otoczeniu*, ed. D. Fatuła, Kraków: Oficyna Wydawnicza KAAFM, 2016, pp. 37–51.

terms, implies the need to operate in an environment with a specific social capital that affects the company's ability to survive.

In considering the *ambidexterity of* relevant security, including at the local level, an important role can be played by analysing the paradoxes of inter-organisational cooperation in a public security management system involving local government, intervention and rescue units, local communities, the media, NGOs and research and development units.[13] Dealing with paradoxes is based, among other things, on activities such as joint exercises, exchange of experience, training, cooperation with local authorities, agreements or the creation of joint procedures. The importance of the impact of individual research and development units, in turn, may be related to their activities resulting from the conditions resulting from the transformations in this field in Poland.[14]

Although Monica Giancotti and Marianna Mauro[15] point out that *ambidexterity* occupies a special place at the response stage, it seems that the problem should be considered more broadly, situating it also in other stages of the development of a crisis, and taking into account the factors that influence the possibility of implementing *ambidexterity* behaviour.

In the consideration of *ambidexterity*, proposals for mechanisms of strategic renewal of the organisation, concerning the revitalisation of certain key competences and their structuring together with supporting actions (using innovative actions) can be used.[16] The author of this publication draws attention to the importance of including in these considerations situations of strategic renewal resulting from the impacts of extreme turbulence of the environment. Dynamic capabilities described in the literature (as organisational routines) can be used to combine, reconfigure and renew resources (in the face of the volatility and unpredictability of the environment) using innovative behaviour. Creative improvisation can also be used for organisational change (independently of dynamic capabilities).[17]

---

[13] B. Kożuch, K. Sienkiewicz-Małyjurek, "Paradoksy współpracy międzyorganizacyjnej w systemie zarządzania bezpieczeństwem publicznym", *Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu*, no. 421: *Sieci międzyorganizacyjne, procesy i projekty w erze paradoksów*, 2016, pp. 289–300.

[14] A. Chodyński, "State support for innovation actions in public security management", *Bezpieczeństwo. Teoria i Praktyka*, no. 4, 2020, pp. 55–73.

[15] M. Giancotti, M. Mauro, "Building and improving the resilience of enterprises in a time of crisis: from a systematic scoping review to a new conceptual framework", *Economia Aziendale Online – Business and Management Sciences International Quarterly Review*, vol. 11, no. 3, 2020, pp. 307–339, http://web.b.ebscohost.com/ehost/pdfviewer/pdfviewer?vid=69&sid=eb57b339-324c-4d82-b6f1-0b390c4c1bc1%40sessionmgr102 [accessed: 3 April 2021].

[16] J. Karpacz, "Mechanizmy odnowy strategicznej przedsiębiorstwa: przegląd literatury", *Zeszyty Naukowe Politechniki Łódzkiej*, no. 1147, 2013: *Organizacja i Zarządzanie*, no. 52, pp. 85–98.

[17] A. Wójcik-Karpacz, "Zdolności dynamiczne w turbulentnym otoczeniu", *Organizacja i Kierowanie*, no. 4(138), 2018, pp. 51–69.

When considering issues of *ambidexterity* in terms of security, it is worth noting the strategic mechanism of organisational development relating to technological entrepreneurship.[18] The author of this publication highlights the importance of this mechanism in view of the possibility of threats to the security of the entity and the benefits of implementing new technologies. It is important to point out the role of entrepreneurial orientation related to innovation both in the long term (innovation strategies) and in response to current threats (ad hoc innovation).[19]

Network aspect of *ambidexterity*

Organisational practices are used in the implementation of management mechanisms. The repetition of practices leads to routines.[20] The theme of routines is addressed in terms of *ambidexterity* also in relation to inter-organisational relationships. In this case, considerations relate to exploitation (based on established partners) and exploration (creating ties with new partners). Within the relationship, there is a differentiated approach to the use of exploratory routines (oriented to the use of partners' knowledge) and exploitative routines, oriented to the use of the company's own knowledge. *Ambidexterity* concerns, among other things, the coordination involved in the simultaneous use of both types of routines with a balance between them. Network research in terms of ambidexterity has addressed, among other things, innovation, openness, network position and top managers' ties. Among the transactional mechanisms of ambidexterity and alliances involving high-tech firms based on learning and mutual knowledge transfer, exchanges of experience and shared interpretation are described, as well as mutual investment and arrangements that enhance knowledge protection (hostage arrangement).[21]

The author of this article expresses the view that *ambidexterity* in the security context should be considered in terms of opportunities for cooperation with partners. It may imply an approach related to the creation of network links in the long and short term, including ad hoc, bearing in mind the access to specific own and partners' resources. A crisis situation, e.g. of a catastrophic nature, may induce actors to create ad

---

[18] P. Kordel, "Konfiguracje elementów procesu zarządzania strategicznego w przypadku przedsiębiorczości technologicznej – analiza zbiorów rozmytych", *Przegląd Organizacji*, no. 7, 2018, pp. 9–18.

[19] A. Chodyński, *Dynamika przedsiębiorczości...*, *op. cit.*, pp. 208–211.

[20] J. Karpacz, "Procedury jako narzędzie utrwalania rekurencyjnych wzorów zachowań pracowników", *Zarządzanie i Finanse*, vol. 1, no. 4 part 2, 2013, pp. 171–180.

[21] A. Zakrzewska-Bielawska, Ambidexterity w obliczu paradygmatu relacyjnego – wyzwaniem współczesnego zarządzania strategicznego, [in:] *Wyzwania współczesnego zarządzania strategiczne*go, eds. A. Sopińska, P. Wachowiak, Warszawa: Oficyna Wydawnicza SGH, 2017, pp. 177–192, http://zakrzewskabielawska.pl/wp-content/uploads/2021/01/publikacja_I_2.pdf [accessed: 16 March 2022].

hoc links through chelation, in which the links between stakeholders are intensified and concern the possibility of using different types of resources for the survival of the organisation, both tangible and intangible.[22] A new approach is required to study the chelation mechanism. The first step would be to identify the partners with their resources, assess the availability of these resources and then assess the possibilities of using them with, for example, bricolage. Ad hoc procedures would be developed regarding the use of resources in the face of risks. An *ambidexterity* approach would mean that the company should be aware of and prepared for risks and, based on the lessons learned, have a strategy for dealing with future risks. With such an approach, mechanisms for managing extreme turbulence in the environment (including chelation mechanisms) should be developed. In the case of sudden threats, according to the author of this publication, collective (collaborative) bricolage can also be used, relying on a network of partners with complementary resources. Among these resources, he points to knowledge. This form of cooperation is treated as an innovative process.[23]

The ecological aspect of *ambidexterity*

Ecological issues, including *ambidexterity* are considered in the context of companies' business strategies.[24] *Ambidexterity* is also discussed in terms of environmental (ecological) entrepreneurship of companies[25] and the implementation of green innovations of *ambidexterity*.[26] Starting from resource and agency theory, the role of *innovation ambidexterity* (IA) was referred to in relation to the concept of *sustainability,* taking into account the natural environment (*environment sustainability*, ES). The components of ES are related to natural environment security activities, while *environmental sustainability* positively influences both *exploitative* and *explorative* innovation. ES is considered as an antecedent for balancing both types of innovation to create competitive advantage. IA is a key dynamic capability of

[22] A. Chodyński, "Security in public governance: an introduction", *Bezpieczeństwo. Teoria i Praktyka*, no. 4, 2020, p. 19.

[23] A. Gurca, M.N. Ravishankar, "A bricolage perspective on technological innovation in emerging markets", *IEEE Transactions on Engineering Management*, vol. 63, no.1, 2015, pp. 53–66.

[24] F. Martinez, "Corporate strategy and the environment: towards a four-dimensional compatibility model for fostering green management decisions", *Corporate Governance: The International Journal of Business in Society*, vol. 14, no. 5, 2014, pp. 607–636.

[25] I. Shafique, M.N. Kalyar, N. Mehwish, "Organizational ambidexterity, green entrepreneurial orientation, and environmental performance in SMEs context: Examining the moderating role of perceived CSR", *Corporate Social Responsibility and Environmental Management*, vol. 28, no. 1, 2021, pp. 446–456, https://ideas.repec.org/a/wly/corsem/v28y2021i1p446-456.html [accessed: 16 March 2022].

[26] Y. Sun, H. Sun, "Green innovation strategy and ambidextrous green innovation: The mediating effects of green supply chain integration", *Sustainability*, vol. 13, no. 9, 2021, 4876, https://www.mdpi.com/2071-1050/13/9/4876/htm [accessed: 16 March 2022].

the organisation. Ambidextrous innovation behaviour is considered as needed by the organisation, it is related to simultaneity in relation to exploitative (based on existing or renewed knowledge) and exploratory behaviour. The implementation of exploitative innovation, oriented towards short-term benefits, is associated with incremental activities. Exploratory innovation, considered over the long term, involves radical activities, using new knowledge.[27] It is possible to present the view that a topic that requires extended research is the area of dynamic capabilities in risk situations, including ecological ones, to ensure the security of organisations.

The author of this paper takes the view that, in an environmental context, *ambidexterity* will refer to the continuous improvement of technology and production (cleaner production) and simultaneous action for radical change, e.g. through innovative measures (realisation of clean production or clean technology). This approach is linked to the implementation of *sustainability*.

Ambidexterity should take into account the reciprocity aspects of company-environmental (ecological, natural) interactions, taking into account ecological risks and the feasibility of ecological security management systems. Within the concept of a sustainable enterprise, which takes into account economic, social and ecological aspects, the issue of an extended understanding of environmental (ecological) risk is raised. It is characterised by a two-sided impact: the impact of human activity on the natural environment and the impact of natural forces on the economy and humans.[28]

Conclusions

The issue of organisational security can be considered in relation to the main research strands of *ambidexterity* already mentioned: learning, knowledge management, innovation, leadership and organisational culture.

The literature indicates that a company pursuing *ambidexterity* can be considered as an intelligent organisation.[29] The proposed solutions concern separate organisational structures for exploration and exploitation activities. Further research should indicate to what extent these activities should encompass the problems (including mechanisms) of organisational security management.

Ecological issues may concern the need for action to build competitive advantage (including innovative behaviour), but also the ongoing response to extreme

[27] M.V. Ciasullo, R. Montera, A. Douglas, "Environmental sustainability and board independence: What effects on innovation ambidexterity?", *Corporate Governance and Research & Development Studie*s, no. 1, 2020, pp. 41–63.

[28] A. Panasiewicz, "Zarządzanie ryzykiem ekologicznym jako narzędzie równoważenia rozwoju organizacji", *Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu*, no. 377: *Zrównoważony rozwój organizacji – odpowiedzialność środowiskowa*, 2015, pp. 230–239.

[29] A. Zakrzewska-Bielawska, "Ambidextrous organization jako przykład przedsiębiorstwa inteligentnego", *Studia i Prace Kolegium Zarzadzania i Finansów SGH*, no. 48, 2016, pp. 161–174.

environmental turbulence (e.g. natural and industrial disasters). In the long term, the effects of global warming on the functioning of companies should be taken into account. Co-ordinating actions (management mechanisms) in current situations with extreme environmental turbulence based on past experience will be difficult due to the unexpected and unpredictable nature of the risks involved. The use of partner resources will require knowledge of these resources and also short-term decision-making. On the one hand, the long-term nature of the cooperation will be a favourable factor, while on the other hand, links with new (ad hoc) partners, necessitated by the situation, will gain in importance.

The unpredictable nature of extreme risks makes it necessary to take a new look at theories of how companies operate, including in crisis situations. More attention should be paid to the issue of non-economic crises with a focus on the possibilities of ensuring the continuity of the organisation.[30]

Today, the issue of businesses, including those operating within critical infrastructure, is considered in the light of technological change, entrepreneurship, innovation or stakeholder influence. Stakeholder impacts may also include considering the importance of the possibility of crisis situations and crises that pose a threat to people and the natural environment and preparing in advance for these threats by adopting *ambidexterity* assumptions.

References

Chodyński A., *Dynamika przedsiębiorczości, i zarządzania innowacjami w firmach. Odpowiedzialność – prospołeczność – ekologia – bezpieczeństwa*, Kraków: Oficyna Wydawnicza KAAFM, 2021, pp. 165–203.

Chodyński A., "Kryzys pozaekonomiczny przedsiębiorstwa – ekologiczny aspekt rezyliencji organizacyjnej", [in:] *Zrównoważony rozwój, systemy informacyjne i zarządzanie bezpieczeństwem w perspektywie długoterminowej przedsiębiorstw*, eds. A. Chodyński, D. Fatuła, M.A Leśniewski, Kraków: Oficyna Wydawnicza KAAFM, 2022 (in print).

Chodyński A., Przedsiębiorstwo sprężyste – odpowiedzialność w skrajnie turbulentnym otoczeniu, [in:] *Obszary zrównoważonego zarządzania organizacjami w zmiennym otoczeniu*, ed. D. Fatuła, Kraków: Oficyna Wydawnicza KAAFM, 2016, pp. 37–51.

Chodyński A., "Security in public governance: an introduction", *Bezpieczeństwo. Teoria i Praktyka*, no. 4, 2020, pp. 17–20.

Chodyński A., "State support for innovation actions in public security management", *Bezpieczeństwo. Teoria i Praktyka*, no. 4, 2020, pp. 55–73.

Ciasullo M.V., Montera R., Douglas A., "Environmental sustainability and board independence: What effects on innovation ambidexterity?", *Corporate Governance and Research & Development Studies*, no. 1, 2020, pp. 41–63.

[30] A. Chodyński, "Kryzys pozaekonomiczny przedsiębiorstwa – ekologiczny aspekt rezyliencji organizacyjnej", [in:] *Zrównoważony rozwój, systemy informacyjne i zarządzanie bezpieczeństwem w perspektywie długoterminowej przedsiębiorstw*, eds. A. Chodyński, D. Fatuła, M.A Leśniewski, Kraków: Oficyna Wydawnicza KAAFM, 2022 [in print].

Giancotti M., Mauro M., "Building and improving the resilience of enterprises in a time of crisis: from a systematic scoping review to a new conceptual framework", *Economia Aziendale Online – Business and Management Sciences International Quarterly Review*, vol. 11, no. 3, 2020, pp. 307–339, http://web.b.ebscohost.com/ehost/pdfviewer/pdfviewer?vid=69&sid=eb57b339-324c-4d82-b6f1-0b390c4c1bc1%40sessionmgr102 [accessed: 3 April 2021].

Gurca A., Ravishankar M.N., "A bricolage perspective on technological innovation in emerging markets", *IEEE Transactions on Engineering Management*, vol. 63, no. 1, 2015, pp 53–66.

Karman A., *Odporność organizacji na ekstrema pogodowe*, Lublin: Wydawnictwo UMCS, 2019.

Karpacz J., "Mechanizmy odnowy strategicznej przedsiębiorstwa: przegląd literatury", *Zeszyty Naukowe Politechniki Łódzkiej*, no. 1147, 2013: *Organizacja i Zarządzanie*, no. 52, pp. 85–98.

Karpacz J., "Procedury jako narzędzie utrwalania rekurencyjnych wzorów zachowań pracowników", *Zarządzanie i Finanse*, vol. 1, no. 4 part 2, 2013, pp. 171–180.

Kordel P., "Konfiguracje elementów procesu zarządzania strategicznego w przypadku przedsiębiorczości technologicznej – analiza zbiorów rozmytych", *Przegląd Organizacji*, no. 7, 2018, pp. 9–18.

Kożuch B., Sienkiewicz-Małyjurek K., "Paradoksy współpracy międzyorganizacyjnej w systemie zarządzania bezpieczeństwem publicznym", *Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu*, no. 421: *Sieci międzyorganizacyjne, procesy i projekty w erze paradoksów*, 2016, pp. 289–300.

Leszczyńska A., "Mechanisms of organisational resilience to weather extremes: an attempt of identification", *5th International Multidisciplinary Scientific Conference on Social Sciences and Arts SGEM 2018, 26 August – 01 September, 2018*, https://www.researchgate.net/publication/338038128_MECHANISMS_OF_ORGANISATIONAL_RESILIENCE_TO_WEATHER_EXTREMES_-AN_ATTEMPT_OF_IDENTIFICATION [accessed: 2 January 2022].

Mamouni Limnios E.A, Mazzarol T., Ghadouani A., Schilizzi S.G.M., "The resilience architecture framework: four organisational archetypes", *European Management Journal*, vol. 32, no. 1, 2014, pp. 104–116.

Martinez F., "Corporate strategy and the environment: towards a four-dimensional compatibility model for fostering green management decisions", *Corporate Governance: The International Journal of Business in Society*, vol. 14, no. 5, 2014, pp. 607–636.

Nowicka A., "Zarządzanie kryzysowe w ujęciu porównawczym na przykładzie Włoch i Polski", *Obronność – Zeszyty Naukowe Wydziału Zarządzania i Dowodzenia Akademii Sztuki Wojennej*, no. 4(28), 2018, pp. 193–224.

Panasiewicz A., "Zarządzanie ryzykiem ekologicznym jako narzędzie równoważenia rozwoju organizacji", *Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu*, no. 377: *Zrównoważony rozwój organizacji – odpowiedzialność środowiskowa*, 2015, pp. 230–239.

Sennewald Ch., Baillie C., *Effective security management*, 7th ed., Oxford: Elsevier, Butterworth-Heinemann, 2020, pp. 3–45, https://www.elsevier.com/books/effective-security-management/sennewald/978-0-12-814794-8 [accessed: 3 January2021].

Shafique I., Kalyar M.N., Mehwish N., "Organizational ambidexterity, green entrepreneurial orientation, and environmental performance in SMEs context: Examining the moderating role of perceived CSR", *Corporate Social Responsibility and Environmental Management*, vol. 28, no. 1, 2021, pp. 446–456, https://ideas.repec.org/a/wly/corsem/v28y2021i1p446-456.html [accessed: 16 March 2022].

Stelmaszczyk M., A. Jarubas, "Zastosowanie podejścia ambidexterity w odniesieniu do wymiany wiedzy i ochrony wiedzy w kontekście zdolności absorpcyjnej", *e-mentor*, no. 2(79), 2019, pp. 68–78.

Stępka M. , "Rezyliencja jako paradygmat bezpieczeństwa w czasach przewlekłych kryzysów", *Przegląd Politologiczny*, no. 2, 2021, pp. 105–117.

Sun Y., Sun H., "Green innovation strategy and ambidextrous green innovation: The mediating effects of green supply chain integration", *Sustainability*, vol. 13, no. 9, 2021, 4876, https://www.mdpi.com/2071-1050/13/9/4876/htm [accessed: 16 March 2022].

Teoh S.Y., Zadeh H.S.., 'Strategic resilience managemant model:complex enterprise systems upgrate implementation', *Pacific Asia Conference on Information Systems, Pacis* 2013, Proceedings, 242.

Wójcik-Karpacz A., "Zdolności dynamiczne w turbulentnym otoczeniu", *Organizacja i Kierowanie*, no. 4(138), 2018, pp. 51–69.

Zakrzewska-Bielawska A., "Paradoks eksploracji i eksploatacji – ambidexterity w zarządzaniu strategicznym", *Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu*, no. 420: *Strategie. Procesy i praktyki*, 2016, pp. 435–449.

Zakrzewska-Bielawska A., "Ambidexterity – światowe trendy eksploracji w naukach o zarządzaniu", *Przegląd Organizacji*, no. 1, 2016, pp. 16–23.

Zakrzewska-Bielawska A., Ambidexterity w obliczu paradygmatu relacyjnego – wyzwaniem współczesnego zarządzania strategicznego, [in:] *Wyzwania współczesnego zarządzania strategiczneg*o, eds. A. Sopińska, P. Wachowiak, Warszawa: Oficyna Wydawnicza SGH, 2017, pp. 177–192, http://zakrzewskabielawska.pl/wp-content/uploads/2021/01/publikacja_I_2.pdf [accessed: 16.03.2022].

Zakrzewska-Bielawska A., "Ambidextrous organization jako przykład przedsiębiorstwa inteligentnego", *Studia i Prace Kolegium Zarzadzania i Finansów SGH*, no. 48, 2016, pp. 161–174.

Using ambidexterity in the ecological security management of organisations

Abstract

The main currents of research on ambidexterity in the context of organisational security with emphasis on the role of network links are indicated. The hypothesis that *ambidexterity*, using governance mechanisms, can support the functioning of an organisation in both strategic and operational perspectives in the face of unexpected extreme turbulence in the environment related to the environmental factor is substantiated.

This implies, on the one hand, the need to prepare a strategy of resistance and resilience and, on the other hand, a readiness for ad hoc behaviour. *Ambidexterity* was considered in the context of cooperation with partners, with a view to accessing certain own and partners' resources in a crisis situation. In an ecological context, the influence of *ambidexterity* on the continuous improvement of the organisation's performance was discussed, paying attention to the simultaneous efforts for radical change based on innovative actions, starting from the assumption of *sustainability*, in cooperation with stakeholders. A review of the concept of *ambidexterity* in relation to the issue of organisational security was conducted based on a critical analysis of the literature on the subject. A research gap related to this area was identified. The aim of the study was to identify opportunities for the use of *ambidexterity* in organisations in emergency situations.

Key words: ambidexterity, resilience, ecological security, management mechanisms

BEZPIECZEŃSTWO TEORIA I PRAKTYKA
SECURITY THEORY AND PRACTICE
e-ISSN 2451-0718
ISSN 1899-6264
2022
No. 2 (XLVII)
DOI: 10.48269/2451-0718-btip-2022-2-004
Received: 26.04.2022
Accepted: 20.07.2022

Anna Bałamut
PhD, Andrzej Frycz Modrzewski Krakow University
https://orcid.org/0000-0001-7300-7367

Hydrogen use in Poland in the light of EU policy to move away from coal: the concepts of hydrogen valleys and smart and sustainable cities

Introduction

Hydrogen, due to its prevalence, generates many opportunities for the energy sector. It should be emphasised that the reaction of hydrogen with oxygen does not produce carbon dioxide. For this reason, one often encounters the term 'clean energy carrier'. This fact generates not only economic benefits, but also, for example, environmental or social benefits. Hydrogen valleys in Poland are expected to contribute to achieving climate neutrality and maintaining the competitiveness of the Polish economy, but the question is whether this will be possible. The essence is cooperation between individual participants in the energy market promoting hydrogen-based solutions, e.g. between enterprises, within clusters, or between enterprises and the public.

The aim of this study is to show the prospects for the realisation of so-called hydrogen valleys and smart sustainable cities as an alternative to EU guidelines. For the purpose of this analysis, a hypothesis was formulated, which assumes that the use of hydrogen in the economy will significantly improve Poland's energy security in the long term. The following research question was asked: Will Poland use hydrogen as a solution to meet EU requirements for a zero-carbon economy?

The article is divided into two parts. The first describes the energy and climate policy framework of the EU and Poland, the second describes hydrogen valleys – the current status of projects and the use of green hydrogen as part of the creation of the so-called smart cities idea. In summary, the article is of a mixed nature, in which the governance aspect and the policy decision aspect will be included. In addition, it will discuss an issue relevant to Poland's energy security concerting on the latest news and developments.

This article uses the method of content analysis of press release documents or websites. The methods used included empirical methods, i.e. observation, description and general methods, i.e. analysis, synthesis, induction and deduction. Primary sources, monographs, articles and publications on the websites of individual ministries, organisations, entities, etc. were used in this article.

The EU energy and climate policy framework and Poland's energy and environmental security strategy

In December 2019, the European Commission presented the so-called Green Deal strategy, i.e. a map of actions to ensure that Europe is, among other things, climate-neutral by 2050. It was proposed to tighten the EU's carbon reduction targets from 40% to 50–55%. The EU emphasises the need for close cooperation for a modern and competitive economy and therefore encourages changes at the level of national legislation. It is important to develop new technologies, while protecting the environment at the same time e.g. green hydrogen or electromobility.[1]

In response to EU regulations, the *National Energy and Climate Plan for 2021–2030* was adopted by Poland on 18 December 2019, confirming the implementation of the so-called Energy Union. It assumes that RES (Renewable Energy Sources) in gross final energy consumption will account for approximately 21–23%. It is also planned to create around 300 sustainable energy areas at local level. The solution supports the EU guidelines for increasing the share of renewable energy in the overall energy mix: RECs – Renewable Energy Communities, and ECs – Energy Communities. Hydrogen is mentioned several times in the document, as an example for the possibilities of developing the Polish economy, e.g. for the natural gas network, as an input for chemical processes, for changing carbon dioxide

[1] Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, *The European Green Deal*, COM/2019/640 final, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52019DC0640 [accessed: 7 April 2022].

into methane so that the resulting gas can be used to produce electricity, or for upgrading the quality of biogas.[2]

In 2020, a document developed by the Polish side appeared on a SWOT analysis of the Green Deal strategy. Weaknesses were identified as: the lack of an energy strategy, the lack of decisions on the transition towards green energy or the significant share of coal in the energy balance, and administrative issues – an insufficient number of people working on this issue. As strengths were indicated: the potential of regions for future modernisation, e.g. Wielkopolska, Silesia, Lower Silesia (mining), support instruments, e.g. the Mój Prąd programme, the Czyste Powietrze programme or the Fundusz Niskoemisyjny, and the potential for development of low-emission transport – the lithium-ion battery factory, LG Chem for electric cars.[3]

In 2020, the *Hydrogen Strategy for a climate-neutral Europe* was presented. Among other things, it proposed installing 40 GW of electrolysers by 2030. The essence, therefore, is the creation of a so-called 'hydrogen eco-system' in Europe by 2050, based on cooperation between, among others, public authorities, industry, business or society. The EU's goal is to produce renewable hydrogen using wind and solar energy. However, this requires time, probably a time horizon of about 25 years. The document stresses that there are different examples of hydrogen: electrolytic hydrogen (electrolysis of water – whatever the energy source), renewable hydrogen – electrolysis of water, electrolysis powered by electricity from renewable sources, pure hydrogen is renewable hydrogen, hydrogen from fossil fuels and hydrogen from fossil fuels using carbon dioxide (greenhouse gases are captured).[4] The creation of a European alliance for clean hydrogen is an opportunity is the creation of a so-called inventory-list of investments and the identification of opportunities to finance them (e.g. the NEXT Generation EU Recovery Plan, or InvestEU).

In 2021, the Directive of the European Parliament and of the Council on the promotion-application of energy from renewable sources (2018) entered into force. The directive indicates how the consumption of renewable energy sources should develop between 2021 and 2030 (RES 32% – by 2030). In addition, it emphasises that

---

[2] "Krajowy plan na rzecz energii i klimatu na lata 2021–2030 przekazany do KE", Ministerstwo Aktywów Państwowych, 13 December 2019, https://www.gov.pl/web/aktywa-panstwowe/krajowy-plan-na-rzecz-energii-i-klimatu-na-lata-2021-2030-przekazany-do-ke [accessed: 8 April 2022].

[3] Kancelaria Senatu, *Polska w Zielonym Ładzie – korzyści, możliwości i ocena SWOT*, Opinie i ekspertyzy, OE–307, Warszawa 2020, https://www.senat.gov.pl/gfx/senat/pl/senatekspertyzy/5619/plik/oe_307.pdf [accessed 8 April 2022].

[4] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *A hydrogen strategy for a climate-neutral Europe*, COM/2020/301 final, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020DC0301&from=pl [accessed: 8 April 2022].

the participation of local actors, including, for example, prosumers, is important. They should have the right, to: generation, storage and sale of generated energy. The document also stresses that the so-called guarantees of origin used for renewable electricity, should be extended to e.g. biomethane. This would be a further step towards the introduction of guarantees of origin for hydrogen.[5]

The response from the Polish side was a *Draft Law on amendments to the law on Renewable Energy Sources and certain other laws*. It was indicated that a 14% share of RES in transport by 2030 was possible. The new regulations were to unify the issues of generation, sale, transmission and storage of energy in the activities of entities at the local level. At the same time, consultations are being carried out within the framework of the draft law on biocomponents and liquid biofuels, in order to implement the RED II directive in transport.[6]

In July 2021, *Fit for 55* was published, a document consisting of 13 legislative proposals. These must be accepted by the European Parliament and the individual Member States. Indications are that this process will last until 2023. An important solution is to limit the registration of combustion vehicles in 2035 (within the EU). In addition, Directive 2014/94/EU of the European Parliament and of the Council of 22 October 2014 has also been repealed, changing AFID (Alternative Fuel Infrastructure Directive) to AFIR (Alternative Fuels Infrastructure Regulation). Zero-emission vehicles will therefore be promoted, which require the creation of an appropriate charging infrastructure. Thus, by the end of 2030, a hydrogen charging infrastructure should already be in place on the TEN-T network. Such solutions require legal regulations, e.g., for payment, information on charging costs, payment by card at the terminal or contactless. In addition, there are expected to be around 1 million charging points across the EU in 2025 and 3 million in 2030.[7]

On 7 December 2021, the *Polish Hydrogen Strategy until 2030 with an outlook until 2040* was published. It was pointed out that hydrogen is the right path to decarbonisation and can be applied in many areas of the economy, from energy to heating, industry or, for example, transport. So-called 'hydrogen valleys' are to appear in Poland, i.e. places for future investments that are convenient for stakeholders, for creating potential for investments, for the scientific and research environment, etc. The strategy is a way to use hydrogen on an industrial scale. In addition, jobs will be

---

5 Directive (EU) 2018/2001 of the European Parliament and of the Council of 11 December 2018 on the promotion of the use of energy from renewable sources (recast), OJ L 328/82, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018L2001&from=PL [accessed: 7 April 2022].

6 Rządowy projekt ustawy o zmianie ustawy o odnawialnych źródłach energii oraz niektórych innych ustaw, Draft No. 1129, 26 April 2021, https://www.sejm.gov.pl/sejm9.nsf/PrzebiegProc.xsp?nr=1129 [accessed: 7 April 2022].

7 European Commission, *Fit for* 55, https://www.consilium.europa.eu/en/policies/green-deal/fit-for-55-the-eu-plan-for-a-green-transition [accessed: 7 April 2022].

created, which will significantly increase the attractiveness of the region. The document emphasises the importance of the entire value chain from production, transmission to storage and use, with regulations in line with EU guidelines and attracting potential investors.[8]

In March 2022, Poland updated the assumptions of *the Polish Energy Policy until 2040*. The change is a result of the ongoing war between Russia and Ukraine. Therefore, it was emphasised that it is important to minimise crisis situations, which involves intensifying efforts to diversify directions and sources of energy acquisition, while maintaining the competitiveness of the economy and limiting environmental impact. It was pointed out that decarbonised gas or hydrogen-based technologies could be a solution to natural gas. Additionally, in the case of transport, there is talk of clean public transport, i.e. the use of bio-components in liquid fuels.[9]

The above documents indicate the EU's promotion of hydrogen investments, which fits in with the zero-carbon strategy. In addition, with the spectre of further war in Ukraine, hydrogen provides an additional alternative to fossil fuel supplies. Poland supports these solutions, emphasising that hydrogen can become a permanent part of the energy mix and participate effectively in it, e.g. by increasing the competitiveness of the economy in the long term.

Hydrogen valleys and the idea of the Smart City

There are many ways to produce hydrogen. The so-called steam reforming of the gas, i.e. converting it under the influence of heat, is mentioned as the most economical way. Another way is the so-called electrolysis of water, i.e. splitting it into hydrogen and oxygen, using an electric current. In the case of hydrogen, the terms grey, green, blue, violet are also used, but this refers to the way it is obtained, e.g. gas, water, etc. The term biohydrogen is mentioned, which refers to the involvement of micro-organisms (fermentation and photolysis). In the case of vehicles, hydrogen can be used to power internal combustion engines and in fuel cells to generate electricity. These solutions offer a number of opportunities when it comes to the energy market, especially in an ever-changing environment where energy and

---

[8] "*Polska Strategia Wodorowa do roku 2030 z perspektywą do roku 2040* opublikowana w Monitorze Polskim", Ministerstwo Klimatu i Środowiska, 9 December 2021, https://www.gov.pl/web/klimat/polska-strategia-wodorowa-do-roku-2030-z-perspektywa-do-roku-2040-opublikowana-w-monitorze-polskim [accessed: 7 April 2022].

[9] "Założenia do aktualizacji Polityki Energetycznej Polski do 2040 r. (PEP2040) – wzmocnienie bezpieczeństwa i niezależności energetycznej", Kancelaria Prezesa Rady Ministrów, 29 March 2022, https://www.gov.pl/web/premier/zalozenia-do-aktualizacji-polityki-energetycznej-polski-do-2040-r-pep2040--wzmocnienie-bezpieczenstwa-i-niezaleznosci-energetycznej [accessed: 29 March 2022].

environmental security issues are constantly being redefined.[10] If photolysis is used, it is possible to generate hydrogen, which contains about 10–20% carbon dioxide, so that the gas does not need to be purified. Another solution can be so-called dark fermentation, where organic compounds, polymers e.g. starch or cellulose, are used. This technology was used by Prof. Jacek Dach from the Poznań University of Life Sciences.[11]

In Poland, five hydrogen valleys (Pol. dolina wodorowa, DW) were planned: Dolnośląska DW, Wielkopolska DW, Mazowiecka DW, Podkarpacka DW and Śląskie Zagłębie Wodorowe. With the support of, among others, the Ministry of Climate and Environment and the Industrial Development Agency, they are to become part of the European system. A hydrogen valley is a geographical area, so it can be a city, a region or e.g. a transmission area, where hydrogen is embedded in the so-called supply chain from production, storage, distribution to its use. Which affects the efficiency and competitiveness of the area. However, a number of investments are needed to make this happen, and this is where the EU can be of help, e.g. under the National Recovery Plan (NRP, Pol. Krajowy Plan Odbudowy, KPO), where EUR 23.850 billion is available in the form of grants and EUR 12.112 billion in the form of loans, including for green energy and mobility. In order to obtain the funds, the Polish side sent the document (in May 2021) to the European Commission (EC), but so far it has not been accepted.[12] The lack of agreement is due, among other things, to the divergence of Polish and EU objectives. Poland indicates that a mutually acceptable solution is still being worked on, e.g. on the issue of justice. The KPO points out the so-called challenges for the sector, highlighting that Poland's hydrogen production in 2020 was 1 million tonnes. This was hydrogen from fossil fuels. Low-carbon hydrogen production facilities are appearing in Poland, but they are of a test nature.

The first hydrogen valley was inaugurated in May 2021 in Jasionka, the so-called Podkarpacka DW.[13] In January 2022, the Śląsko-Małopolska DW was established. According to Paweł Kolczyński, Vice President of the Industrial Development Agency (ARP S.A.), it is necessary to base the industry on hydrogen and support this solution in order to be able to use hydrogen effectively in the energy sector in the

---

[10] A. Chodyński, *Dynamika przedsiębiorczości i zarządzania innowacjami w firmach. Odpowiedzialność – prospołeczność – ekologia – bezpieczeństwo*, Kraków: Oficyna Wydawnicza KAAFM, 2021, pp. 165–169.

[11] "Kierunek przyszłości – biometan i biowodór", Portal Komunalny, 1 December 2021, https://portalkomunalny.pl/kierunek-przyszlosci-biometan-i-biowodor-428075/ [accessed: 7 April 2022].

[12] Portal Funduszy Europejskich, 1 September 2021, https://www.funduszeeuropejskie.gov.pl/strony/o-funduszach/fundusze-na-lata-2021-2027/konsultacje-spoleczne-kpo/o-kpo/ [accessed: 7 April 2022].

[13] "Rzeszów sercem Podkarpackiej Doliny Wodorowej", Ministerstwo Klimatu i Środowiska, 18 May 2021, https://www.gov.pl/web/klimat/rzeszow-sercem-podkarpackiej-doliny-wodorowej [accessed: 7 April 2022].

future.[14] At the end of February 2022, the Dolnośląska DW was established. KGHM Polska Miedź S.A. is the business partner. According to KGHM vice-president Adam Bugajczuk, hydrogen can be used as a fuel and as a reducing agent in smelter furnaces. However, this is not possible without building a base, i.e. infrastructure, creating a network of links and relations with stakeholders, with the support of scientific and research facilities, etc. An important element in the creation of hydrogen valleys is cooperation between research institutes, universities, enterprises – from startups, clusters (so-called local content), to entities that have been on the market longer and have a stable financial position, such as local government units or, for example, State Treasury companies.[15] Also established are: Mazowiecka DW, Zachodnioeuropejska DW, Wielkopolska DW oraz Pomorska DW coordinated by the Hydrogen Technology Cluster. Within the latter, several projects are being implemented (as shown in Table 1).

Table 1. Projects implemented within the Hydrogen technology cluster

Project name	Area of activity
NeptHyne	Hydrogen production – wind farms in the Baltic Sea – seawater desalination project
PDA Support	Hydrogen vehicles in public transport, LOTOS Group, initially 10–15 buses, then more than 40
Pomeranian Hydrogen Valley	Hydrogen Technology Cluster Project
PCHET	Conference on coal technology
H2GLOBAL	Within the framework of the COSME – Programme for the Competitiveness of Enterprises and small and medium-sized enterprises 2014–2020 – the pursuit of cooperation with other European clusters.

Source: author's own elaboration based on: *Klaster Technologii Wodorowych*, https://klasterwodorowy.pl/nepthyne,127,pl [accessed: 22 March 2022].

Deputy Minister of Climate and Environment Ireneusz Zyska announced at the 14th TIME Economic Forum (March 2022) that a concept is being developed to establish a so-called hydrogen valley ecosystem operator in Poland. According to the minister, it is important that: "the valleys should not compete with each other exchange the knowledge and experience gained, and not duplicate the same projects

[14] "Powstała Śląsko-Małopolska Dolina Wodorowa", Agencja Rozwoju Przemysłu, 31 January 2022, https://arp.pl/pl/o-arp/dla-mediow/aktualnosci/powstala-slaskomalopolska-dolina-wodorowa [accessed: 8 April 2022].

[15] "Powstała Dolnośląska Dolina Wodorowa", KGHM Polska Miedź, 25 February 2022, https://media.kghm.com/pl/informacje-prasowe/powstala-dolnoslaska-dolina-wodorowa [accessed: 8 April 2022].

concerning the development of the hydrogen economy in Poland."[16] He also mentioned that a Polish centre for hydrogen technology and a Polish centre for hydrogen certification should be established, so that we can talk about an orderly structure for building a stable hydrogen market in Poland. Moreover, appropriate legal regulations are needed to define the framework for the activities of entities in the sector – work on the so-called 'constitution for hydrogen' is currently underway. This is a continuation of activities resulting from the *Polish Hydrogen Strategy until 2030 with an outlook until 2040.* Work is also underway on regulations on refuelling infrastructure (hydrogen can be used as fuel for fuel cell engines), i.e. hydrogen stations including their operation, modernisation, repair, inspection, or charging.[17] At the beginning of February 2022 PKN Orlen announced that it had signed an agreement with 17 cities to build hydrogen charging stations, including Krakow. In 2022, the first four are to be built, while by 2030, there is talk of 100.[18] It should be noted that according to the Polish Alternative Fuels Association, there were more than 70 vehicles in Poland that run on hydrogen in 2021. However, there is not a single station for charging them to date. This situation significantly limits the possibilities for the development of this sector.[19]

In 2017, the standard PN-ISO 37120:2015-03 *Sustainable social development – Indicators of urban services and quality of life* was made public. It addresses the so-called integrated approach to sustainable development. The aim is to measure the quality of life over a certain time horizon, the effects of activities, the exchange of information on applied solutions within the framework of reducing or changing consumption to an environmentally compatible style. For cities, the most important objective is to meet energy demand in a competitive, secure, low-carbon and affordable manner. Attention should therefore be focused on improving efficiency in transport, communication, transmission, etc.[20]

Warsaw and Krakow appeared in the *Smart Cities Index 2021*, which lists 118 cities. The preparatory work rested with two entities: Lausanne Business School

---

[16] "Zyska: Powstała koncepcja powołania operatora dolin wodorowych", Świat Rolnika, 9 March 2022, https://swiatrolnika.info/ekologia/oze/zyska-powstala-koncepcja-powolania-operatora-dolin-wodorowych-w-polsce.html [accessed: 12 April 2022].

[17] Projekt rozporządzenia Ministra Klimatu i Środowiska w sprawie wymagań technicznych dla stacji wodoru, Rządowe Centrum Legislacji, 10 February 2022, https://legislacja.rcl.gov.pl/projekt/12356050/katalog/12851708#12851708 [accessed: 8 April 2022].

[18] M. Pokorzyński, "Orlen zbuduje stacje tankowania wodoru. Pierwsze powstaną w tym roku", *Auto Świat*, 2 February 2022, https://www.auto-swiat.pl/ev/wiadomosci/orlen-zbuduje-stacje-tankowania-wodoru-pierwsze-powstana-w-tym-roku/m3bz72g [accessed: 8 February 2022].

[19] Polskie Stowarzyszenie Paliw Alternatywnych, https://pspa.com.pl/aktualnosci/ [accessed: 8 April 2022].

[20] *Smart Cities*, Polski Komitet Normalizacyjny, https://www.pkn.pl/smart-cities [accessed: 12.03.2022].

(IMD) and the Singapore University of Technology and Design. Aspects such as technology, transport, science, infrastructure, among others, were taken into account. A scale was created: from A to D, where the letter A indicates the best score. The 2021 report highlights health care issues as a consequence of the COVID-19 pandemic.[21]

Within the framework of Smart Cities in Poland, Białystok, Gdańsk, Gdynia, Kielce, Poznań, Rzeszów, Szczecin, Wrocław should also be mentioned. In these cities, investments are mainly focused on (building roads, car parks, constructing sports facilities, paving roads) promoting entrepreneurship and investments in environmental protection. In addition, cities are creating a policy of incorporating hydrogen as a solution to reduce carbon dioxide emissions, e.g. in Białystok, the Agricultural Hydrogen Valley was created to intensify activities in this area. On the other hand, Gdynia, Kielce, Gdańsk, Lublin and Warsaw have certificates for the ISO-37120 standard.[22] The concept of Smart Cities is not easy to define, one way is to identify the so-called versions: Smart City 1.0, Smart City 2.0 and Smart City 3.0. In version 1.0, the initiators of change were entities known in the IT or telecommunications industry, the essence was to increase demand for the modern products and solutions offered. In the next stage, 2.0, the focus was on local authorities, where the main objective was to improve the quality of life of the inhabitants, e.g. by promoting ecological solutions, universal accessibility to various amenities, e.g. the Internet. Version 3.0 is intended to respond to societal needs and, on the other hand, should implement top-down objectives, such as low-carbon. The relationship between the actor, the society and the local authority will be crucial here in building the country's energy security (by ensuring local security).[23] In Poland, cities are at the 2.0 stage, which gives rise to some optimism (number of ideas, cooperation within clusters), but on the other hand shows how much still needs to be done to be able to speak of stability, e.g. the legal environment and regulations to structure investments within clean hydrogen.

Urban development, raises issues of population movement, whether by public transport or one's own means of transport. This is why intelligent traffic planning (e.g. roads, bridges, tunnels, airports) and the appropriate connection of potential participants (by rail, air or car) is so important. This situation is not only the result of a progressive urbanisation process, but is also due to the bluntness of the environment, its unpredictability and its complexity, in terms of development. On the one hand, there is the technological development and increased consumption for products and

---

[21] *SCO Smart City Observatory*, https://www.imd.org/smart-city-observatory/home/ [accessed: 8 April 2022].

[22] P. Szpecht, "Idea smart city kuleje w Polsce. Może być źródłem oszczędności dla miast", 10 January 2022, https://www.wirtualnemedia.pl/artykul/smart-city-polska-zrodlo-oszczednosci-dla-miast [accessed: 8 April 2022].

[23] M. Zysk, "Idea Smart City 3.0, czyli inteligentne miasta w Polsce", 20 May 2021, https://cityislife.pl/design-i-sztuka/idea-smart-city-3-0-czyli-inteligentne-miasta-w-polsce [accessed: 8 April 2022].

services, and on the other, the growing awareness of resource depletion and the issue of environmental protection, the control and monitoring of processes and, consequently, the need to store large amounts of data.

Hydrogen is a solution to the Smart Cities idea, this is confirmed by investments in, among other things, hydrogen-powered buses. In Poland, the first examples are Gdansk and Gdynia, which tested Solaris Trollino 18 hydrogen trolleybuses in 2017. Manufacturers emphasise their greater efficiency than electric vehicles (longer range and cheaper servicing). In Krakow, for example, the Solaris Urbino 12 hydrogen bus was tested. In January 2021, cities were able to apply for project funding for the purchase of green and zero-emission buses from the *Green Public Transport* programme of the National Fund for Environmental Protection and Water Management. There was a huge amount of interest, with more than 100 applications for the use of hydrogen in public transport. These investments will exceed PLN 1 billion.[24] It should be noted that such solutions are already in use, e.g. Toyota's Woven City in Japan (as part of a collaboration between Toyota and Isuzu and Hino Motors).

Conclusions

To sum up the above considerations, green hydrogen is an important solution for creating a so-called zero-carbon economy. The events in Ukraine have accelerated the debate on the diversification of directions and sources of energy not only in the EU, but also worldwide. Energy independence is also essential and significantly enhances national security. There is no single solution for diversification from the monopoly supplier of raw materials to the European market – Russia. Each country has a different energy mix, a different policy, a differently developed industry, which significantly complicates rapid change. In addition, the EU's low-carbon strategy has long put pressure on countries where coal occupies a significant part of the energy mix, such as Poland. The examples cited above confirm the significant impact of hydrogen valleys on improving the competitiveness of the Polish economy and the possibilities within the creation of solutions in line with the Smart City idea. Investments in green hydrogen offer the possibility of generating energy in a way that is independent of other countries, which significantly improves Poland's energy security, first at the local level, and consequently for the whole country, these premises can be seen in government documents, statements by politicians or publications by individual entities. Which confirms the hypothesis assumed in the introduction. In addition, it is a solution that supports the EU's zero-carbon strategy. To the question of whether Poland will use hydrogen as a solution to meet EU requirements?

[24] "W polskich miastach pojawi się ponad 100 autobusów na wodór", Gramwzielone.pl, 14 March 2022, https://www.gramwzielone.pl/woddor/107489/w-polskich-miastach-pojawi-sie-ponad-100-autobusow-na-wodor [accessed: 22 April 2022].

It is difficult to answer in the affirmative at the present time. Poland has a so-called hydrogen strategy, so-called hydrogen valleys are being created cooperating with energy clusters and creating a whole network of cooperation at the local level. In order to achieve climate neutrality, legal regulations and an amendment to the RES Act are needed. The situation is similar here, investments need the support of the government not only in words (public statements), but appropriate legal regulations are required for this. This is the key to success, due to the visible bottom-up initiative, e.g. of companies at the local level.

References

Chodyński A., *Dynamika przedsiębiorczości i zarządzania innowacjami w firmach. Odpowiedzialność – prospołeczność – ekologia – bezpieczeństwo*, Kraków: Oficyna Wydawnicza KAAFM, 2021.

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *A hydrogen strategy for a climate-neutral Europe*, COM/2020/301 final, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020DC0301&from=pl [accessed: 8 April 2022].

Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, *The European Green Deal*, COM/2019/640 final, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52019DC0640 [accessed: 7 April 2022].

Directive (EU) 2018/2001 of the European Parliament and of the Council of 11 December 2018 on the promotion of the use of energy from renewable sources (recast), OJ L 328/82, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018L2001&from=PL [accessed: 7 April 2022].

European Commission, *Fit for 5*5, https://www.consilium.europa.eu/en/policies/green-deal/fit-for-55-the-eu-plan-for-a-green-transition/ [accessed: 7 April 2022].

Kancelaria Senatu, *Polska w Zielonym Ładzie – korzyści, możliwości i ocena SWOT*, Opinie i ekspertyzy, OE–307, Warszawa 2020, https://www.senat.gov.pl/gfx/senat/pl/senateksperty z/5619/plik/oe_307.pdf [accessed 8 April 2022].

"Kierunek przyszłości – biometan i biowodór", Portal Komunalny, 1 December 2021, https://portalkomunalny.pl/kierunek-przyszlosci-biometan-i-biowodor-428075 [accessed: 7 April 2022].

"Krajowy plan na rzecz energii i klimatu na lata 2021–2030 przekazany do KE", Ministerstwo Aktywów Państwowych, 13 December 2019, https://www.gov.pl/web/aktywa-panstwowe/krajowy-plan-na-rzecz-energii-i-klimatu-na-lata-2021-2030-przekazany-do-ke [accessed: 8 April 2022].

Pokorzyński M., "Orlen zbuduje stacje tankowania wodoru. Pierwsze powstaną w tym roku", *Auto Świat*, 2 February 2022, https://www.auto-swiat.pl/ev/wiadomosci/orlen-zbuduje-stacje-tankowania-wodoru-pierwsze-powstana-w-tym-roku/m3bz72g [accessed: 8 February 2022].

"*Polska Strategia Wodorowa do roku 2030 z perspektywą do roku 2040"* opublikowana w Monitorze Polskim", Ministerstwo Klimatu i Środowiska, 9 December 2021, https://www.gov.pl/web/klimat/polska-strategia-wodorowa-do-roku-2030-z-perspektywa-do-roku-2040-opublikowana-w-monitorze-polskim [accessed: 7 April 2022].

Polskie Stowarzyszenie Paliw Alternatywnych, https://pspa.com.pl/aktualnosci/ [accessed: 8 April 2022].

Portal Funduszy Europejskich, 1 September 2021, https://www.funduszeeuropejskie.gov.pl/strony/o-funduszach/fundusze-na-lata-2021-2027/konsultacje-spoleczne-kpo/o-kpo/ [accessed: 7 April 2022].

"Powstała Dolnośląska Dolina Wodorowa", KGHM Polska Miedź, 25 February 2022, https://media.kghm.com/pl/informacje-prasowe/powstala-dolnoslaska-dolina-wodorowa [accessed: 8 April 2022].

"Powstała Śląsko-Małopolska Dolina Wodorowa", Agencja Rozwoju Przemysłu, 31 January 2022, https://arp.pl/pl/o-arp/dla-mediow/aktualnosci/powstala-slaskomalopolska-dolina-wodorowa/ [accessed: 8 April 2022].

Projekt rozporządzenia Ministra Klimatu i Środowiska w sprawie wymagań technicznych dla stacji wodoru, Rządowe Centrum Legislacji, 10 February 2022, https://legislacja.rcl.gov.pl/projekt/12356050/katalog/12851708#12851708 [accessed: 8 April 2022].

Rządowy projekt ustawy o zmianie ustawy o odnawialnych źródłach energii oraz niektórych innych ustaw, Draft No. 1129, 26 April 2021, https://www.sejm.gov.pl/sejm9.nsf/PrzebiegProc.xsp?nr=1129 [accessed: 7 April 2022].

"Rzeszów sercem Podkarpackiej Doliny Wodorowej", Ministerstwo Klimatu i Środowiska, 18 May 2021, https://www.gov.pl/web/klimat/rzeszow-sercem-podkarpackiej-doliny-wodorowej [accessed: 7 April 2022].

SCO Smart City Observatory, https://www.imd.org/smart-city-observatory/home/ [accessed: 8 April 2022].

Smart Cities, Polski Komitet Normalizacyjny, https://www.pkn.pl/smart-cities [accessed: 12.03.2022].

Szpecht P., "Idea smart city kuleje w Polsce. Może być źródłem oszczędności dla miast", 10 January 2022, https://www.wirtualnemedia.pl/artykul/smart-city-polska-zrodlo-oszczednosci-dla-miast [accessed: 8 April 2022].

"W polskich miastach pojawi się ponad 100 autobusów na wodór", Gramwzielone.pl, 14 March 2022, https://www.gramwzielone.pl/woddor/107489/w-polskich-miastach-pojawi-sie-ponad-100-autobusow-na-wodor [accessed: 22 April 2022].

"Założenia do aktualizacji Polityki Energetycznej Polski do 2040 r. (PEP2040) – wzmocnienie bezpieczeństwa i niezależności energetycznej", Kancelaria Prezesa Rady Ministrów, 29 March 2022, https://www.gov.pl/web/premier/zalozenia-do-aktualizacji-polityki-energetycznej-polski-do-2040-r-pep2040--wzmocnienie-bezpieczenstwa-i-niezaleznosci-energetycznej [accessed: 29 March 2022].

Zysk M., "Idea Smart City 3.0, czyli inteligentne miasta w Polsce", 20 May 2021, https://cityislife.pl/design-i-sztuka/idea-smart-city-3-0-czyli-inteligentne-miasta-w-polsce/ [accessed: 8 April 2022].

"Zyska: Powstała koncepcja powołania operatora dolin wodorowych", Świat Rolnika, 9 March 2022, https://swiatrolnika.info/ekologia/oze/zyska-powstala-koncepcja-powolania-operatora-dolin-wodorowych-w-polsce.html [accessed: 12 April 2022].

Hydrogen use in Poland in the light of EU policy to move away from coal: the concepts of hydrogen valleys and smart and sustainable cities

Abstract

Hydrogen can be used in several ways, including as a raw material, fuel or as an energy carrier. Therefore, hydrogen becomes an object of interest not only to companies, but also to individual governments. The European Union (EU) promotes low-emission solutions, which entails giving up fossil fuels and adapting the energy mix to renewable energy. In addition, the war in Ukraine is reshaping relations on the energy market in Europe and beyond. The well-known concept of diversification takes on a new meaning, it is combined with efficiency and competitiveness in the event of a change in the directions and sources of energy. It should be emphasized that no CO_2 emissions are generated when using hydrogen. This fact becomes a passport to the implementation of the EU's low-emission goals by 2050. Poland is not energy self-sufficient, additionally it still bases its energy mix on fossil fuels, which consequently raises concerns about meeting the EU guidelines. Therefore, the aim of the study is, inter alia, showing the prospects for the implementation of the so-called hydrogen valleys and sustainable smart cities, as alternatives to, for example, EU guidelines, dependence of supplies on the Russian monopoly, inefficiency and inactivity of the energy sector in the long term. For the purposes of this analysis, a hypothesis has been formulated, which assumes that the use of hydrogen in the economy will significantly improve Poland's energy security in the long term. The following research question was asked: Will Poland use hydrogen as a solution to meet the EU requirements for a zero-emission economy?

Key words: EU, Poland, management, hydrogen valleys, Smart City, clusters, competitiveness, low-emission

BEZPIECZEŃSTWO TEORIA I PRAKTYKA
SECURITY THEORY AND PRACTICE
e-ISSN 2451-0718
ISSN 1899-6264
2022
No. 2 (XLVII)
DOI: 10.48269/2451-0718-btip-2022-2-005
Received: 13.05.2022
Accepted: 22.07.2022

Janusz Ziarko
Associate Professor, Andrzej Frycz Modrzewski Krakow University
https://orcid.org/0000-0002-9100-2807

Soft Systems Methodology in identifying and eliminating occupational safety hazards

Introduction

Many occupational safety and health (OSH) problems observed in companies are perceived as complex, open-ended, multidimensional or unsolvable. What are the key features of such problems and how do they differ from routine problems; and do we have ways of solving such problems? There is an ongoing discussion in the English-language literature about unsolvable problems. This paper presents the main thrust of this discussion in the context of Soft Systems Methodology (SSM) as a concept for dealing with such problems. In the Polish scientific literature, little attention has been paid to the identification of complex OHS problems and their solution. Nowadays, both theoreticians and practitioners dealing with OSH issues should focus more attention on finding ways to deal with these challenges, to solve complex problems. It has been recognised that standard approaches to improving OSH conditions, which are variable, uncertain, complex, ambiguous, are clearly inadequate and positive change impossible, as the required level of information about OSH risks and their determinants, as well as the clarity of objectives and ways to achieve them, is too difficult to achieve. On the other hand, it is well known that routinely applied analytical-reductionist approaches to solving OSH problems overlook factors such as values, perspectives, experiences or relationships between stakeholders. Solving complex problems requires reflection and debate on the nature of the problems and proposals for alternative solutions based on diverse views

and value frameworks.[1] Hence, the aim of the article was to indicate the potential for using systems thinking and SSM methodology in the area of identifying and solving complex OSH problems. The problem of consideration was encapsulated in the question: does SSM provide an organisational framework for implementing the process of finding solutions to complex problems and improving OSH? The research thesis was that the use of SSM and systems thinking in solving complex OSH problem situations, would translate into improved individual and organisational safety, into the creation of safe systems of work. The method used was a semi-systematic literature review[2] aimed at identifying selected determinants of SSM use in activities in the area of identifying and solving complex OSH problems.

Perceptions of workers' safety and health at work

Good occupational health of an employee is associated not only with the absence of illness, but also with his or her physical, mental and social well-being. It is conducive to employee productivity and organisations should strive to achieve high performance with the least possible commitment of resources. The most valuable business resource is the employee and their work. Therefore, employers as well as employees should be concerned about health and fitness, the wellbeing of all members of the workforce – a key factor in productive work. Health and fitness – crew wellbeing is a sense of job satisfaction and fulfilment related to work, with positive feelings related to the physical and social working environment.[3] It is also the full intrapersonal harmony of the worker, illustrated by the maximum working efficiency of all his/her systems and organs and the desired level of adaptability to the demands of the external environment.[4] Hence, the actions taken by occupational health and safety managers to ensure a safe and healthy working environment for employees, to create a safe system of work, should not only be a necessity related to compliance with labour law.[5] It is above all a systematic study of the objectives

---

1 B. Head, "Wicked Problems in Public Policy", *Public Policy*, vol. 3, no. 2, 2008, pp. 101–118, https://www.researchgate.net/publication/43502862_Wicked_Problems_in_Public_Policy [accessed: 25 April 2022].

2 H. Snyder, "Literature review as a research methodology: An overview and guidelines", *Journal of Business Research*, vol. 104, 2019 pp. 333–339, https://doi.org/10.1016/j.jbusres.2019.07.039.

3 E. Trzebińska, *Psychologia pozytywna*, Warszawa: Wydawnictwa Akademickie i Profesjonalne, 2008, p. 41.

4 A.M. Grant, M.K. Christianson, R.H. Price, "Happiness, Health or Relationships? Managerial Practices and Employee Well-Being Trade-offs", *Academy of Management Perspectives*, vol. 21, no. 3, 2007, pp. 52–53.

5 Ustawa z dnia 26 czerwca 1974 r. – Kodeks pracy [Labour code], Dz.U., 2020, item 1320, Section 10: Bezpieczeństwo i higiena pracy [Occupational safety and health].

and expected results contained in the strategies and policies of OSH management, the tasks performed and their scope, the means of work, tools and materials used, taking into account their contexts: competence, socio-cultural, environmental, to identify all physical and psychological risks and to define working methods that eliminate or minimise these risks.[6] It is important to act for OSH in such a way that each worker knows how to act, can act and wants to act for his own and other workers' health in order to improve, protect and save it.

OSH requires the management of the working conditions and behaviour of workers, ensuring the required level of protection of their health and life. Work organisers do not always recognise the complexity of OSH risk issues, which consists of a number of soft factors and conditions that must be taken into account and met in order to make the working environment safe. Failure to take even one element into account can seriously undermine safe working conditions, generating disorders at work that result in disease states. Achieving the desired level of OSH is also conditioned by the conceptual scope and understanding of the terms OSH and safe system of work.

Carlo Caponecchia and Anne Wyatt[7] offer an extended definition capturing the content scopes of terms important to OSH, which is in line with general legal requirements. It reads: a safe and healthy/hygienic system of work is characterised by an integrated, continuously improving set of measures taken within a specific work context, which together are to:

- ensure that working environments, processes, procedures and tasks are designed to minimise the likelihood of hazards causing physical or mental harm to employees but also, for example: to customers, passengers, visitors or members of the public;
- identify and control all actual and foreseeable risks on an ongoing basis and keep them at acceptable levels;
- minimise the damage caused by OSH risks associated with physical and psychological injuries and facilitate workers' return to work after an accident.

One aspect that distinguishes the proposed definition is the emphasis on the importance of work design to achieve a safe system of work. The definition emphasises the importance of integrating the various activities related to the elimination of OSH hazards. The combination of these can be helpful in ensuring safety, as opposed to activities that focus on individual hazards or single controls. It also focuses on proactive preventive OSH strategies and actions, rather than less effective strategies to control risks after problems have occurred. Such a proactive approach to creating a safe system of work is integral to productivity and achievement related to organisational goals, good quality of work and life, later economic outcomes. Proper

---

6 C. Caponecchia, A. Wyatt, "Defining a 'Safe System of Work'", *Safety and Health at Work*, vol. 12, no. 4, 2021, pp. 421–423.

7 *Ibidem*.

OSH management influencing the organisation of work, building a safety culture and developing OSH competencies promotes the creation of a safe work system.

Hazards as complex, multidimensional socio-technical OSH problems

Health and safety problems are distinguished clusters of factors/conditions and/or employee behaviours that generate hazards and their negative effects on an individual and/or a larger number of employees and that are widely recognised by employees as harmful factors/conditions and/or behaviours that need to be diagnosed and eliminated or to achieve the desired form or course of action. The definition of an OSH problem has both *objective* and *subjective* elements. The objective elements are the empirical evidence of the negative impact of threatening factors or employee behaviours, while the subjective components include perceptions, valuations and judgements of the interplay of different factors and/or employee behaviours as to whether they are indeed OSH problems that need to be addressed. Many factors in the work environment are hazards to the worker: dangerous, harmful or disruptive, creating difficult and/or impossible problems for OSH. They are multidimensional in the sense that they represent extensive, intricate, multi-track, interconnected sets of socio-technical factors and conditions. Describing, explaining and understanding them poses a number of difficulties, hence it is difficult to propose specific actions for OSH and to predict their results. The difficulties observed in workplaces in ensuring the desired level of OSH, including the solution of complex, multidimensional situations generating OSH risks, are due to the fact that attempts are being made to solve these problematic situations with ordinary management techniques, and this is a fundamental mismatch. More often than not, projects aimed at improving OSH are oriented towards reducing deficits, for example resulting from post-accident conclusions, i.e. based on past experiences and top-down guidelines, while the actual problematic challenges are decentralised, interconnected, multifaceted, trend-based and difficult to define.

The question arises: what approach and what tools should be used to make them useful for solving complex health and safety problems? Let us first look at: a) the way we most often analyse problems, and b) what characteristics we give to problems.

Re a) the observed OSH threat is broken down by the analyst into multiple elements/scenes, into smaller fractions, each with its own specific logic and associated analytical decisions. These concern the people who will be considered, the contexts in which they will be located, their attitudes, their beliefs about the situation and associated behaviours, the objects and tools they will use, and the ways in which they relate to others. The definition being created to describe and explain the problem takes into account groups of information focusing on the construction of a specific situational element/scene, where the motive for gathering information was the scene

highlighted, rather than the nature of the problem, which sees the links that exist between its elements and brings them all together.

Re b) we assume, following Jeff Conklin,[8] that we often treat problems as well-structured and having characteristics:

- relatively well-defined and stable instructions for solving the problem;
- a specific stopping point, i.e. we know when the objective or solution has been reached;
- a solution that can be objectively assessed as good or bad;
- belong to a class of similar problems that can be solved in a tried and tested way;
- solutions that can be practised, improved and possibly discarded.

Well-structured problems are characterised by the fact that a) the quantities/information given and sought, related to the problem, are always well-defined, b) the problem is only solved once the analyst has accumulated sufficient solution knowledge to explain and understand the problem.[9] The question arises: is this analytical approach sufficient to clarify and solve OSH hazard problems?

In responding, we draw attention to the fact that OSH risks are difficult to identify precisely because they concern professional situations involving many colleagues with significant differences: value systems, beliefs, needs, expectations, tasks performed or competences. Characteristically, many of the characteristics of a threatening situation are not known or not well defined, for example, the actual goals pursued by the participants in the situation are unclear and the directly available information is insufficient to know and solve the problem. Difficult problems also provide reliable information, enough to infer what is going on in the situation, and this allows the problem to be defined, to identify options for solving it.

An example of a complex problem is the constantly observed threat of mobbing in the work environment – consisting of persistent harassment, bullying, intimidation, use of psychological violence against a subordinate or co-worker in the workplace. The measures taken to overcome the problem, including educational, preventive measures, often do not find recognition among co-workers, nor do they stop the bullies from carrying out their intentions. We see that often preventive measures do little to reduce the threat and increase the sense of security of employees. Bullying is a complex problem, affecting employees, the organisational environment and the very quality of being an employee very negatively. Although we know the extent of the impact of bullying on a person's mental state, that even seemingly harmless bullying attacks can lead to chronic anxiety, fatigue, job burnout and even depression, we do not react. Addressing the complex problem of bullying requires

[8] As cited: T. Ritchey, *Wicked problems: Structuring social messes with morphological analysis*, Swedish Morphological Society, Discussion Paper, 2007, https://www.academia.edu/715659/Wicked_problems_structuring_social_messeswith_morphological_analysis [accessed: 8 December 2021].

[9] C. Kupisiewicz, *O efektywności nauczania problemowego*, Warszawa: PWN, 1960, p. 93.

a multifaceted diagnosis of the problem. It is also important that the community facing the problem of reducing bullying and improving its safety engages in different ways to create possible solutions.

The boundary between well-structured and ill-structured problems is unclear, fluid and not amenable to formalisation. Badly structured problems are complex, multidimensional problems, generally the opposite of well-structured problems. They do not have definitive solutions or rules that inform the achievement of a solution. Complex problems are often complicated, twisted, continuous and resistant to complete solution, and their solutions are not necessarily good or bad.[10] Each complex problem is fundamentally unique, requiring a specific rather than a standardised approach to solution. Horst W.J. Rittel and Melvin M. Webber[11] have given ten characteristics of complex, unstructured problems:

1) There is no definitive formulation of the complex problem, i.e. even the definition and scope of the problem is contested;
2) Complex problems do not have a 'stopping rule', i.e. they do not have a definitive solution;
3) Solutions to complex problems are not true or false, but good or bad in the opinions of stakeholders;
4) There is no immediate or definitive test for solving a complex problem;
5) Any solution to a complex problem is a 'one-off operation'; results cannot be easily undone and there is no possibility of learning by trial and error;
6) Complex problems do not have a clear set of potential solutions, nor is there a well-described set of acceptable operations that can be incorporated into the plan;
7) Each complex problem is fundamentally unique;
8) Each complex problem can be seen as a symptom of another problem;
9) Existing discrepancies in a complex problem can be explained in a number of ways;
10) The planner has no 'right to err', i.e. there is no social tolerance for initiatives or experiments that fail.

Open problems usually have several viable solutions. Each solution has strengths and weaknesses, it has advantages and disadvantages, which are evaluated according to who is affected by the problem and how it is solved. It is important to be aware that there is no single 'right' solution, and that the chosen solution should be recognised by the majority of employees. It is therefore necessary to consider what the key factors

[10] H.A. Simon, "The Structure of Ill Structured Problems", *Artificial Intelligence*, no. 4, 1973, pp. 181–201, https://ojs.unbc.ca/index.php/design/article/viewFile/1273/1090 [accessed: 25 April 2022].

[11] H.W.J. Rittel, M.M. Webber, "Dilemmas in a general theory of planning", *Policy Sciences*, vol. 4, 1973, pp. 155–169, [as cited in:] B. Head, *op. cit.*

are that trigger the risk, sustain it and often make it impossible to eliminate it, how to recognise them and then eliminate them. If their elimination is not possible, it is worth minimising their impact.

Soft Systems Methodology *versus* problematic health and safety situations

The problem: is OSH: a) a concrete reality, consisting of real elements, or b) an emergent reality, through values and meanings subjectively attributed to factors of the work environment and work itself by workers? The systems thinking that grows out of reflection on the question posed rejects the thesis of a concrete reality of OSH and inclines towards the view that it is an area with an emergent structure, extremely complex and changing. This makes OSH a multifaceted and multilevel reality, the cognition of which requires a multidirectional coupling of human perceptual, intellectual and emotional activities.[12] Researchers such as Peter B. Checkland have begun to argue that 'human systems' are diverse, and that their description and understanding of how to confront the problems we face in our daily work should be done on the basis of the meanings people give to the world.[13] Soft Systems Methodology (SSM) is a form of systems thinking by Checkland that allows us to perceive, describe and explain social reality as a construct of interpretations of human experience. SSM, as proposed by Checkland, is a method of structuring complex problems and developing desirable and feasible changes that are accepted by a diverse group of people. For example, such a heterogeneous team of employees may consist of: blue-collar workers, administrative staff, management staff, programmers, customers, making each of them perceive and interpret the problem differently. Checkland described SSM as a structured, flexible process for dealing with what are considered to be problematic, disordered situations that require structured action to improve. Thus, SSM is a participatory methodology, bringing together stakeholders with different worldviews and perspectives and involving them in constructive deliberations to determine the meaning of a problem, assuming that it transcends cultural or cognitive boundaries, the stakeholder(s) and the organisation. SSM stimulates a team approach to discussing the problem situation and related insights and ideas. This approach serves to better guide development and present new ways of making the problem situation more acceptable, less fraught with tension

---

[12] K. Dąbrowski, *Trud istnienia*, Warszawa: Wiedza Powszechna, 1986, p. 14.

[13] P.B. Checkland, *Systems Thinking, Systems Practice*, Chichester–New York: Wiley, 1981, [as cited in:] S. Simon-Solomon, *Systems Thinking in the Workplace – An Action Research Approach*, Research Paper, University of Missouri–St. Louis, https://www.umsl.edu/~sauterv/analysis/F08papers/Simon_Solomon_Systems_Thinking_in_the_Workplace.html [accessed: 1 May 2022].

and unanswered questions.[14] SSM is particularly useful for developing realistic action plans to solve complex socio-technical situations where people are: confused, have different views about the nature and origin of the problem, where they differ about the goals to be achieved to solve the problem and the possible ways to achieve them. In plans created using SSM, neither a set of health and safety requirements to which the work system should conform is developed, nor is such a system designed. SSM is used to create a set of feasible and environmentally acceptable actions that can be taken to improve the actual problem situation. These actions should be as helpful as possible in creating a set of organisational process improvements, where a process is a set of organisational tasks performed intentionally by employees. The core of SSM is the identification of activities to bridge the gap between the 'actual problem situation' and the 'conceptual picture of the desired situation' emerging in the thoughts of the people involved.

An important idea to support SSM is to involve project stakeholders in learning the problem situation together, as equal members of the team. Encouraging the sharing of their experiences, which helps stakeholders to understand the situation more fully. To inspire stakeholders to creatively find solutions in collaboration and consensus. SSM debates help people understand each other, accept different worldviews and reach a common judgement that can be the basis for action to overcome a problematic situation. This makes it easier to coordinate a team across divisional boundaries.[15]

We note that SSM prefers to capture 'problem situations' in which the actors are people, and does not use the concept of a problem. Assuming that there is a problem we assume that there is a solution to the problem and that finding this solution will make the problem disappear. In reality, problems do not disappear, so the aim of SSM is to learn about the problem situation and to propose feasible actions that bring about the desired changes accepted by the stakeholders.[16] Therefore, Checkland believes that the SSM process, is a structured process of thinking about and learning ways to make changes that take into account the different perceptions of the situation by its participants, depending on their worldview. Learning facilitates a better understanding of the problem situation as an unstructured 'soft' problem in any organisational or social context, by the people involved. It allows reasonable actions to be

[14] P. Checkland, J. Poulter, *Learning for Action: A Short Definitive Account of Soft Systems Methodology, and its use for Practitioners, Teachers and Students*, Chichester, UK: Wiley, 2006, pp. 4–5.

[15] D. McDonald, G. Bammer, P. Deane, *Research integration using dialogue methods*, Chapter 3: *Dialogue methods for understanding a problem broadly: integrating judgments: Soft Systems Methodology*, http://press-files.anu.edu.au/downloads/press/p60381/mobile/ch03s10.html [accessed: 30 April 2021].

[16] P. Checkland, J. Poulter, *Soft Systems Methodology*, [in:] *Systems Approaches to Managing Change: A Practical Guide*, eds. M. Reynolds, S. Holwell, London: Springer, 2010, p. 191.

taken to improve the problem situation and finally it is a process based on a specific set of ideas, namely systemic ideas.[17]

However, little is known so far about the usefulness of SSM for investigating and resolving problematic OHS situations. It is thought that the use of SSM in the area of OSH provides: 1) the participation of different representatives of the work environment in a design focused on improving OSH; 2) an excellent approach for revealing multiple situational perspectives in the analysis of a problem, for exploring alternatives to serve the relevance of decisions. How we use SSM and what impact it will have on OSH depends on: 1) treating what workers do in the course of their duties as purposeful systems; 2) declaring their views on the origins of OSH and its risks and revealing the assumptions made about how they perceive, understand, interpret OSH, its place in the hierarchy of importance of needs, and the contexts from the perspective of which we define OSH, such as: attitudes, beliefs, perceptions and actions of people variously involved in OSH problem situations; 3) treating SSM as a learning system to help learn about hazards, identify their course and impact on other phenomena, assess their probable and actual effects, and find facilities to take preventive and precautionary action.[18]

Application of SSM as an action learning system for OSH

Actual OSH problems are difficult, complex problems, containing many tangled sub-problems that cannot be untangled – and therefore cannot be objectively defined.[19] We can, however, define the problems associated with the various malfunctioning activities, or hazardous events of importance to OSH, occurring in the problem situation. The fundamental principle of SSM is the whole system. Then, thinking systemically about the problem situation, we select from it those elements that, in our subjective opinion, contribute to the incorrect execution of an action or the occurrence of a specific hazardous event. We treat these instances as systems, define them and set their boundaries. We exclude the remaining elements from our analysis of the problem.

According to the SSM, the defined systems are spheres of human activity. They are called core definitions. Appropriately named and described, they make it possible to build models depicting the dynamics of the case under study – a fragment of a problem situation – illustrating the functional conditions of the analysed activity

---

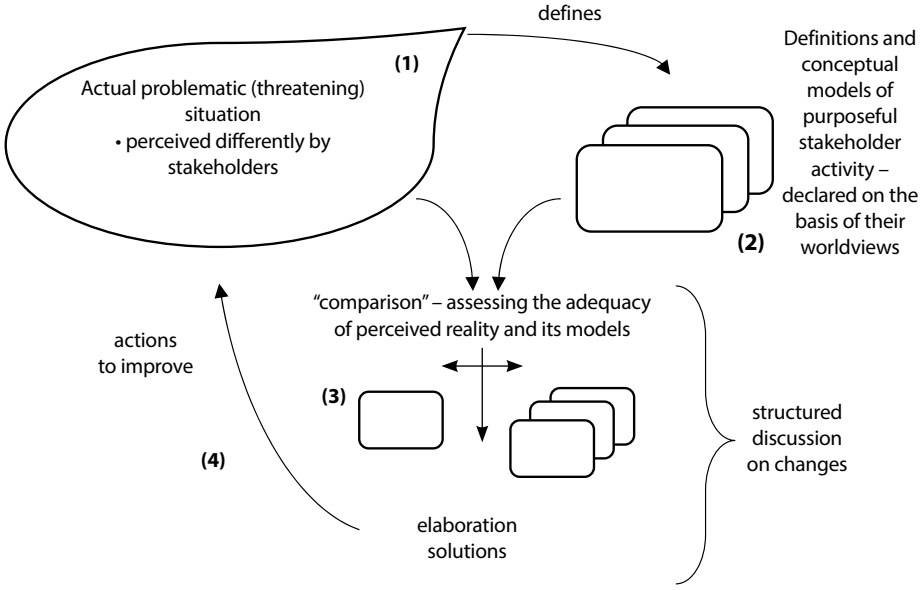
17 P. Checkland, J. Poulter, *Learning for Action…*, *op. cit.*, p. 4.

18 P. Checkland, J. Scholes, *Soft Systems Methodology in Action*, Chichester, UK: John Wiley and Sons Ltd., 1999, [as cited in:] *Soft Systems Methodology. Introduction to SSM*, Improvising Design, https://blog.improv-design.com/soft-systems-methodology/introduction-to-ssm [accessed: 1 May 2022]; T. Kocowski, *Potrzeby człowieka. Koncepcja systemowa*, Wrocław, Warszawa–Kraków–Gdańsk–Łódź: Ossolineum, 1982, p. 40.

19 H.W.J. Rittel, M.M. Webber, *op. cit*.

system and its effects/consequences. In SSM, hierarchy is also important. A problem should be looked at from different levels of resolution, with each level being characterised by an emergent pattern of system behaviour (emergence), generating specific effects of that behaviour. The concepts of hierarchy and emergent properties are fundamental to the SSM approach.[20] Related to hierarchy and emergent properties of systems are the concepts of communication and control. The realisation of the system's objectives and its course are determined by the quality of communication between system actors and the effectiveness of control. Seeking to improve a problem situation using SSM is a way for the actors in that situation to engage in collaborative learning about the actual problem situation in order to explore relevant perspectives on its goals, processes and what needs to change. SSM analyses should allow the analyst to see and assess hitherto unrecognised flaws in the existing work system, and within it the factors and their interrelationships affecting OSH. Moreover, if such defects are detected, SSM enables the reflective analyst to make recommendations and take action to improve the work organisation and eliminate OSH risks. The SSM model is shown in Figure 1.

Figure 1. Iconic representation of the SSM learning cycle



Source: compiled from: P. Checkland, "Soft Systems Methodology: A Thirty Year Retrospective", *Systems Research and Behavioral Science*, vol. 17, 2000, p. 16, https://download.clib.psu.ac.th/datawebclib/e_resource/trial_database/WileyInterScienceCD/pdf/SRBS/SRBS_4.pdf [accessed: 1 May 2022].

[20] N.V. Patel, "Application of soft systems methodology to the real world process of teaching and learning", *International Journal of Educational Management*, vol. 9, no. 1, 1995, pp. 13–23, https://www.measureevaluation.org/resources/training/capacity-building-resources/basic-me-concepts-portuguese/Methodologies_IS_Development.pdf [accessed: 7 May 2022].

When undertaking an analysis of a threatening health and safety situation (stage 1), using SSM, the intention is to accurately identify and fully understand the problem posed by the threat, which requires gathering complete and accurate information about it. The analysis focuses on identifying those situational issues that the people involved in the situation consider to be problematic. We begin by describing and explaining each stakeholder's understanding of the phenomena generating the OSH hazards. Each stakeholder is, as it were, at the centre of the work system and is surrounded by a number of elements with which they interact. He or she perceives risk-generating situations, in unstructured form, from his or her own perspective: that of the human worker. They offer their opinions and views about the situation, e.g. about the events and processes generating health and safety problems, the cultural values and norms in force, or power relations and opportunities for improvement. Each of them, using their own mental models, sees the same situation differently and makes a different judgement about it. They describe it, taking into account the local socio-organisational context in which the work is done. He or she depicts his or her role in the situation and how it relates to other elements of the situation, such as, for example: colleagues, tasks, tools, technology, physical environment and organisational problems. Refers to the prevailing culture, social and organisational structure in the organisation. Recognises and demonstrates the importance and impact of culture and organisational structure, as well as the organisation itself, on the behaviour of colleagues. In particular, it shows how employees actually interact with elements of the situation and which are potentially the source of the developing threat.[21]

The participants in the problem situation then sort out this disorder in order to capture the diversity of perceptions and views of the situation, presenting it by drawing a rich picture. This is often a visual representation, not of the problem-threat, but of the situation in which this threat evolves and is dangerous. The picture depicts/describes the participants in the situation and the problems they are experiencing, it illustrates the connections between the participants in terms of their roles, the tasks they perform and how they perform them. It serves, through the identification of the problem situation, the learning of the stakeholders, their accumulation of knowledge about the causes and effects of situational health and safety risks. Learning, this creation and agreement of rich images, is a source of inspiration for the situation's stakeholders indicating those aspects/elements of the situation related to human activities that need to be named and represented in the form of conceptual models. The rich image does not attempt to model the situation in a precise way. It is a representation of how a team of stakeholders together might look at and think about a problematic situation. The picture can be refined as understanding of the situation becomes

[21] P. Carayon, P. Hancock, N. Leveson, *et al.*, "Advancing a sociotechnical systems approach to workplace safety – developing the conceptual framework", *Ergonomics*, vol. 58, no. 4, 2015, pp. 548–564, https://pubmed.ncbi.nlm.nih.gov/25831959/ [accessed: 3 May 2022].

more complete and the relationships within it become clearer.[22] The rich picture of our area of interest essentially has two components: 1) a structure component and 2) a process component. When creating a rich picture, it is necessary to use material and symbolic elements separated from the problem situation and present them in the form of a structure generating a specific pattern of behaviour, generating a threat (having specific emergent properties). Such elements in a problematic bullying situation, for example, would be: the employees of the team, the tasks performed by the employees, the relationships occurring between the employees and the employees and the tasks they perform, and the boundary separating these elements. The second component deals with the processes of interest generated by the structure in question. The elements to be included here essentially answer the question "what is happening?; who, what is the perpetrator?; why is it happening?" Such elements could be, among other things, a violent communicative supervisor–subordinate relationship, having the characteristics of bullying, and the attitudes of other employees witnessing such communicative behaviour. The relationship between structure and process influences a situational climate that overwhelms employees in a problematic situation related to an existing OSH risk.

The structures, processes and problems of the organisation, presented in a rich picture, provide the basis for naming and formulating the basic definitions of the problem (stage 2). These will allow to separate, name and describe the objectives and activities of the different subsystems of employee activity in the problem situation that contribute to the activation of OSH risks. Creating a master definition involves two steps and clarifies two aspects of the focus area for further analysis. The first is to select from the rich picture the problem(s) or task(s) that need to be addressed, i.e. to identify the problem behaviours/activities – that is, all those elements that need improvement. The second step is to identify and define the system, which is the system of human activity that creates the problem(s) and becomes the focus of concern and that will be used for further analysis related to problem solving and/or task performance.

Master definitions are formulated in a way that is useful for investigating and proposing a solution to a problem situation. In the course of formulating a definition, a given threatening element (input to the system) is transformed into an acceptable form (output).

The main definition may start with the words (entry into the action system) "in the communication of the manager with some subordinates, aggressive wording prevails ...., which are perceived by employees as ..., causing them ... states; which often results in reduced performance...," followed by an idea-proposal formulated as a deliberate

[22] P. Checkland, "Autobiographical Retrospectives: Learning your way to 'action to improve' – the development of soft systems thinking and soft systems methodology", *International Journal of General Systems*, vol. 40, no. 5, 2011, pp. 487–512.

transformation of communicative problem situations into situations... (exits from the action system).

A master definition defines what is being transformed, by whom and for what purpose. Helpful in formulating master definitions is the mnemonic CATWOE,[23] which facilitates the questions: 1) Who is/are the client(s) (C)? 2) Who are the actors (A)? 3) What is the transformation about (T)? 4) What are the world views of the stakeholders (W)? 5) Who is the owner of the system (O)? 6) What are the environmental conditions (E)? For the problematic bullying situation in question, we identify the following key elements of the system,[24] answering the questions:

- Customer: Who is served by the improved system? – people who feel at risk in terms of health and safety;
- Actors: who will perform the transformation process activities? – Employees performing the activities defined in the system – manager, health and safety officer, staff;
- Transformation process: What process will transform the input data into output data? – showing how a system – a problem-eliminating structure (output data) is created from the input data (taken from the rich image);
- Stakeholder worldviews: What view makes this transformation worth the effort? Stakeholders' worldviews mean that the transformation process should be considered and created with contexts in mind;
- Owner: who has the right to say whether a system will be implemented or not? – Every system has an owner who has the right to start or stop the system;
- Environmental constraints: what are the constraints that may prevent the system from operating? Elements that exist outside the system that affect transformation processes and system operation.

The core definitions form the basis for the construction of conceptual models, which models present a clear arrangement of actions intended to be implemented by transformative actors. These are models of purposeful action that can be considered relevant to the debate and dispute on how to solve a problematic situation. At this stage of the SSM methodology, they are not considered as practical projects. They usually take the form of a layout/map of actions needed to bring about improvements in the system of action. In step one of building such models, the layout of activities is specified to then show how these activities are interrelated and complementary. For example, the actions required for a transformation that eliminates aggressive forms of communication (bullying communication) that violate the wellbeing of the other can be put as follows:

1) Identify the conditions/requirements for safe communication behaviour (verbal and non-verbal) desired in the organisation;

---

[23] P. Checkland, J. Poulter, *Soft Systems Methodology*, *op. cit.*, p. 221.

[24] *Ibidem*.

2) Disseminate/inform about the requirements related to the improvement of the communication culture eliminating aggressive communication;
3) Identify ways of aggressive highly undesirable communication behaviour that should be stigmatised;
4) Monitor incidents of aggressive communication (verbal and non-verbal) affecting the well-being of another person;
5) Record people breaking the rules of safe communication behaviour (verbal and non-verbal) and identify what the breach consisted of and what the consequences were;
6) Inform about incidents of aggressive forms of communication, stigmatise them;
7) Enforce the use of safe communication behaviours (verbal and non-verbal) that do not compromise the welfare of the other person;
8) Monitor progress in improving communication culture, take corrective/improving actions;
9) Evaluate the impact of the measures applied on improving the communication culture and eliminating undesirable communication behaviour;
10) Keep employees informed of the results of efforts to improve the communication culture.

Working with models, is the comparison of conceptual models with the real world, rich images representing problem situations, and the debate related to the results of these comparisons. This is another SSM activity to ensure the preparation of an ever better set of actions/recommendations, in line with the priorities for change/transformation contained in the core definitions, to be introduced into existing action systems. The outcome of the debate should be the identification of streamlining changes that meet two criteria: systemically desirable and culturally feasible in a given situation.

Conclusions

SSM is a significant step in methodologies for dealing with OSH problem situations to improve working conditions, translating into higher safety and better health for workers. It allows going beyond the traditional ways of doing things for OSH (which activates after the fact of an accident at work), and favours proactive ways, focusing attention on latent or emerging risks, exploring and developing the potential of work systems to meet the growing OSH challenges of new technologies or a more competent workforce.

References

Caponecchia C., Wyatt A., "Defining a 'Safe System of Work'", *Safety and Health at Work*, vol. 12, no. 4, 2021, pp. 421–423.

Carayon P., Hancock P., Leveson N. *et al.*, "Advancing a sociotechnical systems approach to workplace safety – developing the conceptual framework", *Ergonomics*, vol. 58, no. 4, 2015, pp. 548–564, https://pubmed.ncbi.nlm.nih.gov/25831959/ [accessed: 3 May 2022].

Checkland P., "Soft Systems Methodology: A Thirty Year Retrospective", *Systems Research and Behavioral Science*, vol. 17, 2000, p. 16, https://download.clib.psu.ac.th/datawebclib/e_resource/trial_database/WileyInterScienceCD/pdf/SRBS/SRBS_4.pdf [accessed: 1 May 2022].

Checkland P., Poulter J., *Learning for Action: A Short Definitive Account of Soft Systems Methodology, and its use for Practitioners, Teachers and Students*, Chichester, UK: Wiley, 2006.

Checkland P., Poulter J., *Soft Systems Methodology*, [in:] *Systems Approaches to Managing Change: A Practical Guide*, eds. M. Reynolds, S. Holwell, London: Springer, 2010, pp. 191–242.

Checkland P., "Autobiographical Retrospectives: Learning your way to 'action to improve' – the development of soft systems thinking and soft systems methodology", *International Journal of General Systems*, vol. 40, no. 5, 2011, pp. 487–512.

Dąbrowski K., *Trud istnienia*, Warszawa: Wiedza Powszechna, 1986.

Grant A.M., Christianson M.K., Price R.H., "Happiness, Health or Relationships? Managerial Practices and Employee Well-Being Trade-offs", *Academy of Management Perspectives*, vol. 21, no. 3, 2007, pp. 51–63.

Head B., "Wicked Problems in Public Policy", *Public Policy*, vol. 3, no. 2, 2008, pp. 101–118, https://www.researchgate.net/publication/43502862_Wicked_Problems_in_Public_Policy [accessed: 25 April 2022].

Kocowski T., *Potrzeby człowieka. Koncepcja systemowa*, Wrocław, Warszawa–Kraków–Gdańsk–Łódź: Ossolineum, 1982.

Kupisiewicz C., *O efektywności nauczania problemowego*, Warszawa: PWN, 1960.

McDonald D., Bammer G., Deane P., *Research integration using dialogue methods*, Chapter 3: *Dialogue methods for understanding a problem broadly: integrating judgments: Soft Systems Methodology*, http://press-files.anu.edu.au/downloads/press/p60381/mobile/ch03s10.html [accessed: 30 April 2021].

Patel N.V., "Application of soft systems methodology to the real world process of teaching and learning", *International Journal of Educational Management*, vol. 9, no. 1, 1995, pp. 13–23, https://www.measureevaluation.org/resources/training/capacity-building-resources/basic-me-concepts-portuguese/Methodologies_IS_Development.pdf [accessed: 7 May 2022].

Ritchey T., *Wicked problems: Structuring social messes with morphological analysis*, Swedish Morphological Society, Discussion Paper, 2007, https://www.academia.edu/715659/Wicked_problems_structuring_social_messeswith_morphological_analysis [accessed: 8 December 2021].

Simon H.A., "The Structure of Ill Structured Problems", *Artificial Intelligence*, no. 4, 1973, pp. 181–201, https://ojs.unbc.ca/index.php/design/article/viewFile/1273/1090 [accessed: 25 April 2022].

Simon-Solomon, *Systems Thinking in the Workplace – An Action Research Approach*, Research Paper, University of Missouri–St. Louis, https://www.umsl.edu/~sauterv/analysis/F08papers/Simon_Solomon_Systems_Thinking_in_the_Workplace.html [accessed: 1 May 2022].

Snyder H., "Literature review as a research methodology: An overview and guidelines", *Journal of Business Research*, vol. 104, 2019 pp. 333–339, https://doi.org/10.1016/j.jbusres.2019.07.039.

Soft Systems Methodology. Introduction to SSM, Improvising Design, https://blog.improv-design.com/soft-systems-methodology/introduction-to-ssm [accessed: 1 May 2022].

Trzebińska E., *Psychologia pozytywna*, Warszawa: Wydawnictwa Akademickie i Profesjonalne, 2008.

Ustawa z dnia 26 czerwca 1974 r. – Kodeks pracy [Labour code], Dz.U., 2020, item 1320.

Soft Systems Methodology in identifying and eliminating occupational safety hazards

Abstract

Soft Systems Methodology (SSM) and occupational safety and health (OSH) are areas of human knowledge and interest that are important to, but relatively independent of, each other. SSM uses the idea of systems to find solutions to complex, poorly defined, so-called soft problems that we face in work environments. The aim of this article was to identify the potential for using systems thinking and SSM methodology in the area of identifying and solving complex health and safety problems. The method used was a semi-systematic literature review aimed at identifying selected determinants of the use of SSM in activities to improve OSH.

It was pointed out how important it is for the effectiveness of OSH undertakings to be able to use SSM and systems thinking as a structured and systematic approach to analysing and eliminating occupational safety and health hazards present in the working environment.

Key words: systems thinking, Soft Systems Methodology, problem situation, occupational safety and health (OSH), health and safety risks

BEZPIECZEŃSTWO TEORIA I PRAKTYKA SECURITY THEORY AND PRACTICE
e-ISSN 2451-0718
ISSN 1899-6264
2022
No. 2 (XLVII)
DOI: 10.48269/2451-0718-btip-2022-2-006
Received: 28.04.2022
Accepted: 18.07.2022

Agnieszka Giszterowicz
PhD, Andrzej Frycz Modrzewski Krakow University
https://orcid.org/0000-0003-3900-6795

Operationalising a safety culture in the management of a business entity (case study)

Introduction

The topic of developing a safety culture is of great interest to businesses. This is evidenced by the ever-increasing number of organisations implementing CE or B (construction) certification. Safety culture – in addition to quality and environmental culture – determines a positive image, competitive advantage and financial benefits. Safety culture can be considered from the point of view of philosophy, sociology, anthropology, economics and management, as evidenced by Andrzej Chodyński's rich compilation of terms, definitions and points of reference.[1] The purpose of this article, however, is to look at safety culture as an object of economic accounting and to answer the questions: can safety culture be an object of operationalisation based on the principle of dualism dominating in accounting? Can safety culture, therefore, be a measurable category using the profitability index developed on the basis of the scientific theory of capital?

Conducting empirical research into safety culture requires the adoption of a specific path of inquiry. The path of cognition in this case can be made the so-called scientific approach. The same one that applies to the category of capital. It is characterised

[1] A. Chodyński, *Dynamika przedsiębiorczości i zarządzania innowacjami w firmach. Odpowiedzialność – prospołeczność – ekologia – bezpieczeństwo*, Kraków: Oficyna Wydawnicza KAAFM, 2021, pp. 141–143.

in detail in the study by Agnieszka Giszterowicz.[2] It is an approach grounded in accounting theory. It appears that safety culture is a category that can be described by the characteristics with which intellectual capital is also described and defined, and then the operationalisation tools developed on the basis of accounting theory can be applied to it. In this study, a generalised profitability indicator, the ROAH model, is used to identify and value safety culture.

The first part of the article pursues theoretical and cognitive objectives related to intellectual capital, operationalisation and safety culture, while the second part is devoted to empirical research. Answers to the research problems posed are provided by literature analysis, financial document analysis and a case study.

Safety culture and intellectual capital

The category of safety culture is included in the broader category of culture, i.e. the totality of the spiritual and material achievements of society.[3] Safety culture as a domain of culture has accompanied humanity since the beginning of time. Ensuring safety has always been the basis of humanisation and, as Stanisław Jarmoszko writes, "it constituted *conditio sine qua non* not only for the survival of the human species, but also for the development of other planes of human culture."[4] The author defines it as follows: a collection of tangible and intangible elements (and thus capable of being considered in mental, rational and physical dimensions) developed to enhance or restore the security of various entities. A recognised researcher of safety culture in Poland is Professor Marian Cieślarczyk,[5] who pointed out that security is closely related to defence with the latter also having a non-military character. The researcher calls it the potential to counter, prevent and resist danger (threat). Cieślarczyk's definition of safety culture is: a set of basic principles, a canon adopted by a given entity, which influences its perception of opportunities and threats coming from the environment. Safety culture is also a specific feeling, thinking, behaviour and (worked out and learned) action serving the development and achievement of objectives in the broadly understood security useful

[2] A. Giszterowicz, "Kapitał jako zdolność do wykonywania pracy i antecedensy teorii", *Przegląd Nauk Stosowanych*, no. 23(2), 2019, pp. 23–35.

[3] This framing already suggests that safety culture is an abstract category and can be considered in relation to the theory of capital developed in accounting, for which the principle of dualism is central.

[4] S. Jarmoszko, Nowe wzory kultury bezpieczeństwa a procesy deterioracji więzi społecznej, [in:] *Jedność i różnorodność: kultura vs. kultury*, eds. E. Rekłajtis, R. Wiśniewski, J. Zdanowski, Warszawa, Oficyna Wydawnicza Aspra-JR, 2010, p. 110.

[5] J. Piwowarski, "Słowo wstępne", *Kultura Bezpieczeństwa. Nauka – Praktyka – Refleksje*, no. 9, 2012, p. 4.

for the implementing entity as well as the environment.[6] The author also defines it as a body of knowledge and skills, as well as a certain technology of the intellect, which functions within the system (entity, organisation) and which makes it possible to feel security and react to its absence.[7] In summary: safety culture is the result of subjective characteristics, attitudes, perceptions, competences and behavioural patterns.[8] According to Cieślarczyk, safety culture has three pillars. These are: knowledge together with a certain idea, value and spirituality of man; the social impact of organisations and legal systems; and the material aspects of human existence. The presented approaches to safety culture and, above all, its key terms such as: tangible, intangible, knowledge and potential, create the possibility to consider this category in the context of accounting theory, scientific theory of capital and, finally, intellectual capital.

As is well known, intellectual capital is not uniformly defined. "A terminological jungle" – as Lesław Niemczyk writes[9] – has arisen as a result of the "rash" of definitions, classifications and concepts of management and memento of intellectual capital. Nevertheless, there is an unambiguous definition of intellectual capital in accounting theory. This definition states that since capital is the abstract ability to do work, human capital the ability of a person (employee) to do work, intellectual capital is his/her ability (potential) for intellectual performance. Both the scientific formulation of this category and the definitions coined successively by various intellectual capital researchers (Thomas A. Stewart, Leif Edvinsson and Michael S. Malone, Karl M. Wigg, Steven M.H. Wallman or Karl-Erik Sveiby) provide an assumpt to define intellectual capital as an abstract category linked to organisational culture that brings tangible benefits, i.e. a potential that can be transformed into something of real higher value. However, this – seemingly overly general and therefore also problematic – definition offers many possibilities for exploration. Indeed, the elements that make up intellectual capital can be configured freely – i.e. depending on the utility function defined by management. For Safety First, this would be safety culture. The typologies of intellectual capital presented in the literature (e.g. typology by Bogusz Mikuła and Anna Pietruszka-Ortyl[10]) can be, as Niemczyk[11] "explored in all possible directions."

---

6 M. Cieślarczyk, *Teoretyczne i metodologiczne podstawy badania problemów bezpieczeństwa i obronności państwa*, Siedlce: Wydawnictwo Akademii Podlaskiej, 2009, p. 157.

7 M. Cieślarczyk, K. Kachniarz, "Kultura bezpieczeństwa w lotnictwie w sytuacjach kryzysowych", *Zeszyty Naukowe – Wyższa Szkoła Oficerska Sił Powietrznych*, no. 2, 2012, p. 27.

8 J. Fieducik, "Kultura bezpieczeństwa w życiu człowieka", *Kultura bezpieczeństwa. Nauka – Praktyka – Refleksje,* no. 18, 2015, p. 44.

9 L. Niemczyk, *Kapitał intelektualny w księgach rachunkowych oraz sprawozdawczości przedsiębiorstwa*, Rzeszów: Wydawnictwo Uniwersytetu Rzeszowskiego, 2015, p. 27.

10 B. Mikuła, A. Pietruszka-Ortyl, "Studium niematerialnych zasobów organizacji", *Zeszyty Naukowe Uniwersytetu Ekonomicznego w Krakowie*, no. 820, 2010, p. 27.

11 L. Niemczyk, *op. cit.*, p. 27.

An approach in which safety culture is treated as one of the elements-components of intellectual capital, or even its only or most important form, is therefore justified. This may be precisely the situation in Safety First organisations. The flagship example of such an organisation is DuPont – where "Safety, Caring and Concern for People, Environmental Protection and Worker and Company Integration are the greatest values and there is no compromise in this regard (...)."[12] Other organisations belonging to this group are: 3M, Guide, uvex, Honeywell, SafetyFirst, Delta Plus, Sundström. It is from their point of view that the operationalisation of the (broadly defined) safety culture will be of the greatest importance.

The problem of operationalisation is synthesised by Czesław Mesjasz. The author's research shows that operationalisation is the process of defining an object that cannot be unambiguously described (measured), although its existence is indicated by other phenomena. They are, therefore, activities that lead to the measurability of the characteristics of an object. This is why they have become the focus of management science. This is because operationalisation extends the possibilities of empirical research (it makes it possible to measure even such concepts as anger, job satisfaction or efficiency).[13] It makes it possible to make theoretical sense of, occurring in business reality, constructs. These constructs can be both qualitative and quantitative in nature and will be related *ex definition* to the functioning, management and governance of the organisation.[14] Operationalisation as an idea is also sometimes criticised. This is because it generates the possibility of over-legitimising "metaphysical" concepts.[15] However, its key functions cannot be questioned. This is because, in relation to safety culture, it is the identification and valuation, and thus the provision (or striving to provide) access to data that is stable, cyclical, quantified, expressed in monetary terms and, above all, clarifying the information flowing from the accounting system and financial reports. One of the tools that makes this possible is the generalised ROAH, developed on the basis of accounting theory and presented in many literature items.[16] which represents the relationship between added value and the human and physical capital operating in the entity.

---

[12] M. Milczarek, "Kultura bezpieczeństwa w przedsiębiorstwie – nowe spojrzenie na zagadnienia bezpieczeństwa pracy", *Bezpieczeństwo pracy*, no. 10, 2000, p. 20.

[13] Cz. Mesjasz, "Operacjonalizacja cech kapitału intelektualnego", *Studia Ekonomiczne. Zeszyty Naukowe Uniwersytetu Ekonomicznego w Katowicach*, no. 263, 2016, p. 22.

[14] K. Hryniewicz, *Operacjonalizacja zmiennych psychologicznych*, Metodolog.pl, 18 October 2016, http://nauka.metodolog.pl/operacjonalizacja-zmiennych-psychologicznych-metodolog-pl [accessed: 14 April 2022].

[15] Cz. Mesjasz, *op. cit.*, p. 22.

[16] E.g. D. Dobija, *Pomiar i sprawozdawczość kapitału intelektualnego przedsiębiorstwa*, Warszawa: Wydawnictwo Wyższej Szkoły Przedsiębiorczości i Zarządzania im. Leona Koźmińskiego, 2003.

Operationalisation of the organisation's safety culture

As mentioned, in today's economy there are so-called Safety First organisations for which the main "wealth" and greatest value is safety culture. Examples are DuPont, 3M and the other companies mentioned in part one. The companies described generate their profits, among other things, on the basis of a policy of care, care for people and the environment, health protection, i.e. precisely a broadly defined safety culture. At the same time, they declare that they do not recognise any compromise on this issue. This means, therefore, that safety culture is the feature of intellectual capital that holds the highest rank in an organisation. In other words, the utility function defined by the management points to the baseline safety culture as the characteristic with the highest importance for the organisation's functioning.

A model that can be helpful in identifying and valuing safety culture is that developed from the scientific theory of capital, which is based on viewing capital as an abstract category and defining it as the ability to do work.[17] This model represents the relationship between added value and the human and physical capital operating in an entity. It takes the form of:

$$ROAH = \frac{Z_{brutto} + W}{A + H(p)}$$

where:
Z_{brutto} – profit including taxes, depreciation and amortisation, interest;
W – wages and salaries including also insurance premiums and other benefits;
A – value of company assets;
H – value of human capital of people employed in the company.

The human capital of the people employed by the company, on the other hand, is determined using the formula:

$$H(p) = \frac{L}{p}$$

where:
L – basic salary;
p – economic constant of potential growth equal to 0.08 [1/year].

The verification and evaluation of this tool is carried out by analysing data from the financial statements (obtained from Monitor Sądowy i Gospodarczy [Court and Commercial Gazette] and Ministerstwo Sprawiedliwości [Ministry of Justice])[18] of

[17] A. Giszterowicz, *op. cit.*

[18] The financial statements published in the Monitor Sądowy i Gospodarczy are those covering the period 2003–2016; those published on the Ministerstwo Sprawiedliwości portal (ms.gov.pl) cover the period 2017–2018.

the company Nexus Systems sp. z o.o.[19] It results in comparative statements and charts. The data obtained as a result of the calculation is then evaluated to identify and value safety culture as an economic quantity characterising the intellectual capital of the company.

The calculation table (Table 1) compiles the calculation data[20] necessary to indicate the percentage of ROAH, which allows a company to be diagnosed for the presence of any intellectual capital characteristics. This is done by setting a research-confirmed cut-off value of 8% for this indicator. If the actual ROAH exceeds $p = 0.08$, there is an undisclosed quantity in the company's assets (in the denominator of the indicator), which in the case of Safety First companies can be called the company's safety culture (SC).

Table 1. Safety culture of Nexus Systems sp. z o.o. from 2003 to 2018 identified and valued using the ROAH model

Data extracted from the financial statements	2003	2004	2005	2006
Gross profit Z_{brutto}	**62,391.37**	**421,771.38**	**456,501.77**	**635,809.51**
Net profit	45,546.37	341,455.38	370,272.77	513,567.51
Income tax	16,845.00	80,316.00	86,229.00	122,242.00
Labour costs *W*	**4,831.60**	**109,773.08**	**344,896.43**	**720,193.42**
Salaries	4,000.00	85,446.45	287,765.91	606,457.43
Additional remuneration components	831.60	24,326.63	57,130.52	113,735.99
Value of company assets *A*	**340,999.48**	**1,012,000.08**	**1,856,610.46**	**2,746,504.51**
Non-current assets	58,000.00	50,438.96	91,410.71	164,409.91
Current assets	282,999.48	961,561.12	1,765,199.75	2,582,094.60
Human capital of the people employed by the company *H*	**50,000.00**	**1,068,080.63**	**3,597,073.88**	**7,580,717.88**
Basic salary *L*	4,000.00	85,446.45	287,765.91	606,457.43
Risk premium *p*	0.08	0.08	0.08	0.08
ROAH	**0.1719**	**0.2555**	**0.1469**	**0.1313**
Data extracted from the financial statements	2003	2004	2005	2006
Subsidiary value *V*	67,222.97	531,544.46	801,398.20	1,356,002.93
Gross profit Z_{brutto}	62,391.37	421,771.38	456,501.77	635,809.51
Labour costs *W*	4,831.60	109,773.08	344,896.43	720,193.42

[19] A manufacturing and trading company operating in the IT sector, in the form of a limited liability company belonging to the SME sector, founded in 2003, with approximately 30 employees, considered a spectacular debut of the optical technology industry at the beginning of the third millennium.

[20] For what appears to be a clearer presentation of the calculation process and to make it easier, an auxiliary value *V* was introduced, which is the sum of the gross profit value (Z_{brutto}) and the labour costs (*W*).

Value of company assets *A*	340,999.48	1,012,000.08	1,856,610.46	2,746,504.51
Human capital of persons employed by the company *H*	50,000.00	1,068,080.63	3,597,073.88	7,580,717.88
Safety culture SC	**449,287.65**	**4,564,225.05**	**4,563,793.17**	**6,622,814.24**
Data extracted from the financial statements	2007	2008	2009	2010
Gross profit Z_{brutto}	**1,158,606.72**	**1,236,103.72**	**-4,010.67**	**34,252.73**
Net profit	932,956.72	996,256.72	-12,056.67	19,054.73
Income tax	225,650.00	239,847.00	8,046.00	15,198.00
Labour costs *W*	**1,070,485.46**	**1,395,181.54**	**1,623,545.43**	**1,731,740.62**
Salaries	893,702.51	1,192,249.39	1,382,184.00	1,469,406.09
Additional remuneration components	176,782.95	202,932.15	241,361.43	262,334.53
Value of company assets *A*	**2,870,569.62**	**3,556,716.90**	**3,502,798.30**	**3,469,901.42**
Non-current assets	195,284.63	196,197.55	144,863.89	110,168.79
Current assets	2,675,284.99	3,360,519.35	3,357,934.41	3,359,732.63
Human capital of the people employed by the company *H*	**11,171,281.38**	**14,903,117.38**	**17,277,300.00**	**18,367,576.13**
Basic salary *L*	893,702.51	1,192,249.39	1,382,184.00	1,469,406.09
Risk premium *p*	0.08	0.08	0.08	0.08
ROAH	**0.1587**	**0.1425**	**0.0779**	**0.0809**
Data extracted from the financial statements	2007	2008	2009	2010
Subsidiary value *V*	2,229,092.18	2,631,285.26	1,619,534.76	1,765,993.35
Gross profit Z_{brutto}	1,158,606.72	1,236,103.72	-4,010.67	34,252.73
Labour costs *W*	1,070,485.46	1,395,181.54	1,623,545.43	1,731,740.62
Value of company assets *A*	2,870,569.62	3,556,716.90	3,502,798.30	3,469,901.42
Human capital of persons employed by the company *H*	11,171,281.38	14,903,117.38	17,277,300.00	18,367,576.13
Safety culture SC	**13,821,801.26**	**14,431,231.48**	**-535,913.80**	**237,439.33**
Data extracted from the financial statements	2011	2012	2013	2014
Gross profit Z_{brutto}	**380,326.32**	**158,858.00**	**125,447.91**	**131,128.71**
Net profit	310,786.32	125,584.00	91,868.91	94,930.71
Income tax	69,540.00	33,274.00	33,579.00	36,198.00
Labour costs *W*	**1,957,197.99**	**2,130,253.06**	**2,163,739.92**	1,683,022.54
Salaries	1,665,597.10	1,788,923.16	1,801,132.72	1,683,022.54
Additional remuneration components	291,600.89	341,329.90	362,607.20	326,010.91
Value of company assets *A*	**3,856,207.01**	**4,089,958.90**	**635,301.04**	**4,269,443.89**
Non-current assets	182,808.72	259,867.99	237,396.78	208,181.74
Current assets	3,673,398.29	3,830,090.91	397,904.26	4,061,262.15
Human capital of the people employed by the company *H*	**20,819,963.75**	**22,361,539.50**	**22,514,159.00**	**21,037,781.75**
Basic salary *L*	1,665,597.10	1,788,923.16	1,801,132.72	1,683,022.54
Risk premium *p*	0.08	0.08	0.08	0.08

ROAH	**0.0947**	**0.0865**	**0.0989**	**0.0717**
Data extracted from the financial statements	2011	2012	2013	2014
Subsidiary value *V*	2,337,524.31	2,289,111.06	2,289,187.83	1,814,151.25
Gross profit Z_{brutto}	380,326.32	158,858.00	125,447.91	131,128.71
Labour costs *W*	1,957,197.99	2,130,253.06	2,163,739.92	1,683,022.54
Value of company assets *A*	3,856,207.01	4,089,958.90	635,301.04	4,269,443.89
Human capital of the people employed by the company *H*	20,819,963.75	22,361,539.50	22,514,159.00	21,037,781.75
Safety culture SC	**4,542,883.12**	**2,162,389.85**	**5,465,387.84**	**-2,630,335.02**
Data extracted from the financial statements	2015	2016	2017	2018
Gross profit Z_{brutto}	379,690.59	31,940.21	58,878.06	444,135.97
Net profit	298,360.59	23,362.21	45,883.06	356,727.97
Income tax	81,330.00	8,578.00	12,995.00	87,408.00
Labour costs *W*	2,213,674.20	2,133,142.82	1,935,612.27	1,975,820.66
Salaries	1,854,101.66	1,787,470.29	1,627,564.05	1,655,419.84
Additional remuneration components	359,572.54	345,672.53	308,048.22	320,400.82
Value of company assets *A*	4,771,699.43	5,535,702.82	5,308,016.12	5,453,024.04
Non-current assets	344,796.61	1,225,262.64	1,204,425.12	1,214,360.67
Current assets	4,426,902.82	4,310,440.18	4,103,591.00	4,238,663.37
Human capital of the people employed by the company *H*	23,176,270.75	22,343,378.63	20,344,550.63	20,692,748.00
Basic salary *L*	1,854,101.66	1,787,470.29	1,627,564.05	1,655,419.84
Risk premium *p*	0.08	0.08	0.08	0.08
ROAH	**0.0928**	**0.0777**	**0.0778**	**0.0926**
Data extracted from the financial statements	2015	2016	2017	2018
Subsidiary value *V*	2,593,364.79	2,165,083.03	1,994,490.33	2,419,956.63
Gross profit Z_{brutto}	379,690.59	31,940.21	58,878.06	444,135.97
Labour costs *W*	2,213,674.20	2,133,142.82	1,935,612.27	1,975,820.66
Value of company assets *A*	4,771,699.43	5,535,702.82	5,308,016.12	5,453,024.04
Human capital of persons employed by the company *H*	23,176,270.75	22,343,378.63	20,344,550.63	20,692,748.00
Safety culture SC	**4,469,089.69**	**-815,543.57**	**-721,437.62**	**4,103,685.84**

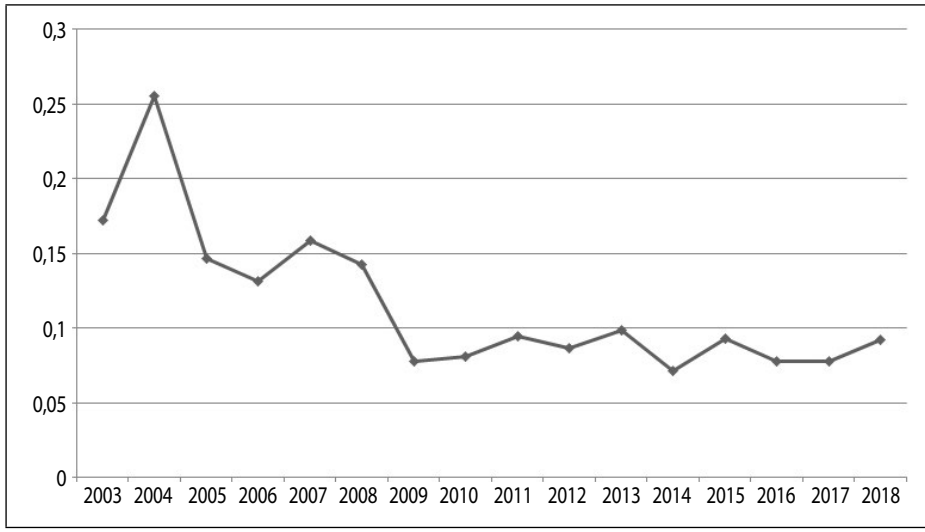
Source: own study.

In the case of the company Nexus Systems sp. z o.o., the value of the ROAH indicator for individual periods of activity (2003–2018) is illustrated by the chart 1. It turns out that the initial phase of the company's activity (2003–2008), i.e. the phase of the most dynamic development (confirmed by the management[21]) is

[21] This information is available on the company's internet site: Nexus System, O firmie, https://swiatlowody.com.pl/o-firmie.html [accessed: 14 April 2022].

characterised by high values of the ROAH indicator, as the lowest value from this period is about 13%, and the highest 25%. From 2009 onwards (the moment of gaining market stability and stabilising the size of employment), these values are at the level of 7–10%.

Figure 1. Rate of return on tangible and human assets (ROAH) at Nexus Systems sp. z o.o. from 2003 to 2018 taking into account the safety culture

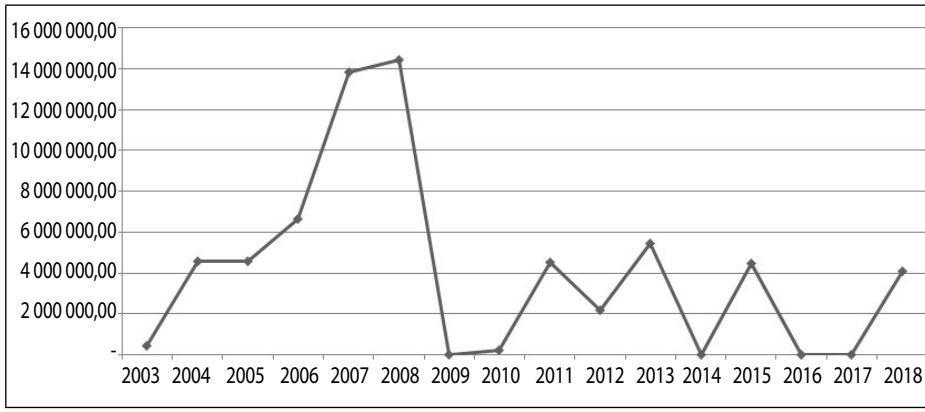


Source: own study.

The percentage values of ROAH (Figure 1) and the values of the intellectual capital characteristics (Figure 2), expressed in PLN, characteristic of the described company in each period of its activity, testify to the existence of high management efficiency and employee effectiveness, as well as to the company's ability to defend itself against business risks. This, in turn, could be attributed to a safety culture if management identified it as the most important characteristic in the process of defining the utility function. Importantly, the disclosed value of safety culture can be presented in the asset balance sheet.[22] This balance sheet can include both the information contained in the "actual" financial statements (2003–2018) of Nexus Systems sp. z o.o. and the results of the calculations carried out using ROAH and the safety culture measurement model constructed on its basis, and therefore takes into account not only information about the company's tangible components and assets, but also information about important and hitherto elusive economic categories.

[22] This refers to the so-called knowledge-based balance sheet according to the concept of L. Niemczyk, *op. cit.*, pp. 78–79.

Figure 2. Value (PLN) of intellectual capital attributes* of Nexus Systems sp. z o.o. between 2003 and 2018



* this article assumes that safety culture is a feature of intellectual capital.

Source: own study.

Conclusions

The aim of the article was to look at safety culture as an object of economic calculation (broadening the perception of the category of intellectual capital) and to answer the question: can safety culture be operationalised? And additionally: can safety culture be a measurable category using a specific profitability indicator?

Through theoretical and cognitive considerations, it has been determined that the category of safety culture can be operationalised and an adequate instrumentarium has been proposed for this purpose. The starting point, however, is to take into account the knowledge that capital – according to scientific theory – is the ability to do work and should be considered in the light of the basic identity of dual accounting. It differentiates tangible assets from capital – the abstract medium within them. Without an understanding of the ubiquitous principle of duality and an awareness that all natural processes are subject to it, it is not possible to properly define and study the phenomena occurring in the economy. These phenomena include, among others, the existence of intellectual capital and its abstract qualities and, therefore, the broadly defined safety culture within a company and its employees.

Despite the fact that the case study does not allow for the generalisation of conclusions, from the point of view of business management, the information obtained appears to be cognitively valuable, and as an added value (created as a result of theoretical and empirical research) should undoubtedly be indicated: the resolution of the issue of the measurability of abstract categories, to which safety culture can be

included, and the introduction, verification and evaluation of a tool capable of realising this objective grounded – as indicated – in accounting theory.

References

Chodyński A., *Dynamika przedsiębiorczości i zarządzania innowacjami w firmach. Odpowiedzialność – prospołeczność – ekologia – bezpieczeństwo*, Kraków: Oficyna Wydawnicza KAAFM, 2021.

Cieślarczyk M., *Teoretyczne i metodologiczne podstawy badania problemów bezpieczeństwa i obronności państwa*, Siedlce: Wydawnictwo Akademii Podlaskiej, 2009.

Cieślarczyk M., Kachniarz K., "Kultura bezpieczeństwa w lotnictwie w sytuacjach kryzysowych", *Zeszyty Naukowe – Wyższa Szkoła Oficerska Sił Powietrznych*, no. 2, 2012, pp. 23–32.

Dobija D., *Pomiar i sprawozdawczość kapitału intelektualnego przedsiębiorstwa*, Warszawa: Wydawnictwo Wyższej Szkoły Przedsiębiorczości i Zarządzania im. Leona Koźmińskiego, 2003.

Fieducik J., "Kultura bezpieczeństwa w życiu człowieka", *Kultura bezpieczeństwa. Nauka – Praktyka – Refleksje*, no. 18, 2015, pp. 39–51.

Giszterowicz A., "Kapitał jako zdolność do wykonywania pracy i antecedensy teorii", *Przegląd Nauk Stosowanych*, no. 23(2), 2019, pp. 23–35.

Hryniewicz K., *Operacjonalizacja zmiennych psychologicznych*, Metodolog.pl, 18 October 2016, http://nauka.metodolog.pl/operacjonalizacja-zmiennych-psychologicznych-metodolog-pl [accessed: 14 April 2022].

Jarmoszko S., Nowe wzory kultury bezpieczeństwa a procesy deterioracji więzi społecznej,[in:] *Jedność i różnorodność: kultura vs. kultury*, eds. E. Rekłajtis, R. Wiśniewski, J. Zdanowski, Warszawa: Oficyna Wydawnicza Aspra-JR, 2010, pp. 101–114.

Mesjasz Cz., "Operacjonalizacja cech kapitału intelektualnego", *Studia Ekonomiczne. Zeszyty Naukowe Uniwersytetu Ekonomicznego w Katowicach*, no. 263, 2016, pp. 19–35.

Mikuła B., Pietruszka-Ortyl A., "Studium niematerialnych zasobów organizacji", *Zeszyty Naukowe Uniwersytetu Ekonomicznego w Krakowie*, no. 820, 2010, pp. 31–46.

Milczarek M., "Kultura bezpieczeństwa w przedsiębiorstwie – nowe spojrzenie na zagadnienia bezpieczeństwa pracy", *Bezpieczeństwo Pracy*, no. 10, 2000, pp. 17–20.

Niemczyk L., *Kapitał intelektualny w księgach rachunkowych oraz sprawozdawczości przedsiębiorstwa*, Rzeszów: Wydawnictwo Uniwersytetu Rzeszowskiego, 2015.

Piwowarski J., "Słowo wstępne", *Kultura Bezpieczeństwa. Nauka – Praktyka – Refleksje*, no. 9, 2012, pp. 3–8.

Operationalising a safety culture in the management of a business entity (case study)

Abstract

Safety culture – along with quality and environmental culture – determines a positive image, competitive advantage and financial benefits. As a result, interest in this category continues to grow (CE or B certification). Safety culture can be considered from the point of view of philosophy, sociology, anthropology, economics and management as evidenced by Andrzej Chodyński's rich compilation of terms, definitions and points of reference. The aim of the article is to look at safety culture as an object of economic accounting,

thus treating safety culture as an economic category and answering the questions: can safety culture be an object of operationalisation based on the principle of dualism dominant in accounting and, therefore, can safety culture be a measurable category using the general profitability index? These issues are particularly important from the perspective of Safety First companies. The answers to the research problems posed are provided by a literature analysis, an analysis of financial documents and a case study. For the identification and valuation of safety culture, the generalised ROAH was used. The article thus resolves the measurability of safety culture and introduces, verifies and evaluates a tool grounded in accounting theory.

Key words: safety culture, intellectual capital, operationalisation, accounting, ROAH

BEZPIECZEŃSTWO TEORIA I PRAKTYKA SECURITY THEORY AND PRACTICE
e-ISSN 2451-0718
ISSN 1899-6264
2022
No. 2 (XLVII)
DOI: 10.48269/2451-0718-btip-2022-2-007
Received: 23.04.2022
Accepted: 21.07.2022

Michał Adam Leśniewski
PhD, Andrzej Frycz Modrzewski Krakow University
https://orcid.org/0000-0003-2411-8911

The manager and the safety culture of the organisation: a conceptual model

Introduction

The issue of safety is a fundamental insight into the future of any organisation.[1] It can be argued that a secure organisation functions and develops better than an organisation without safety. Every day people strive to maintain safety.[2] Organisational safety can be defined as a process, a state that relatively guarantees a sense of certainty for the permanent functioning of an organisation in a changing environment. By analysing the environment, we are able to identify/indicate factors that can stabilise or destabilise organisational safety. Paying attention to the issue of organisational safety reinforces the field of practice and theory of management and quality sciences. Safety as a component of an organisation cannot exist without the participation of a human being (employee).[3] The person responsible, from the point of view of the implementation of the management process, for shaping the safety of the organisation is the manager embedded in the realities of

1 *Bezpieczeństwo: wymiar współczesny i perspektywy badań*, ed. M. Kwieciński, Kraków: Krakowskie Towarzystwo Edukacyjne. Oficyna Wydawnicza AFM, 2010.

2 A. Chodyński, "Sieciowość w zarządzaniu bezpieczeństwem na poziomie regionalnym i lokalnym", *Bezpieczeństwo. Teoria i Praktyka*, no. 1, 2014, pp. 13–27.

3 M. Silic, P.B. Lowry, "Using design-science based gamification to improve organizational security training and compliance", *Journal of Management Information Systems*, vol. 37, issue 1, 2020, pp. 129–161, https://doi.org/10.1080/07421222.2019.1705512.

the given organisational culture. This positioning of the manager in the safety reality of the organisation constitutes the shaping of the manager's safety culture.

The purpose of the study is to present the author's conceptual model of an organisation's safety culture manager. The paper is the result of a study of the literature on the subject together with the author's interpretation.

Manager in organisation management

The manager creates the future of the organisation in carrying out the management process and the organisation, owing to the functioning of the manager, will be able to stay in the market and gain a competitive advantage. It is the person responsible for the present and future of the organisation (enterprise). The term "manager" is used to refer to a director, manager, supervisor or superior, including a master or foreman.[4]

A manager is defined as a planner, organiser, leader, controller of an organisation. He/she is a politician representing the team, a coach motivating and helping the team to spread its wings, a strategist and an administrator enabling the team to work.[5] Every manager is characterised by multi-characteristics as a set of qualities that enable him or her to be a manager.

Skills have to be modified according to the circumstances, the situation in which the managers or the organisation find themselves. Taking the view that a manager is a multifaceted person who interacts with others, it is correct to say that an effective manager is a person who modifies his or her skills. A manager's skills cannot lack safety skills.[6] The operation of an organisation in a changing environment means that the profile of the manager's physique is constantly being changed, refined and modified so that the manager is fully adapted to the organisation and the organisation to the environment.[7]

The functioning of managers in an organisation contributes to the formation of the organisational culture.[8] A changing environment creates conditions for the

---

4 U. Ornatowicz, *Menedżer XXI wieku. Definicja, identyfikacja, edukacja*, Warszawa: Oficyna Wydawnicza Szkoły Głównej Handlowej, 2008, s. 18.

5 *Kierownik* [headword], Encyklopedia Zarządzania, https://mfiles.pl/pl/index.php/Kierownik [accessed: 1 April 2022].

6 Safety skills are the manager's learned abilities to provide a sense of assurance and a relative reduction in the level of threat in the organisation.

7 A. Gurba, J. Kowal, Z. Knecht, "Menedżer w procesie zarządzania zmianą we współczesnym przedsiębiorstwie", *Gospodarka, Rynek, Edukacja*, vol. 17, no. 2, 2016, p. 14.

8 M. Choi, "Leadership of information security manager on the effectiveness of information systems security for secure sustainable computing", *Sustainability*, vol. 8(7), 638, 2016, https://doi.org/10.3390/su8070638.

interest of the organisation's managers in the issue of safety.[9] The concept of safety is fully shaped by organisational culture. Safety culture (subculture) is a component of organisational culture (leading culture).

Organisational culture vs. safety culture of the organisation

The changes that are taking place in the external environment mean that organisations are constantly looking for new ways to achieve competitive advantage in the market.[10] Increasingly, competitive advantage is being determined by the originality of the company, its employees and the way in which potential customers perceive the economic entity. It is important to perceive the differences and similarities between the economic entity under analysis and the companies in its external environment. Answering the questions: who are we? how do we act? what motivates us?, becomes one of the fundamental elements of the competitive game. With this approach, the tool that makes it possible to concretise strategy is organisational culture, which is strongly linked to the company's areas of development. When employees have a sense of connection between the company's activities and their own values, their motivation and point of view about the rightness of the work they do increases to a great extent.[11]

Business practitioners regard changes in organisational culture as a unique social entity, an element, a resource that develops the organisation.[12] Executives quite often do not take the decision to modify the organisational culture in the organisation, but draw from it patterns, symbols, values or ways of communication. The external environment is dynamic in nature, changes in the organisation and the associated modification of the organisational culture are processes that are not easy, but realistic to implement.[13] The modification of organisational culture should occur from the needs of the exogenous and endogenous environment. With the

---

[9] D. Fatuła, "Elementy kultury bezpieczeństwa a zachowania klientów instytucji finansowych", *Bezpieczeństwo. Teoria i Praktyka*, no. 4, 2018, pp. 17–34.

[10] A. Jabłoński, M. Jabłoński, "Zarządzanie bezpieczeństwem w transporcie kolejowym – kluczowe aspekty", *Bezpieczeństwo. Teoria i Praktyka*, no. 3, 2014, pp. 57–68.

[11] P. Gajewska, M. Kubański, Wpływ kultury organizacyjnej na efektywność przedsiębiorstwa, [in:] *Etyka, kultura organizacyjna i społeczna odpowiedzialność biznesu w kształtowaniu potrzeb i relacji z klientami*, eds. H. Howaniec, Z. Malara, W. Waszkielewicz, Bielsko-Biała: Wydawnictwo Naukowe Akademii Techniczno-Humanistycznej, 2014, pp. 78–79.

[12] J. Stachowicz, J. Michulik, "Dylematy procesu koniecznych zmian kultury organizacyjnej przedsiębiorstw przemysłowych. Przypadek transformacji przedsiębiorstw przemysłów tradycyjnych", *Zarządzanie Zasobami Ludzkimi*, vol. 6, 2008, pp. 59–69.

[13] J. Szubielska, Kultura organizacyjna i kultura bezpieczeństwa, [in:] *Kultura bezpieczeństwa w przedsiębiorstwie. Modele, diagnoza i kształtowanie*, ed. A. Rakowska, Warszawa: CeDeWu, 2013, pp. 9–46.

modification of the organisational culture the culture of safety is modified,[14] which should provide a relatively possible sense of certainty, a guarantee for the organisation in question.

The discussion in the world of practice and academia about the importance of safety culture as a variable of management processes began with the Chernobyl disaster in Ukraine. In 1986, the International Atomic Energy Agency published the Chernobyl Accident Summary Report, which used the term "safety culture" for the first time to illustrate how the thinking and behaviour of safety personnel caused the disaster.[15] The origins of safety culture in practical and scientific considerations are characteristic of management and quality sciences (e.g. safety management or crisis management), where the bulk of problems originate in business practice. The exploration of safety culture issues needed to be located in the research conducted, with a particular focus on organisational culture.[16] Relating the exploration of safety culture to research into organisational culture was facilitated by the research programmes conducted, i.e.: it made it possible to define the relationship between organisational culture and safety culture. It has made it possible to define the essence of safety culture more comparably to organisational culture which has made it possible to use concepts, models and tools to represent safety culture.[17]

Safety culture can be verified in its three basic dimensions, i.e.:[18]

1) the mental dimension: norms, values, ideas, etc.,
2) the social and rational dimensions: socio-cultural interactions, law-organisations or innovation-entrepreneurship, etc.,
3) the material dimension: the material features of human existence and functioning.

A sustainable safety culture[19] needs a holistic approach to the trichotomy of its dimensions. The tendency towards the predominance of detailed, specialised approaches that suppress or fail to take into account the return to synthesis or

---

[14] M.A. Leśniewski, "Decyzyjność i decyzja a bezpieczeństwo pracy menedżera w organizacji – studium teoretyczne problemu badawczego", *Bezpieczeństwo. Teoria i Praktyka*, vol. 4, 2021, pp. 155–168, https://doi.org/10.48269/2451-0718-btip-2021-4-009.

[15] Y. Kim, J. Park, M. Park, "Creating a Culture of Prevention in Occupational Safety and Health Practice", *Safety and Health at Work*, vol. 7, 2016, pp. 89–96, https://doi.org/10.1016/j.shaw.2016.02.002.

[16] K.S. Cole, S.M. Stevens-Adams, C.A. Wenner, *A Literature Review of Safety Culture*, Sandia National Laboratories, Albuquerque, NM – Livermore, CA, 2013, pp. 3–47.

[17] P. Jedynak, "Od kultury bezpieczeństwa do kultury prewencji – terminologia i relacje znaczeniowe", *Przedsiębiorczość i Zarządzanie*, vol. 19, no. 11, part 1, 2018, pp. 9–17.

[18] A. Kłoskowska, *Socjologia kultury*, preface Z. Bokszański, 3rd edition, Warszawa: Wydawnictwo Naukowe PWN, 2007, p. 103; A. Kroeber, *Istota kultury*, transl. P. Sztompka, 3rd edition, Warszawa: Wydawnictwo Naukowe PWN, 2002, p. 195.

[19] J. Czaja, *Kulturowe czynniki bezpieczeństwa*, Kraków: Krakowskie Towarzystwo Edukacyjne – Oficyna Wydawnicza AFM, 2008.

comparative capture of exploratory results can result in a lack of knowledge of safety culture and a decline in its level.[20]

In the situation of organisational culture and safety culture, the supervisor is the safety culture manager, who should base the organisation on models of organisational culture formation with features, safety elements appropriate to the situation.

The organisation's safety culture manager: a conceptual model

The manager in the process of building a safety culture is a key figure. His or her responsibilities are comprehensive and largely dependent on the size of the company.[21] Each manager is responsible for achieving the company's objectives, maintaining the values, norms and principles of the organisation's safety culture. His or her assurance of proper working conditions, their reporting and analysis affect the organisational capacity of all units in the enterprise.

A safety culture manager is a person who implements and is responsible for the management process towards the formation of such an organisational culture that will create conditions in which the organisation, despite the external threat,[22] will achieve its objectives.

The safety culture manager takes full responsibility for the working conditions in the company, by constantly checking the workstations of production workers, ensuring that machines are in working order and that the tools needed to make the product are safely accessible.[23] He/she is responsible for the mistakes of workers related to non-compliance with these rules, while at the same time he/she is obliged to rectify any irregularities arising from non-compliance with H&S rules. The most important aspect of the safety culture manager is his or her knowledge, skills or attitudes and beliefs in the area of safety. Among the prerequisites for an effective safety culture are his or her commitment to knowledge transfer regarding safety rules and open communication.[24] Open and honest communication is based on

---

[20] M. Cieślarczyk, Fenomen bezpieczeństwa i zjawisko kryzysów postrzegane w perspektywie kulturowej, [in:] *Jedność i różnorodność: kultura vs. kultury*, eds. E. Rekłajtis, R. Wiśniewski, J. Zdanowski, Warszawa: Oficyna Wydawnicza Aspra-JR, 2010, p. 96.

[21] A.B. Ruighaver, S.B. Maynard, S. Chang, "Organisational security culture: Extending the end-user perspective", *Computers & Security*, vol. 26, issue 1, 2007, pp. 56–62, https://doi.org/10.1016/j.cose.2006.10.008.

[22] An external threat is any action of the external environment closer or further away that has a destructive, detrimental effect on the functioning of an organisation. Examples of external threats are: socio-economic crises, states of war, war or other situations that destabilise organisations.

[23] S.R. Kessler, S. Pindek, G. Kleinman, S.A. Andel, P.E. Spector, "Information security climate and the assessment of information security risk among healthcare employees", *Health Informatics Journal*, vol. 26(1), 2020, pp. 461–473, https://doi.org/10.1177/1460458219832048.

[24] M. Milczarek, *Kultura bezpieczeństwa pracy*, Warszawa: CIOP, 2002.

communicating with others in the organisation, persuading, teaching, listening, talking, reaching a compromise or consensus. Communication applies to all employees, at all levels of the organisational structure. In terms of occupational health and safety, it should include honest and systematic communication about the risks involved, technical protection measures, as well as desirable behaviour to minimise the risks involved.[25]

A safety culture manager, in order to be able to effectively protect an organisation from external threats, should have a safety culture model developed and implemented in the organisation. The creation of such a model should involve all managers (regardless of management level) and subordinates, i.e. the whole community of the organisation. Figure 1 presents a conceptual model of the organisation's safety culture manager.

Figure 1. The organisation's safety culture manager: conceptual model[26]

Source: own elaboration based on: R. Tyszkiewicz, "Istota kultury bezpieczeństwa pracy w systemie zarządzania", *Quality Production Improvement*, no. 2, 2019, pp. 94–101; P. Jedynak, "Od kultury bezpieczeństwa do kultury prewencji – terminologia i relacje znaczeniowe", *Przedsiębiorczość i Zarządzanie*, vol. 19, no. 11, part 1, 2018, p. 13.

Shaping an organisation's safety culture manager model is not an easy task, but it is very important for the future of the organisation. Every aspect of an organisation's

[25] *Kształtowanie kultury bezpieczeństwa i higieny pracy w organizacji*, ed. J. Ejdys, Białystok: Oficyna Wydawnicza Politechniki Białostockiej, 2010.

[26] The factors presented in the model are not quantified, e.g. from most important to less important or which factor is first and which is last, and do not have weights, but are based on a qualitative, out-of-the-box and non-hierarchical occurrence in the reality of a given organisation.

functioning should take safety into account. The order of the factors for shaping the safety culture manager in the model presented is not important, but the application of these factors is.

The starting point in the model presented is the organisational culture, which should be conducive to organisational safety. Each organisation should develop its own concept of safety. Another element of the model is the safety behaviourality of employees, which manifests itself in safety-enhancing behaviour. Safety behaviourality is supposed to be a certain habit in employees moving towards security. The work environment refers to the interior of the organisation and the prevailing atmosphere (organisational climate) in the workplace. The work environment is also influenced by the external environment, which is a source of safety risks for the organisation.[27] Among other things, the work environment is linked to the organisational structure, which should be modified under the influence of increasing the organisation's safety capacity. Human interaction is another factor in the model presented, which relates to the relationships existing at work between employees. The external environment of an organisation is a situation resulting from changes in this environment and having a direct impact on the organisation. One of the changes in the external environment is, for example, the war in Ukraine (migration of the Ukrainian population to Poland), which translates directly into changes in the functioning of the organisation. Trust between managers and subordinates is another factor of the model. A safety model based on trust will provide a strong foundation for the development of organisational safety. Adherence to safety is any kind of guideline that enables safety, e.g. H&S, occupational hygiene or firefighting regulations. Employee safety conformism and non-conformism are two opposites. Safety conformism is the adaptation (subordination) of the employee to the norms, values related to the safety model created or developed by the organisation. Safety non-conformist is the non-adaptation or non-subordination of the employee to the norms, values associated with the safety model created or developed by the organisation. The quality of organisational safety is the relatively satisfactory utility value of the systemic sense of safety and the guarantee of its preservation in the long term. This quality will manifest itself in the organisation whenever a sense of safety is created among employees. Improving safety means making fundamental changes to the way in which solutions are implemented that provide a basis for a relative sense of safety in the organisation. A correlating factor with the improvement of safety is the competence and responsibility of the manager creating support for measures to improve the organisation's safety against the adverse effects of the external environment.

[27] An example of this is the war in Ukraine (date of war: 24.02.2022), which could contribute to a war with NATO, which could consequently lay the foundations for World War III.

Conclusions

The issue of safety is not only related to the military sphere (e.g. army, police, border guards or municipal guards) aimed at internal or external order, but also to the sphere of operation of any organisation in the state, e.g. businesses. The issue of safety concerns every state and every organisation. It can be said that safety is an interdisciplinary, multidimensional and multi-organisational concept. The interdisciplinarity of safety is the perception of safety by different scientific disciplines (e.g. management and quality sciences, economics and finance, sociology, psychology or political science, etc.).[28] The multidimensionality of safety means that it applies to every area of an organisation (e.g. marketing, finance, logistics, organisational structure, production, the organisation's customer service office or the organisation's resources, etc.). The multi-organisational nature of safety means that it applies to any organisation (e.g. hospitals, universities, local government or commercial organisations, etc.). This framing creates a clear picture that provides an opportunity to understand the fundamentals of organisational safety functioning. A significant role in shaping safety is played by managers from the point of view of the organisational management process. Managers and subordinates are the foundation of organisational safety. One of the areas of implementing safety is an organisational culture profiled towards a safety culture headed by a manager. A manager with the safety of the organisation in mind constitutes the existence of a safety culture manager, who can be defined as a person who safeguards the organisation against threats arising from the external environment and is able to implement the management process in such a way that the organisation can face potential threats in the future. The concept of the safety culture manager emphasises the softness of safety, an issue that can be shaped by organisational culture. The norms, values and behaviour of employees related to safety can influence the overall safety of an organisation. It is important to remember that safety is also a perception of the state in which an organisation or an individual employee is.

References

Bezpieczeństwo: wymiar współczesny i perspektywy badań, ed. M. Kwieciński, Kraków: Krakowskie Towarzystwo Edukacyjne. Oficyna Wydawnicza AFM, 2010.

Chodyński A., "Sieciowość w zarządzaniu bezpieczeństwem na poziomie regionalnym i lokalnym", *Bezpieczeństwo. Teoria i Praktyka*, no. 1, 2014, pp. 13–27.

Choi M., "Leadership of information security manager on the effectiveness of information systems security for secure sustainable computing", *Sustainability*, vol. 8(7), 638, 2016, https://doi.org/10.3390/su8070638.

[28] W. Jiao, "Portfolio manager home- country culture and mutual fund risk- taking", *Financial Management*, vol. 49, issue 3, 2020, pp. 805–838, https://doi.org/10.1111/fima.12265.

Cieślarczyk M., Fenomen bezpieczeństwa i zjawisko kryzysów postrzegane w perspektywie kulturowej, [in:] *Jedność i różnorodność: kultura vs. kultury*, eds. E. Rekłajtis, R. Wiśniewski, J. Zdanowski, Warszawa: Oficyna Wydawnicza Aspra-JR, 2010, pp. 83–100.

Cole K.S., Stevens-Adams S.M., Wenner C.A., *A Literature Review of Sefety Culture*, Sandia National Laboratories, Albuquerque, NM – Livermore, CA, 2013.

Czaja J., *Kulturowe czynniki bezpieczeństwa*, Kraków: Krakowskie Towarzystwo Edukacyjne – Oficyna Wydawnicza AFM, 2008.

Fatuła D., "Elementy kultury bezpieczeństwa a zachowania klientów instytucji finansowych", *Bezpieczeństwo. Teoria i Praktyka*, no. 4, 2018, pp. 17–34.

Gajewska P., Kubański M., Wpływ kultury organizacyjnej na efektywność przedsiębiorstwa, [in:] *Etyka, kultura organizacyjna i społeczna odpowiedzialność biznesu w kształtowaniu potrzeb i relacji z klientami*, eds. H. Howaniec, Z. Malara, W. Waszkielewicz, Bielsko-Biała: Wydawnictwo Naukowe Akademii Techniczno-Humanistycznej, 2014, pp. 75–88.

Gurba A., Kowal J., Knecht Z., "Menedżer w procesie zarządzania zmianą we współczesnym przedsiębiorstwie", *Gospodarka, Rynek, Edukacja*, vol. 17, no. 2, 2016, pp. 11–18.

Jabłoński A., Jabłoński M., "Zarządzanie bezpieczeństwem w transporcie kolejowym – kluczowe aspekty", *Bezpieczeństwo. Teoria i Praktyka*, no. 3, 2014, pp. 57–68.

Jedynak P., "Od kultury bezpieczeństwa do kultury prewencji – terminologia i relacje znaczeniowe", *Przedsiębiorczość i Zarządzanie*, vol. 19, no. 11, part 1, 2018, pp. 9–17.

Jiao W., "Portfolio manager home- country culture and mutual fund risk- taking", *Financial Management*, vol. 49, isssue 3, 2020, pp. 805–838, https://doi.org/10.1111/fima.12265.

Kessler S.R., Pindek S., Kleinman G., Andel S.A., Spector P.E., "Information security climate and the assessment of information security risk among healthcare employees", *Health Informatics Journal*, vol. 26(1), 2020, pp. 461–473, https://doi.org/10.1177/1460458219832048.

Kierownik [headword], Encyklopedia Zarządzania, https://mfiles.pl/pl/index.php/Kierownik [accessed: 1 April 2022].

Kim Y., Park J., Park M., "Creating a Culture of Prevention in Occupational Safety and Health Practice", *Safety and Health at Work*, vol. 7, 2016, pp. 89–96, https://doi.org/10.1016/j.shaw.2016.02.002.

Kłoskowska A., *Socjologia kultury*, preface Z. Bokszański, 3rd edition, Warszawa: Wydawnictwo Naukowe PWN, 2007.

Kroeber A.L., *Istota kultury*, transl. P. Sztompka, 3rd edition, Warszawa: Wydawnictwo Naukowe PWN, 2002.

Kształtowanie kultury bezpieczeństwa i higieny pracy w organizacji, ed. J. Ejdys, Białystok: Oficyna Wydawnicza Politechniki Białostockiej, 2010.

Leśniewski M.A., "Decyzyjność i decyzja a bezpieczeństwo pracy menedżera w organizacji – studium teoretyczne problemu badawczego", *Bezpieczeństwo. Teoria i Praktyka*, vol. 4, 2021, pp. 155–168, https://doi.org/10.48269/2451-0718-btip-2021-4-009.

Milczarek M., *Kultura bezpieczeństwa pracy*, Warszawa: CIOP, 2002.

Ornatowicz U., *Menedżer XXI wieku. Definicja, identyfikacja, edukacja*, Warszawa: Oficyna Wydawnicza Szkoły Głównej Handlowej, 2008.

Ruighaver A.B., Maynard S.B., Chang S., "Organisational security culture: Extending the end-user perspective", *Computers & Security*, vol. 26, issue 1, 2007, pp. 56–62, https://doi.org/10.1016/j.cose.2006.10.008.

Silic M., Lowry P.B., "Using design-science based gamification to improve organizational security training and compliance", *Journal of Management Information Systems*, vol. 37, issue 1, 2020, pp. 129–161, https://doi.org/10.1080/07421222.2019.1705512.

Stachowicz J., Michulik J., "Dylematy procesu koniecznych zmian kultury organizacyjnej przedsiębiorstw przemysłowych. Przypadek transformacji przedsiębiorstw przemysłów tradycyjnych", *Zarządzanie Zasobami Ludzkimi*, vol. 6, 2008, pp. 59–69.

Szubielska J., Kultura organizacyjna i kultura bezpieczeństwa, [in:] *Kultura bezpieczeństwa w przedsiębiorstwie. Modele, diagnoza i kształtowanie*, ed. A. Rakowska, Warszawa: CeDeWu, 2013, pp. 9–46.

Tyszkiewicz R., "Istota kultury bezpieczeństwa pracy w systemie zarządzania", *Quality Production Improvement*, no. 2, 2019, pp. 94–101.

Manager and the safety culture of an organisation: a conceptual model

Abstract

Safety is a problem that every organization that wants to shape its competitiveness must be able to face in order to maintain its advantage on the market. From the point of view of the management process, the implementer of the organisation's safety is a manager who – in shaping the organisational culture – must take into account safety factors in the broad sense of the word. Safety culture is a determinant of an organisation operating in the second decade of the 21st century. The aim of the study is to present the proprietary conceptual model of the organisation's safety culture manager. The article was created as a result of a study of the literature on the subject along with the author's interpretation.

Key words: manager, organisational culture, organisational safety culture

BEZPIECZEŃSTWO TEORIA I PRAKTYKA SECURITY THEORY AND PRACTICE
e-ISSN 2451-0718
ISSN 1899-6264
2022
No. 2 (XLVII)
DOI: 10.48269/2451-0718-btip-2022-2-008
Received: 29.04.2022
Accepted: 4.07.2022

Marta du Vall
Associate Professor, Andrzej Frycz Modrzewski Krakow University, Poland
https://orcid.org/0000-0003-1245-730X

Marta Majorek
Associate Professor, Andrzej Frycz Modrzewski Krakow University, Poland
https://orcid.org/0000-0001-6541-5184

Information management and engaged journalism in the conditions of manipulated mainstream media transmission – OKO.press as the example

Introduction

Nowadays, it is really difficult to tell the truth from hypocrisy and populism. It is enough that politicians throw several false statements and, in an instant, a significant part of the public follows the views of their political idols – instead of seeking the truth. The public these days

This conflict gains power from continuous stretching the point so that the truth fits particular party needs. In this conflict, Poland, as a nation, a country, and a society is what counts the least.[1] Therefore, (not only) in Poland there is this enormous urgency for reliable and engaged journalism practiced to the benefit of the social and civic interest. The authors assume that in order to speak about journalistic craftsmanship in the above categories, we need to combine the elements of both the engaged

[1] G. Marczak, "Świetny serwis dziennikarski o 'prawdzie'", Antyweb.pl, 24 June 2016, https://antyweb.pl/dziennikarstwo-sledcze-oko-press [accessed 14 December 2022].

and civic journalism known from common definitions and guard the professionalism. This is the only combination that can provide an antidote to lies and manipulation.

The article presents the fact-checking logic of a Polish press title published online since 2016, OKO.press, which in the authors' view is an excellent example of reliable journalism practiced to the benefit of the public. The study was of a qualitative nature, and it was preceded with research review and theoretical deliberations on the social engagement in the era of new media and the definition issues directly related to the engaged and civic journalism.

An internal fact-checking procedure in authors opinion is a mandatory procedure for journalists, an important and necessary stage in a journalistic routine.[2] The good practice is that the journalists do internal fact-checking every time they publish a news piece. Based on their decision-making patterns, they select the method of fact-checking or – unfortunately – sometimes skip this stage. We called these patterns "fact-checking logic"' as a part of general media logic. Media logic is a concept intended to describe relations between media and the information that they hold. In a general sense, it is a set of criteria that journalists usually use to decide whether some particular information should be covered in the news outlet or not.[3] It is also worth noting, right from the beginning of the analysis, that there are no standardized practices for journalists on how to provide fact-checking.

Trying to prove the assumption, the authors, in their qualitative research, analysed the contents of the press title's website, methods of information management – ways by which the editorial office collected information and the methods for verification of this information. In this aspect, the authors considered the concept of "infomorphosis" in the new media, as the theoretical basis. It is a process that presents internal dynamics, is open, and shows the importance of many new elements (eg commercialization of the internet, geography of information flow, shrinking field of freedom and the increasing scope of control on the internet), as well as mechanisms that have not been investigated yet, and remains unrecognized.[4] In view of the need to limit the volume of the article, as well as following the Silverman's recommendations[5] to limit the research material as much as possible, authors decided that it would be appropriate to look closer at the tab on the OKO.press website called "true or false". A short time interval was chosen – a few days before the Russian invasion of Ukraine till the

---

2 L. Graves, M.A. Amazeen, "Fact-Checking as Idea and Practice in Journalism", [in:] *Oxford Research Encyclopedia of Communication*, Oxford: Oxford University Press, https://doi.org/10.1093/acrefore/9780190228613.013.808.

3 More: T. Harcup, D. O'Neill, "What Is News? Galtung and Ruge revisited", *Journalism Studies*, 2(2), 2001, pp. 261–280.

4 M. Nowina-Konopka, *Infomorfoza. Zarządzanie informacją w nowych mediach*, Toruń: Wydawnictwo Uniwersytetu Jagiellońskiego, 2018.

5 D. Silverman, *Interpretacja danych jakościowych*, trans. M. Głowacka-Grajper, J. Ostrowska, Warszawa: Wydawnictwo Naukowe PWN, 2012.

end of March 2022. The authors make an assumption that the journalism practiced by OKO.press can be considered engaged, civic as well as professional.

New media and engagement in contemporary public affairs

Two main approaches can be indicated in various research that focuses on the analysis of relations between using new information and communication technologies, in particular from the internet, and the level of activity, knowledge and actual participation in public life.[6] We can find at least two opposing viewpoints. On the one hand, there are those who assume that using new technologies has no correlation whatsoever with the phenomenon of participation (its growth or decay). They argue that individuals who get their political knowledge from the internet are mostly those recruited from groups of very high political activity or interested in politics to such an extent that access to the internet bears no relevant impact on the increase in their political participation. We should add that it is not advisable to expect any individuals not interested in politics, seeking information in this field on the internet.

Leaning on the above diagnosis, it seems justified to assume that the current knowledge about politics, and thus the level of political participation within a given society, despite consistent improvement in internet access, fails to show any particularly pronounced growth trends.[7] Even worse, in a more extreme case, the internet may to some extent be dangerous and disastrous to participation, encouraging individuals to restrict themselves to their private affairs and limiting their interactions with others only to the social dimension.[8] In addition, it may pose a threat to less prepared recipients and become a tool for deliberate manipulation and spreading disinformation. Currently, we are dealing with a number of manifestations of the so-called hybrid war, in which the internet and the skilful generation of an alternative, untrue reality play a major role. However, on the other hand, a more optimistic belief comes to rescue, shared by a relatively sizable group of experts in the field. They assume that using technological innovation increases engagement in public affairs in a more or less direct way. In their opinion the internet strengthens political effectiveness, at the same time improving the knowledge on political topics, and this further positively influences the level and intensity of individual participation. Apart from the role played

---

6 K. Kenski, N.J. Stroud, "Connections between Internet use and political efficacy, knowledge, and participation", *Journal of Broadcasting & Electronic Media*, vol. 50, issue 2, 2006, pp.173–192.

7 M. du Vall, M. Majorek, *Nowe media w służbie sieciowych aktywistów*, [in:] M. Wysocka-Pleczyk, B. Świeży, *Człowiek zalogowany*, Kraków: Biblioteka Jagiellońska, 2013, p. 28.

8 J. Wojniak, Uczestnictwo polityczne w obliczu nowych technologii informacyjnych i komunikacyjnych, [in:] M. du Vall, A. Walecka-Rynduch, *"Stare" i "nowe" media w kontekście kampanii politycznych i sprawowania władzy*, Kraków 2010, p. 88.

by an information source in political issues that are important from the society's viewpoint, the internet is undoubtedly a medium that greatly facilitates the contact with politicians, and provides the citizens with the feeling of control over their actions. Furthermore, it is also worth noticing that the internet specificity does not make the individuals uncomfortable with their ignorance in the field of politics.[9]

Hence, we can conclude that an increase in accessibility to a medium, the internet, and an increase in the level of education, not only technological education, exert some impact on a greater level of public participation of the citizens. What is more, it is worth noting that the internet provides some new possibilities of using personal and political freedoms. The supporters of IT influence on democracy believe that this will save the world from further dictatorships and the creation of closed societies. It can be also stated that an information society features a far greater freedom of participation, and first of all the possibility to make more informed choices accompanied by an opportunity for fuller self-determination and thus broader autonomy in decision-making.[10]

Engaged civic journalism

While analysing the normative social theory of the media, Denis McQuail distinguishes the basic elements that construct the paradigm of social responsibility. In the first place, the researcher points out the obligations of the media and journalists towards society. In this context, he points to media ownership as a commodity entrusted by the society. Secondly, the media – first of all the news media – should be characterized with a specific system of values composed of truthfulness, reliability, honesty and objectivity. The third element of "Social Responsibility Theory" is the freedom of the media, albeit subject to self-regulation. The main issues at stake here are freedom of speech and freedom of journalism. Another imperative is the need to adhere to established codes of ethics and good professional practices.[11] According to the above-mentioned rules, the engaged journalism is the way how a journalist understand, experience and carries out their profession, which consists in adopting the responsibility for researching and presenting to public opinion a given issue, event or social process where the evil is escalated, while this evil – unseen by the public opinion, hidden on purpose, etc. – is the cause of individual suffering, the spread of corruption or the growth of social pathologies. Therefore engaged

---

9 *Ibidem*.

10 L. Carter, F. Bélanger, "Internet voting and political participation: An empirical comparison of technological and political factors", *ACM SIGMIS Database*, vol. 43, issue 3, 2012, pp. 26–46.

11 B. Secler, A. Stępińska, A., E. Jurga-Wosik *et al*., "Model dziennikarstwa zorientowany na obywateli w perspektywie paradygmatu społecznej odpowiedzialności mediów. Przykład prasy w Polsce", *Acta Universitatis Lodziensis Folia Litteraria Polonica*, vol. 2, issue 32, 2016, p. 168.

journalism is sometimes called civic journalism. The reason for moving to the position of engaged journalism may be their own reflection, shock caused by a meeting with a "witness of conscience", collusion of the environment (especially the establishment or lobby), etc. A committed journalist leaves the position of a neutral observer relating "a plain course of events". They explore the subject, taking the side of the wronged individual or the common good of the common good of the community in their reports, documentaries or columns. Hence, engaged journalism does not mean propaganda, political or marketing journalism, where a journalist – for the sake of benefits, due to party connotation or so-called wealth of the company – defends a wrong issue or promotes a product that does not deserve the customers' interest. An exposed or disclosed evil can affect the journalist themselves (ostracism of the environment, threat of losing their job, direct or indirect threat to life, death). Engaged journalism reveals the dimension of journalism as a vocation.[12]

Andrew Boyd wrote that journalism is biased. According to Boyd, journalistic bias can be justified and justified in the name of the universal good of humanity. It is characterized by creative expression combined with social responsibility, strong emotional saturation, that experiencing the described reality excludes objectivity.[13] Ryszard Kapuściński's attributes another important feature to engaged journalism – its intentionality.[14] An engaged journalist sets goals and tries to carry out some form of transformation of reality and audience.

The engaged journalism is bravely taking the side of those defenceless and harmed, triggered by the sense of responsibility; it is showing that there is some hope, that you can change something; it opens one's eyes to harm. Engaged journalism is always intentional – it has some clear objectives, the achievement of which is the journalist's priority, regardless of the consequences. Engaged journalists know what they fight for, and what is important is that is also known by their audience. They take steps that take them closer to their goal, but they do not pursue this goal ruthlessly. The engaged journalism is supposed to draw attention to a certain issue, where the evil escalates. It is intended to somehow "open the eyes", not to destroy a man. Of course when we talk about dictatorship that violates human rights we cannot overlook a dictator. But the theme that a journalist is supposed to devote themselves is to tell the public opinion about injustices that affect people, not to destroy a man who stands behind it. An engaged journalist is aware of their responsibility for their words, especially in the face of a certain issue, event or social process. This is when they change their position and transform from a neutral observer into an integral part of the reality they describe. By revealing the escalation of the evil done, a journalist fights either on the side of the

[12] A. Maślana, "Dziennikarstwo zaangażowane – poszukiwanie zagubionego sensu", *Kultura – Media – Teologia*, issue 3, 2010, pp. 121–129.

[13] A. Boyd, *Dziennikarstwo radiowo-telewizyjne. Techniki tworzenia programów informacyjnych*, Kraków: Wydawnictwo Uniwersytetu Jagiellońskiego, 2006, p. 281.

[14] R. Kapuściński, *Autoportret reportera*, Kraków: Znak, 2008, p. 20.

injured or on their behalf. The journalist is forced to deeply research the raised issue and explore the topic – which by the way is their natural reflex when they face the reality that cannot be left unsaid. Engaged journalism is the responsibility that cannot be framed within political correctness, it is the responsibility for noticing something more, the responsibility ready to take the consequences (environmental ostracism, the threat of losing the job, direct or indirect life threat or even death). This is journalism understood as a missionary profession, a vocation to serve the truth.[15]

In this paper we are interested in the category of civic journalism, which is based on civic media created by communities – both real and virtual – and the existence of a medium created by this community.

In documents and studies devoted to this type of media, most attention is paid to two basic types of communities that make it up: those that share a common residence or interest. The virtual space is a special type place, where people while connecting through computer networks can communicate on both levels – individual and group. This fosters development of new social forms, namely the virtual communities. The research shows that communication through new media keeps the social bonds because it provides the users with the sense of belonging. However, it should be borne in mind that it is not a separate reality, an isolated social phenomenon. A network is just one of the forms of interactions which people undertake while accompanied by their "background" meaning the socio-economic status, cultural environment, age, sex, relationships from the real world, to name a few.[16] Nowadays, the internet should not be separated from other means of communication between human beings. Large internet networks based on weak relationships and accessibility of interpersonal online interaction modes actually support collective actions.[17] The Internet is a medium that fosters development of relatively weak social bonds, in specific contexts consciously valued higher by people than stronger bonds (weak bonds turn out to be more useful when it comes to implementation of organizations' or social movements' objectives). In this context, "hidden" bonds – potentially possible but not activated by social interaction – are also important. Individuals belonging to the same network (eg through digital networking: mailing lists, social networking profiles, databases) have developed "hidden" ties, accessible through communication structures that, when activated, have weak yet potentially strong ties.[18]

It is worth pointing out what are the characteristics of the civic media created by those communities. According to the definition of civic media proposed in the

---

15 A. Maślana, *op. cit*., pp. 121–129.

16 M. Szpunar, "Społeczności wirtualne jako nowy typ społeczności – eksplikacja socjologiczna", *Studia Socjologiczne*, issue 2(173), 2004, pp. 107 and 99.

17 L.A. Lievrouw, *Media alternatywne i zaangażowane społecznie*, Warszawa: Wydawnictwo Uniwersytetu Jagiellońskiego, 2012, p. 199.

18 J. Nowak, *Aktywność obywateli online. Teoria a praktyka*, Lublin: Wydawnictwo Uniwersytetu Marii Curie-Skłodowskiej, 2011, p. 86.

Declaration of the Committee of Ministers on the role of community media in promoting social cohesion and intercultural dialogue,[19] media types should meet the following conditions: be independent of governmental, commercial or religious institutions as well as political parties; operate on a non-profit basis; be based on cooperation of volunteers from civil society members in their conduct and management; act for the benefit of civil society and the community they serve; be owned and accountable to the community they serve; be involved in activating representatives of various social groups and intercultural dialogue.[20]

Civic journalism is undoubtedly a manifestation of civil society – one that feels responsible for itself. "I" understood in individual terms is replaced by "we" in civil society; the responsibility for one's own and one's relatives' development is gradually supplemented by the need for responsibility for others, the "strangers". This manifests itself in greater political participation, greater interest in the idea of volunteering, as well as concern for the life of local communities.[21]

To sum up this section, the civil journalism involved is co-responsible and participatory. Nowadays, it uses technology to create, select and disseminate information. Its objective is to provide people with information that help them make decisions in a conscious manner. It uses the democratic potential of the internet and of the new-type (virtual) societies, thus transforming the previous centralized social structure. This activity consists in raising awareness and advocacy.

OKO.press's information management strategy in the face of democracy instability

Throughout the 20th century, the role of print media and television in shaping political processes was decisive. It became clear that independent press and other media along with have been seen as the fourth power, promoting economic and social growth, looking at the decision-makers' hand in particular. This view is supported by the fact that significant part of research in this scope shows that freedom of the media has some substantial impact on public policy of democratic governance. On the other hand, the theoretical and empirical knowledge of mechanisms

[19] *Declaration of the Committee of Ministers on the role of community media in promoting social cohesion and intercultural dialogue*, Council of Europe, 11 February 2009, www.coe.int/en/web/freedom-expression/news-media/-/asset_publisher/Mo0WV0OwvbhA/content/declaration-of-the-committee-of-ministers-on-the-role-of-community-media-in-promoting-social-cohesion-and-intercultural-dialogue-adopted-on-11-februar?inheritRedirect=false [accessed: 16 April 2022].

[20] U. Doliwa, "Dziennikarstwo obywatelskie, czyli jakie?", *Nowe Media*, no. 3, 2012, pp. 81–100.

[21] "Dziennikarstwo obywatelskie – definicja, diagnoza i przyszłość", E.redaktor, 6 June 2011, http://eredaktor.pl/media-internetowe/dziennikarstwo-obywatelskie-definicja-diagnoza-i-przyszlosc [accessed: 13 April 2022].

that stand behind the global variability in the freedom of the media is more limited. This is a result of semi democratic systems, or even facade democracies or hybrid systems that distort the space for the flow of information. Hence, the widely held view among the media experts and analysts of this space that the majority of regimes describing themselves as democratic should be classified in terms of autocratic statehood due to the interference in the flow of information. A direct factor that influences this classification is the tendency to more or less suppress media messages and treating censorship as an inseparable component for functioning of a system.

Imbalances in the relations between the power and media along with the intensity of these imbalances allow to show some authoritarian subtypes within which it is possible to identify the levels of media freedom. However, it is worth asking a question about what do we mean by the simple term "freedom of the media"? The freedom of the media, or more precisely its scope, is defined as a degree to which each country allows for the freedom in the flow of information that depends mainly on: the scope of political interference, eg through intimidation, censorship or coercion (which is influenced by the political environment); implemented constitutional standards and the regulations resulting from the constitution (legal surroundings); and the independence of the publishers' decisions from the commercial or private interests (economic surroundings).[22] According to the Universal Declaration of Human Rights of the United Nations (UN), freedom of expression is a universal human right protecting the right to "seek, receive and impart information and ideas by any means, regardless of frontiers."[23] It seems that this approach would need to be adopted as a starting point for further deliberations on restrictions to the freedom of the flow of information. Thus, the importance of civic journalism, combined with the overarching principle of freedom of speech, understood in terms of human rights, create (in a sense) a space for the emergence of grass-roots publishers that will provide a reliable analysis of reality and will guard the integrity of the message. OKO.press is an example of this type of online publisher.

"OKO.press has been established as a result of concerns with the situation in Poland – authoritarian aspirations of the political majority, radicalization of social attitudes, especially the right-wing fundamentalism and nationalism, the increasing conflict but also the weakness of the opposition. Our response is reliable analysis of words and deeds in public life, tracking forgeries and lies, revealing the political corruption, populism and purges. A critical approach, without any preferential treatment, with discipline."[24]

---

[22] M.J. Abramowitz, J. Dunham, "Freedom of the Press", Freedom House, 2017, https://freedomhouse.org/report/freedom-press/freedom-press-2017 [accessed: 15 April 2022].

[23] Powszechna deklaracja praw człowieka, art. 19, ONZ, https://amnesty.org.pl/wp-content/uploads/2016/04/Powszechna_Deklaracja_Praw_Czlowieka.pdf.

[24] "Ruszył serwis OKO.press patrzący na ręce władzy. W redakcji dziennikarze z "GW", "Polityki", TVN i TOK FM", Wirtualne Media, 15 June 2016, https://www.wirtualnemedia.pl/artykul/

The OKO.press website tells us that this is a portal that verifies the facts and carries out investigative journalism. This is a social medium and an archive of public life. First of all, this is the "civic tool for control over authorities."[25] The medium was created in the face of concerns about the paralysis of Polish democracy and as a shield protecting from the flood of words spoken without any responsibility, lies and half-truths.

From the very moment of its creation the portal has been repeatedly appreciated and awarded by the journalistic environment itself, it among others has received several Grand Press[26] awards, and in 2018, the journalist of OKO.press received the Amnesty International Poland "Pen of Hope" award. It is worth mentioning that the engaged nature of journalism may be proven by the courage and tenacity of those who write for the portal. A small independent editorial office has repeatedly embarrassed the powerful media corporations and taken its toll on the authorities. At the same time, we should not forget that the Polish law enforcement authorities tried to cool down the OKO.press' enthusiasm, among other things they abused their power towards this independent medium by harassing journalists and carrying out illegal searches in order to obtain journalistic materials.[27]

An element that clearly demonstrates the engagement and civic character of the presented website is the emphasis on cooperation with readers. As it has been already stressed, one of the OKO.press website's missions is to reveal any irregularities and scandals related to operations of the public institution, as well as publicizing corruption, nepotism, cronyism and other abuses of those in power. It would not have been possible without the help and engagement of the society, the members of which encounter misuse of powers in the workplace or in everyday life. However, the editorial staff, being aware that subsequent regulations implemented by the Polish authorities, making the surveillance of citizens easier, does not encourage cooperation with media, made a secure and anonymous inbox available to its readers – "SYGNAŁ" (SIGNAL). What is important, it was the first editorial office in Poland to do this, using an Internet tool that protects both the communicated contents and the identity of the informants.[28] It can be clearly seen that the editorial office cares that the persons sending information about any abuses or crimes committed by the people in power do not only feel safe, but are actually provided with this security.

---

ruszyl-serwis-oko-press-patrzacy-na-rece-wladzy-w-redakcji-dziennikarze-z-gw-polityki-tvn-i-tok-fm [accessed: 14 April 2022].

25 *O nas*, OKO.press 2022, https://oko.press/o-nas [accessed: 14 December 2022].

26 Grand Press – an annual prize awarded from 1997 by the nationwide journalistic monthly magazine "Press" for the best Polish press, radio and TV journalists.

27 E. Siedlecka, "Policja przeszukała mieszkania dziennikarzy OKO.press i zabrała materiały dziennikarskie", Polityka.pl, 2018, https://www.polityka.pl/tygodnikpolityka/kraj/1774768,1,policja-przeszukala-mieszkania-dziennikarzy-okopress-i-zabrala-materialy-dziennikarskie.read [accessed: 12 April 2022].

28 "Jak oceniamy prawdę i fałsz", OKO.press, 2016–2019, https://oko.press/oceniamy-prawde-falsz. [accessed 14 December 2022].

The OKO.press contact box is available in the TOR browser,[29] allowing for anonymous access to the internet. The readers can leave their accounts of various irregularities and abuses of those in power, documents, pictures and videos on the "SYGNAŁ" page. The materials are encrypted and transferred over the TOR network. Only the investigative journalists from OKO.press have access to those materials, but they also do not know who the sender of the message is, unless the sender disclose this information themselves. It is important that even then the informant – according to the press law – has the choice of whether to reveal themselves in the OKO.press articles or remain anonymous for other readers.[30]

Darknet that the above-mentioned TOR browser is a part of is popular among journalists and political bloggers, especially in those countries where censorship and political prison are common. Online anonymity allows the people, also the informants, to communicate with their "sources" and publish contents without being afraid of their security. The readers can use the same anonymity to access the information published in a local network, which is blocked by various agencies, created for that purpose, operating mainly in authoritarian or totalitarian regimes.[31] The activists use the Darknet also with a purpose of free self-organization, without being afraid of the intervention from the authorities that they oppose.[32]

The above suggests that full anonymity is possible on the internet, although we often hear some information that all we do on the internet may be easily identified. This is undoubtedly right, and an average Internet user associates using the Darknet tools with something complicated, unreachable, with comprehensive procedures and super-fast hi-tech computers.[33] However, it turns out that using the Darknet is not particularly complex (at least to some extent) and it does not entail the need to invest in any technological innovations. TOR browser gives the user a much greater potential for anonymity in the virtual space, can be used to surf the web while providing the user with additional protection against unwanted traffic observers, and above all it protects the user against hackers, various forms of online espionage, collection of

---

[29] TOR is a network that prevents network traffic analysis and consequently provides users with almost anonymous access to internet resources.

[30] "'Cebulowy ruter' przeciw cenzurze internetu w Rosji. Czyli pora na Tora. I na Snowflake!", OKO.press, 20 March 2022, https://oko.press/tor-przeciw-cenzurze-internetu-w-rosji [accessed: 14 December 2022].

[31] Q. Wang, G. Xun, G.T.K. Nguyen *et al*., "Censorspoofer: asymmetric communication using ip spoofing for censorship-resistant web browsing", *Proceedings of the 2012 ACM conference on Computer and communications security, ACM*, 2012, pp. 121–132, www.researchgate.net/publication/221672885_CensorSpoofer_Asymmetric_Communication_with_IP_Spoofing_forCensorship-Resistant_Web_Browsing.

[32] A. Klimburg, "Roots Unknown–Cyberconflict Past, Present & Future", *S&F Sicherheit und Frieden*, no. 32, issue 1, 2014, p. 2.

[33] M. Majorek, "Darknet. Ostatni bastion wolności w internecie", *Bezpieczeństwo. Teoria i praktyka*, issue 4, 2017, pp. 85–96.

personal data without the user's will and consent, and of other sensitive information.[34] The tool also gives you the opportunity to visit websites published anonymously on the web, which are inaccessible to people surfing the virtual space in a traditional way. This is one of the most frequently used features of the browser.[35]

The OKO.press website's structure is very clear, and a reader can easily find any topics that are interesting for them. The whole thing is divided into seven main tabs: about us, investigations (OKO.press conducts reliable journalistic investigations; vets the activities of politicians and officials, publicizes corruption, nepotism, cronyism; intervenes in cases of obstructing access to public information; reports on court trials), true or false (OKO.press checks whether politicians are telling the truth; it analyses the statements of politicians, senior officials, church hierarchies, leaders of social movements, and each verified statement is discussed in more detail in the article), analyses and surveys (OKO.press publishes analytical texts on economic, demographic and social problems; popularizes studies and reports of non-governmental organizations, scientific circles, think tanks, independent media; it orders its own and discusses other opinion polls), events (the portal publishes articles on current political events, abuses of power, acts of social resistance), audio-video (here you can find reports and documentaries, live reports from events, editorial discussions, podcasts), support us. An additional tab appears for the election time #OKOnaWybory (#OKOforElections) (where election programs are analysed, election campaigns are evaluated, results of polls are published or election results are commented on). It is even easier to reach specific materials using the "Our Topics" panel prepared by the editorial team, where we can choose from the following keywords: scandals, education, ecology, economy, history, women, church, culture, LGBT+, media, nationalism, NGO, disability, opposition, police and services, social policy, foreign policy, human rights, animal rights, propaganda, protests, judiciary, refugees and immigrants, power, elections, health.[36]

The fact-checking logic of the OKO.press journal

It is worth taking a closer look at selected texts published on the portal. The authors decided that in order to illustrate and prove the engaged character of journalism in OKO.press it will be appropriate to look closer at the tab on the website called truth or false. A short time interval was chosen – few days before Russian invasion of Ukraine till the end of march 2022.

---

[34] *Ibidem*.

[35] M. Spitters, S. Verbruggen, M. van Staalduinen, Towards a comprehensive insight into the thematic organization of the tor hidden services, [in:] *Intelligence and Security Informatics Conference, 2014 IEEE Joint*, ed. J.E. Guerrero, Danvers, MA: IEEE Computer Society, 2014, pp. 221–222.

[36] OKO.press, https://oko.press.

In the "Truth and false" tab, OKO.press checks whether the politicians tell the truth. A "falsemeter" is used for this purpose, based on 12 principles:

"1. We analyse statements of politicians, senior state and local government officials, church hierarchies, leaders of social movements, leaders of influential organizations, leaders of economic life, etc. We do not analyse statements of media people, artists, bystanders, anonymous opinions in social media, etc.
2. Every day we search through public speeches, party and governmental documents, media, social media, etc., for statements worth checking.
3. The choice is based on whether or not the statement:
   - Is verifiable, whether we can reach information that will allow to asses it;
   - Refers to facts, describes events, gives figures, etc;
   - Considers an important issues and/or the speaker is a relevant figure;
   - Is catchy, confirms a stereotype, may infect the mass imagination;
   - Is in such a form that the receivers find it hard to decide whether it is true or not without having any deeper knowledge.
4. e follow the rule that at least one third of the attention is paid to the statement of people outside the ruling group.
5. We assess the statements with the 'Oko falsemeter', which can indicate six states:
   - False – manifestly contradictory to facts;
   - Rather false – there is some truth in it, but the whole is contradictory to the facts and/or the context is misleading;
   - Half-truth – rather factually correct, but no important information is available;
   - Almost true – in fact, it is this way, but it is not precise enough;
   - Truth – the statement is true, there's evidence to prove it;
   - The 'falsemeter' is breaks down – absurd, insinuation.
6. Furthermore, 'Oko' awards two 'distinctions':

- Koziołek matołek[37] – for statements that are exceptionally foolish, proving lack of elementary knowledge or orientation in the subject matter;
- Dyzma[38] – for insulting, ruthless statements, manipulation of the truth.

7. We take context into account.
8. We assume that when making a statement, a politician (a public person) should present facts that support it. Evidence lies with whoever informs/discloses information to the public.
9. While verifying whether a given statement is true or false, 'Oko' provides factual arguments, figures, statistics. We refer to the sources we use.

---

[37] Literary character created by Kornel Makuszyński and Marian Walentynowicz in one of the first children's picture stories in Poland

[38] Nikodem Dyzma – fictional literary character. The title character of the novel "Nikodem Dyzma career" by Tadeusz Dołęga-Mostowicz and its subsequent adaptations.

10. We try not to impose our assessments and we are open to criticism of our work. We update the assessment when something important changed. We accept suggestions, corrections and hints. In justified cases we publish corrections and apologize to those who we misjudged. Each correction of an assessment is written on the primary version, and it remains visible.
11. Even if we use a lighter tone or a humorous title, we analyse as reliably and honestly as we can.
12. We discuss every assessment in a team, and we also use the help of experts in a given field if we need it."[39]

Considering the above, since the beginning of the war in Ukraine (February 24, 2022), OKO.press has not ceased to fight fake news and has been trying to reveal false information to Poles, which is largely necessary for maintaining relative peace in the face of ongoing war. Particularly noteworthy is the construction of the new section devoted to the war in Ukraine. This department is called "Goworit Moskwa". It is devoted to reporting on and analysing every slice of Russian propaganda presented daily in the government media. The analysis presented in the indicated section shows the point of view of the recipient of the message, which has been manipulated for years (the assumption is that it is the average Russian watching government TV). OKO.press focuses on specific terminology, showing its enormous strength. Here we are talking about denazification, special operation, defence of the Russian-speaking population. Added to this we have the anti-Christian character of the defenders of Ukraine, who are compared to the occultists and the servants of Satan.[40] On the one hand, it may seem absurd, but OKO.press perfectly explains this type of aberration, which gives answers to questions about the possibility of denying obvious facts. This denial of facts on the Russian side is carried out in an extremely well thought out and exceptionally organized manner. The "Goworit Moskwa" series is an excellent example of a reliable refutation of fake news and an in-depth analysis of each sentence uttered by the aggressor.

In the context of spreading disinformation, great concern was caused, inter alia, by reports of fighting and a fire at the Enerhodar nuclear power plant, which raised concerns about radioactive contamination in Europe. After the fact checking procedure was carried out, OKO.press showed that today nuclear power plants are built in such a way that they are not threatened by fires or, for example, aircraft falls, and that the fire in Enerhodar did not affect the reactors at all.[41] Subsequent reports related to the

---

[39] "Jak oceniamy prawdę i fałsz", *op. cit.*

[40] A. Jędrzejczyk, "Goworit Moskwa, 10 uzasadnień zniszczenia Mariupola i zabicia jego obrońców", OKO.press, 20 April 2022, https://oko.press/goworit-moskwa-10-uzasadnien-zniszczenia-mariupola [accessed: 20 April 2022].

[41] "Największa elektrownia jądrowa w Europie płonęła po rosyjskim ostrzale. Bać się? Wyjaśniamy", OKO.press, 4 March 2022, https://oko.press/najwieksza-elektrownia-jadrowa-w-europie-plonela-po-rosyjskim-ostrzale-bac-sie-wyjasniamy [accessed: 14 December 2022].

radioactive threat said, among others, about the need for Poles to obtain Lugol's iodine fluid. Pharmacists reported that people were buying up liquid from pharmacies en masse. Journalists proved that Ukrainian power plants are too far away for a radioactive cloud to reach Poland, and that Lugol's iodine liquid can be very harmful to some people, especially when used without medical supervision.[42]

OKO.Press also denied the words uttered by the Russian President Vladimir Putin in his speech on February 21, 2022, in which he stated that "Modern Ukraine was entirely created by Russia, or, to be more precise, by Bolshevik communist Russia." Journalists proved that this information was false and clearly emphasized that the Ukrainians created their own state in 1918.[43]

Another topic in the OKOPress True or False section is the issue of Russian coal and its import by Poland. The newspaper specialists analysed, among others, statements by Paweł Szrot (Poranek TOK FM) on March 25 and by Speaker of the Senate, Tomasz Grodzki (statement to the Supreme Council of Ukraine) on the same day. The first statement assumed that Poland no longer imports coal from Russia and that was considered as a half-truth. It was explained that the available data show that the state and state-owned companies do not buy coal from Russia. At the same time, it was recognized that the Polish government had not done enough to push Russian coal out of the market so far. On the other hand, Grodzki's statement, who explicitly stated that the government imports Russian coal, was found to be false after a fact checking inquiry by journalists. Similarly to the above – yes, Poland has a problem with Russian coal, but it is not brought by the Polish government or state-owned companies. It is done by private entities, and coal is burned in small heating plants and domestic boiler houses.[44]

One of the popular arguments preached in the public debate, that Europe could not afford an embargo on Russian energy raw materials, was also refuted. This claim was found to be false. Yes, some economies will lose at first, but they will be able to adapt quite quickly, and the financing of the Putin regime is much more dangerous.[45]

Both the "Goworit Moskwa" section and the True or False section refer to high standards in the context of examining irregularities and inaccuracies in the media

---

42 "Płyn Lugola – pić, czy nie pić? Nie pić, bo może zaszkodzić! I nie ma zagrożenia radioaktywną chmurą", OKO.press, 4 March 2022, https://oko.press/plyn-lugola-pic-czy-nie-pic-nie-pic-bomoze-zaszkodzic [[accessed: 14 December 2022].

43 "Ukrainę stworzyła komunistyczna Rosja? Było inaczej. Pokazujemy, jak Putin fałszuje historię", OKO.press, 22 February 2022, https://oko.press/ukraine-stworzyla-komunistyczna-rosja-bylo-inaczej [accessed: 14 December 2022].

44 "Rząd zapowiada embargo na rosyjski węgiel. Do przyszłej zimy już trzeba się przygotować", OKO.press, 29 March 2022, https://oko.press/wegiel-z-rosji-w-polsce [accessed: 14 December 2022].

45 "Obecne sankcje to za mało: czas odciąć ropę i gaz z Rosji. Europa poradzi sobie bez nich", OKO.press, 18 March 2022, https://oko.press/rosja-na-razie-nie-bankrutuje-czas-na-sankcje-na-rope-i-gaz [accessed: 14 December 2022].

coverage. In the present situation, when hybrid and conventional war is waged, the analysis and interpretation of the message, as well as the translation of hidden content is a necessary condition for maintaining proper social awareness. We are talking about Poland, but similar initiatives probably arose or are being created elsewhere. Working in accordance with the patterns described above gives a chance to create a solid counterbalance to the wave of Russian disinformation that is present in social media around the world.

Final remarks

At a basic level, contemporary engaged journalism is practiced in the virtual space, and it is a significant change and an example of improving the ways of communication and cooperation with community members. This is journalism that has been reformulated in a way – from the (one-way) function of broadcasting, the focus is shifted to the community and the content is communicated in two directions. The message is now a kind of a flow, a form of conversation with the community, and the messages are more relevant, responsive and they reflect the interests and needs of the community. In this case, OKO.press absolutely meets the above requirements, and what is more it also fits into the model of missionary journalism, which requires the authors to have particular predispositions, especially when they deal with topics that are inconvenient for the representatives of the establishment. Another element that confirms the thesis is a business model of the OKO.press portal, which is based on grants and community funding. There is no doubt that a website which relies on engaged investigative journalism needs significant resources for the reliable implementation of the topics under investigation, and therefore this model, although in line with the principles of participatory journalism, may prove difficult to be maintained in the long term.

The important element of the original assumption which gives rise to most of the doubts when it comes to the civic character of the discussed portal, namely the professionalism, is undoubtedly necessary for the quality and reliability of the published contents. It is often pointed out that engaged, civic journalism does not go hand in hand with journalism practiced by professionals. Nevertheless, the analysis of the content published on the discussed portal and the parallel analysis of the current political situation allows us to state that this untypical model of journalism is extremely valuable to citizens. The model of information management presented by OKO.press, assuming an in-depth analysis of the content and exposing false assumptions and statements by the rulers, both in Poland and in the international arena, should be assessed positively. Indeed, this type of publisher seems necessary from the point of view of maintaining properly functioning mechanisms of democracy and preventing the spread of fake news and mass disinformation. The

professional and engaged approach to the investigated issues allows the citizens to feel sure that the presented information is reliable and to keep the hope that the strongly undermined democratic mechanisms that guard the freedom of expression are used to the maximum extent for the public good.

References

Abramowitz M.J., Dunham J., "Freedom of the Press", Freedom House, 2017, https://freedomhouse.org/report/freedom-press/freedom-press-2017 [accessed: 15 April 2022].

Boyd A., *Dziennikarstwo radiowo-telewizyjne. Techniki tworzenia programów informacyjnych*, Wydawnictwo Uniwersytetu Jagiellońskiego, Kraków 2006.

Carter L., Bélanger F., "Internet voting and political participation: An empirical comparison of technological and political factors", *ACM SIGMIS Database*, vol. 43, issue 3, 2012, pp. 26–46.

Chaabane A., Manils P., Kaafar M.A., "Digging into anonymous traffic: A deep analysis of the tor anonymizing network", *2010 Fourth International Conference on Network and System Security*, 2010, pp. 167–174.

"'Cebulowy ruter' przeciw cenzurze internetu w Rosji. Czyli pora na Tora. I na Snowflake!", OKO.press, 20 March 2022, https://oko.press/tor-przeciw-cenzurze-internetu-w-rosji [accessed: 14 December 2022].

Declaration of the Committee of Ministers on the role of community media in promoting social cohesion and intercultural dialogue, Council of Europe, 11 February 2009, https://www.coe.int/en/web/freedom-expression/news-media/-/asset_publisher/Mo0WV0OwvbhA/content/declaration-of-the-committee-of-ministers-on-the-role-of-community-media-in-promoting-social-cohesion-and-intercultural-dialogue-adopted-on-11-februar?inheritRedirect=false [accessed: 16 April 2022].

"Dziennikarstwo obywatelskie – definicja, diagnoza i przyszłość", E.redaktor, 6 June 2011, http://eredaktor.pl/media-internetowe/dziennikarstwo-obywatelskie-definicja-diagnoza-i-przyszlosc [accessed: 13 April 2022].

Doliwa U., "Dziennikarstwo obywatelskie, czyli jakie?", *Nowe Media*, no. 3, 2012, pp. 81–100.

du Vall M., Majorek M., Nowe media w służbie sieciowych aktywistów, [in:] M. Wysocka-Pleczyk, B. Świeży, *Człowiek zalogowany*, Kraków: Biblioteka Jagiellońska, 2013, pp. 27–37.

Graves L., Amazeen M.A., Fact-Checking as Idea and Practice in Journalism, [in:] *Oxford Research Encyclopedia of Communication*, Oxford: Oxford University Press 2019, https://doi.org/10.1093/acrefore/9780190228613.013.808.

Grela S., "Freedom House obniża ocenę wolności mediów w Polsce. Stowarzyszenie Dziennikarzy Polskich protestuje, ale argumentów brak", OKO.press, 17 July 2017, https://oko.press/freedom-house-obniza-ocene-wolnosci-mediow-w-polsce-stowarzyszenie-dziennikarzy-polskich-protestuje-argumentow-brak [accessed: 12 April 2022].

Harcup T., O'Neill D., "What Is News? Galtung and Ruge revisited", *Journalism Studies*, 2(2), 2001, pp. 261–280.

"Jak oceniamy prawdę i fałsz", OKO.press, 2016–2019, https://oko.press/oceniamy-prawde-falsz. [accessed: 14 December 2022].

Jędrzejczyk A., "Goworit Moskwa, 10 uzasadnień zniszczenia Mariupola i zabicia jego obrońców", OKO.press, 20 April 2022, https://oko.press/goworit-moskwa-10-uzasadnien-zniszczenia-mariupola [accessed: 20 April 2022].

Kapuściński R., *Autoportret reportera*, Kraków: Znak, 2008.

Kenski K., Stroud N.J., "Connections between Internet use and political efficacy, knowledge, and participation", *Journal of Broadcasting & Electronic Media*, vol. 50, issue 2, 2006, pp.173–192.

Klimburg A., "Roots Unknown–Cyberconflict Past, Present & Future", *S&F Sicherheit und Frieden*, no. 32, issue 1, 2014, pp. 1–8.

Lievrouw L.A., *Media alternatywne i zaangażowane społecznie*, Warszawa: Wydawnictwo Naukowe PWN, 2012.

Majorek M., "Darknet. Ostatni bastion wolności w internecie", *Bezpieczeństwo. Teoria i praktyka*, issue 4, 2017, pp. 85–96.

Marczak G., "Świetny serwis dziennikarski o 'prawdzie'", Antyweb.pl, 24 June 2016, https://antyweb.pl/dziennikarstwo-sledcze-oko-press [accessed: 14 December 2022].

Maślana A., "Dziennikarstwo zaangażowane – poszukiwanie zagubionego sensu", *Kultura – Media – Teologia*, issue 3, 2010, pp. 121–129.

"Największa elektrownia jądrowa w Europie płonęła po rosyjskim ostrzale. Bać się? Wyjaśniamy", OKO.press, 4 March 2022, https://oko.press/najwieksza-elektrownia-jadrowa-w-europie-plonela-po-rosyjskim-ostrzale-bac-sie-wyjasniamy [accessed: 14 December 2022].

Nowak J., *Aktywność obywateli online. Teoria a praktyka*, Lublin: Wydawnictwo Uniwersytetu Marii Curie-Skłodowskiej, 2011.

Nowina-Konopka M., *Infomorfoza. Zarządzanie informacją w nowych mediach*, Toruń: Wydawnictwo Uniwersytetu Jagiellońskiego, 2018.

"Obecne sankcje to za mało: czas odciąć ropę i gaz z Rosji. Europa poradzi sobie bez nich", OKO.press, 18 March 2022, https://oko.press/rosja-na-razie-nie-bankrutuje-czas-na-sankcje-na-rope-i-gaz [accessed: 14 December 2022].

"O nas", OKO.press 2022, https://oko.press/o-nas [accessed: 14 December 2022].

"Płyn Lugola - pić, czy nie pić? Nie pić, bo może zaszkodzić! I nie ma zagrożenia radioaktywną chmurą", OKO.press, 4 March 2022, https://oko.press/plyn-lugola-pic-czy-nie-pic-nie-pic-bo-moze-zaszkodzic [14 December 2022].

Powszechna deklaracja praw człowieka, art. 19, ONZ, https://amnesty.org.pl/wp-content/uploads/2016/04/Powszechna_Deklaracja_Praw_Czlowieka.pdf.

"Ruszył serwis OKO.press patrzący na ręce władzy. W redakcji dziennikarze z "GW", "Polityki", TVN i TOK FM", Wirtualne Media, 15 June 2016, www.wirtualnemedia.pl/artykul/ruszyl-serwis-oko-press-patrzacy-na-rece-wladzy-w-redakcji-dziennikarze-z-gw-polityki-tvn-i-tok-fm [accessed: 14 April 2022].

"Rząd zapowiada embargo na rosyjski węgiel. Do przyszłej zimy już trzeba się przygotować", OKO.press, 29 March 2022, https://oko.press/wegiel-z-rosji-w-polsce [accessed: 14 December 2022].

Secler B., Stępińska A., Jurga-Wosik E. *et al*., "Model dziennikarstwa zorientowany na obywateli w perspektywie paradygmatu społecznej odpowiedzialności mediów. Przykład prasy w Polsce", *Acta Universitatis Lodziensis Folia Litteraria Polonica*, vol. 2, issue 32, 2016, pp. 167–185.

Siedlecka E., "Policja przeszukała mieszkania dziennikarzy OKO.press i zabrała materiały dziennikarskie", Polityka.pl, 9 December 2018, https://www.polityka.pl/tygodnikpolityka/kraj/1774768,1,policja-przeszukala-mieszkania-dziennikarzy-okopress-i-zabrala-materialy-dziennikarskie.read [accessed: 12 April 2022]

Silverman D., *Interpretacja danych jakościowych*, trans. M. Głowacka-Grajper, J. Ostrowska, Warszawa: Wydawnictwo Naukowe PWN, 2012.

Spitters M., Verbruggen S., Staalduinen M. van, Towards a comprehensive insight into the thematic organization of the tor hidden services, [in:] *Intelligence and Security Informatics Conference*

(JISIC), 2014 IEEE Joint, ed. J.E. Guerrero, Danvers, MA: IEEE Computer Society, 2014, pp. 220–223.

Szpunar M., "Społeczności wirtualne jako nowy typ społeczności – eksplikacja socjologiczna", *Studia Socjologiczne*, issue 2(173), 2004, pp. 95–135.

"Ukrainę stworzyła komunistyczna Rosja? Było inaczej. Pokazujemy, jak Putin fałszuje historię", OKO.press, 22 February 2022, https://oko.press/ukraine-stworzyla-komunistyczna-rosja-bylo-inaczej [accessed: 14 December 2022].

Wang Q., Xun G., Nguyen G.T.K. *et al*., "Censorspoofer: Asymmetric communication using ip spoofing for censorship-resistant web browsing", *Proceedings of the 2012 ACM conference on Computer and communications security, ACM*, 2012, pp. 121–132, www.researchgate.net/publication/221672885_CensorSpoofer_Asymmetric_Communication_with_IP_Spoofing_forCensorship-Resistant_Web_Browsing.

Wojniak J., Uczestnictwo polityczne w obliczu nowych technologii informacyjnych i komunikacyjnych, [in:] *"Stare" i "nowe" media w kontekście kampanii politycznych i sprawowania władzy*, eds. M. du Vall, A. Walecka-Rynduch, Kraków: Krakowska Akademia AFM, 2010, pp. 87–98.

Information management and engaged journalism in the conditions of manipulated mainstream media transmission – OKO.press as the example

Abstract

The article presents an internal fact-checking procedure which in the opinion of the authors is a mandatory procedure for journalists, an important and necessary stage in a journalistic routine. The good practice is that the journalists do internal fact-checking every time they publish a news piece. Based on their decision-making patterns, they select the method of fact-checking or – unfortunately – sometimes skip this stage. We called these "fact-checking logic" patterns as a part of general media logic. In this article, we present the fact-checking logic of a Polish press title published online since 2016, OKO.press, which, in the authors' view, is an excellent example of reliable journalism practiced to the benefit of the public. Particular attention was paid to information management methods: obtaining, verifying and presenting information. Nowadays, there is enormous urgency for reliable and at the same time engaged journalism practiced to the benefit of the social and civic interest. The authors assume that, in order to speak about journalistic craftsmanship in the above categories, we need to combine the elements of both the engaged and civic journalism known from common definitions and to guard the professionalism. This is the only combination that can provide an antidote to manipulation and disinformation. The case study was of a qualitative nature, and it was preceded with research review and theoretical deliberations on the social engagement in the era of new media. The main goal is to present and analyse the activities of the OKO.press journal in the context of combating disinformation spread in the media dependent on the Kremlin's authorities.

Key words: information management, engaged journalism, fact-checking, civic interest, independent journalism, disinformation

BEZPIECZEŃSTWO TEORIA I PRAKTYKA
SECURITY THEORY AND PRACTICE
e-ISSN 2451-0718
ISSN 1899-6264
2022
No. 2 (XLVII)
DOI: 10.48269/2451-0718-btip-2022-2-009
Received: 29.04.2022
Accepted: 18.07.2022

Marta Majorek

Associate Professor, Andrzej Frycz Modrzewski Krakow University
https://orcid.org/0000-0001-6541-5184

Top-down selection of information as an element of strategic information management in the event of a threat of internal destabilisation

Introduction

Undoubtedly, even in authoritarian states it is possible to identify ways to publish sensitive material. Such situations occur because the authorities do not, by definition, exercise absolute control over the media. This is often because they cannot, or because they do not have to. The reason for this type of situation is that it takes advantage of certain cracks that can be identified in state mechanisms for controlling the flow of information. However, there is then pressure and at the same time risk, which is even less conducive to the free and unhindered flow of information.[1] For the purposes of the analysis carried out within the framework of this article, Russia appears as an excellent example that can be used to show the specificity of the region in terms of the management of information and free media space in systems with authoritarian characteristics. Moreover, the state indicated has a legally elected government with the real support of a significant segment of Russian society. Furthermore, Russia gives its citizens constitutional guarantees of freedom of speech and freedom of the press, but does not actually boast a free media. Russia has both

[1] S. Stier, "Democracy, Autocracy and the News: the Impact of Regime Type on Media Freedom", *Democratisation*, vol. 22, issue 7, 2015, p. 1274, https://doi.org/10.1080/13510347.2014.964643.

official and unofficial censorship and is marked by a low media freedom index published by NGOs such as Reporters Without Borders and Freedom House.[2]

Although media control is relatively common in semi-authoritarian countries, the authorities of these countries do not exercise total control over the press. On the contrary, it takes place in a notable majority through the use of indirect methods. The information management model is usually supported by the implementation of so-called soft methods, by which is meant the absence of direct interference involving the use of violence and coercion. There are undoubtedly cases in some countries where such extreme tools are used against those who publish content, of which Russia is an infamous example.[3]

One can distinguish various norms that the Russian authorities used to impose on media content, however, these laws often do not focus on purely political content. Instead, the law restricts media freedom in somewhat different ways, for example, by prohibiting the promotion of dangerous substances, making indecent content public, insulting state authorities, or prohibiting the promotion of extremist activities in the broadest sense. Although the wording of these norms is not directly aimed at restricting freedom of expression, they are used to suppress sensitive political content operating in the media.[4]

The use of the above methods leads to a gradual deformation of society's vision of reality. Despite the widespread availability of the media, and above all of the Internet, it is gradually being deprived of access to reliable information. The methods indicated above are not, however, crucial for the control of the media, especially the electronic media. Indeed, the challenge for the authorities has been to maintain social support and stability in the internet age, given the growing availability and popularity of this medium and a number of social revolutions observed around the world, which have been fuelled mainly by social networks. The essential hypothesis, which will be confirmed later in the article, is the claim that the traditional means used to manage the flow of information proved insufficient in the case of the Russian regime. The question that needs to be answered is what methods and techniques of information management and selection can offset the danger of social unrest and be conducive to maintaining internal stability in a situation of aggressive external policy and military campaign. The essential aim of the article is, on the one hand, to show the mechanisms of effective information management in the era of new media, and on

---

2 Worth pointing out, according to a report by the organisation Freedom House, is that Russia has a higher rate of various factors limiting press freedom than countries such as Afghanistan, India or Indonesia. See: M.J. Abramowitz, "Press Freedom's Dark Horizon", Freedom House, https://freedomhouse.org/report/freedom-press/freedom-press-2017 [accessed: 10 March 2022].

3 M. Hem, *Evading the censors: critical journalism in authoritarian states*, University of Oxford 2014, p. 5.

4 *Ibidem*.

the other hand, to outline the full range of methods, the proper application of which, in multiple ways, leads to maintaining a high level of confidence in the authority[5] and achieving internal stability despite the complicated economic and international situation in Russia. In order to achieve the above goal, it was decided to use the method of content analysis, as the record of communication[6] fixed on the Internet provides excellent analytical material in the area of top-down selection and management of information by the authorities that interests us. Particularly useful in this area will be the analysis of the discourse operating in the Internet space. As a non-reactive research method, it allows for an effective analysis of content[7] posted within the blogosphere and social networks.

Top-down information management methods and techniques by state authorities

Thanks to the multitude of ongoing empirical studies on media systems in the 20th and 21st centuries, we can draw on a rich literature that presents findings on the sources of media bias. These are not infrequently referred to as "[...] distortions that originate on the supply side of the media market."[8] In contrast to the problems presented earlier, several authors agree that private ownership of the media reduces media bias, and stress the need for competition in news markets, as concentration of ownership makes it easier for political and economic interests to dominate the media. It is also argued that government ownership of media companies is negatively correlated with a variety of public policies, including press freedom.[9]

At the outset, it is worth pointing out the basic types and methods of top-down control of the media by non-democratic governments. These, of course, do not give the full picture, as they reveal the underlying mechanisms that lead to a significant restriction of media freedom. In most modern democracies, the media industry, despite guaranteed, constitutional freedoms, is subject to a licensing system. Broadcasting licences are issued by specially appointed state bodies. However, in countries with authoritarian characteristics, concessions can be a welcome weapon in the fight against media freedom, despite legally falling within the regulations of a democratic state. For broadcasting via terrestrial transmitters, concessions are necessary for the allocation

---

5 E. Karczewski, "Destabilizacja bezpieczeństwa społecznego a problemy bezpieczeństwa wewnętrznego", *Przegląd Nauk o Obronności*, no. 3, 2017, p. 248, https://doi.org/10.5604/01.3001.0012.9856.

6 E. Babbie, *The Basics of Social Research*, 4th ed., Belmont: Thomson Wadsworth, 2008, p. 350.

7 D. Batorski, M. Olcoń-Kubicka, "Prowadzenie badań przez Internet – podstawowe zagadnienia metodologiczne", *Studia Socjologiczne*, no. 3, 2006, p. 102.

8 M. Gentzkow, J.M. Shapiro, "Competition and Truth in the Market for News", *Journal of Economic Perspectives*, vol. 22, no. 2, 2008, pp. 134.

9 S. Stier, *op. cit*, p. 1275.

of broadcasting bands to media players, which is the modern democratic norm. However, for some governments, the concession and the decision to grant it is only a means to an end of exercising control over the broadcaster. Authorities may decide not to renew a licence without indicating a reason.[10] Thus, if the media company in question is not granted a renewed licence, content creators will not know where the line between acceptable and unacceptable content is, as the authority is not obliged to communicate the reasons for refusal. Such a phenomenon inevitably leads to self-censorship.[11] Another example of the clear abuse of the institution of concessions by the authorities of non-democratic states, is Russia. Under Vladimir Putin, the right to freedom of expression is notoriously violated. The basic argumentation is that democratic authorities influence the transmission of content anyway using various types of social engineering, and that media freedom is a façade.[12] In Russia, as in most countries, newspapers, radio and television stations need licences to operate. A number of publications have had their licences revoked for, among other things, inciting religious hatred, or violating other laws, although the withdrawal of licences has largely been political.[13]

In the vast majority of countries around the world, laws are implemented to regulate the media market, as part of the state authorities' management of information. These mechanisms are applied in parallel to concessions, and are specifically referred to protection against hate speech, racist messages or attacks on religion. It is not uncommon for these to be provisions that are not specifically aimed at the media, and while they may restrict freedom of expression to some extent, they are not considered a direct tool for media control. Nevertheless, in a large number of cases, such laws can be used in just such a way. For example, Russia has implemented laws prohibiting the promotion of drugs. These laws are used to intimidate media outlets, or even close them down, when they publish material deemed sensitive. In the December 2011 edition of the Russian magazine *Esquire*, the story of opposition leader Alexei Navalny was told, with a photograph depicting him on the cover. The same issue also published a report on illegal trade on the internet, which mentioned, among other things, the sale of banned substances online. As a result, *Esquire* magazine was accused of promoting drug trafficking and received a warning from the Russian Federal Drug

---

[10] M. Majorek, S. Olczyk, M. Winiarska-Brodowska, *Cyberpolityka. Internet jako przestrzeń aktywności politycznej*, Warszawa: Texter, 2018, p. 91.

[11] W. Wijayanto, "Old Practice in a New Era: Race as the Basis of Self-Censorship in Kompas Daily Newspaper", *GSTF Journal on Media & Communications*, vol. 2, no. 2, 2015, p. 67, https://www.globalsciencejournals.com/content/pdf/10.7603%2Fs40874-014-0019-0.pdf [accessed: 3 November 2017].

[12] D. Skillen, *Freedom of Speech in Russia: Politics and Media from Gorbachev to Putin*, London – New York: Routledge, 2017, p. 321.

[13] M. Hunt, *Gorodskiye vesti*, 22 February 2006, http://blog.matthewhunt.com/2006/02/gorodskiye-vesti.html [accessed: 11 March 2022].

Control Service. Under current law, when a publishing house receives two warnings in one year, its licence can be revoked.[14]

The law is also used to blacklist websites, both domestic and foreign, effectively limiting access for Russian internet users. For those in power, the main advantage of this method is that it is not always clear whether action is being taken against the promotion of drugs or the censorship of otherwise uncomfortable content. The government may claim that political censorship has not been applied, but editors will see it as a warning against unwanted coverage of events from the political scene.[15]

A relatively simple yet practical way for authoritarian authorities to manage information is for the government to have its own media. However, this method is all too obvious, and it is not uncommon for the authorities, as part of their information management strategy, to choose to hand over the media to people close to the regime. Despite the fact that the authority is no longer directly in possession of the public media, it entrusts them into the hands of people who are significantly dependent on it. In countries with authoritarian features, this is not uncommonly becoming the norm. Dependent Russian news agencies have successfully used the idea of freedom of speech to spread disinformation in American and European media spaces. According to Timothy Snyder, an American historian, the aim of Russian propaganda is to show that the truth does not actually exist.[16] Thus, everything that is portrayed in the media is dependent on the interpretation and perspective from which an event is assessed. Modern information management initially served primarily to ensure Putin's power. Subsequently, the Kremlin, having mobilised the media in Russia and pro-Russian media abroad, significantly strengthened its influence in Ukraine's information space. At the same time, Russian propaganda began to operate in a more diversified manner towards the population, i.e. ordinary consumers of information. Pro-Russian media in Ukraine convinced citizens of the need for friendship, cooperation and strategic partnership between the two countries. In addition, the Kremlin actively using the mass media, in which for many years it was difficult to find more or less objective material about Ukraine, consciously formed among Russians an image of the indolence of the Ukrainian state and thus intensified anti-Ukrainian sentiment in Russian society.[17]

---

[14] A. Galperin, "Putting on Putin. Criticism gets creative at Russian Esquire", *Columbia Journalism Review*, March/April 2008, http://archives.cjr.org/short_takes/putting_on_putin.php [accessed: 11 March 2022].

[15] "Russian federal censor adds Snapchat to government list of instant messengers without company's knowledge", Meduza Project, 10 August 2017, https://meduza.io/en/news/2017/08/10/the-first-major-western-instant-messenger-caves-to-russian-internet-censors-it-s-snapchat [accessed: 11 March 2022].

[16] L. O'Neal, "Yale Professor Talks Russian Propaganda in Ukraine", *The Emory Wheel*, 9 February 2015, http://emorywheel.com/yale-professor-talks-russian-propaganda-in-ukraine [accessed: 14 April 2022].

[17] P. Katerynchuk, "Russian Media Policy As A Factor Of Political Destabilization In Central And Eastern European Countries", *Eurolimes*, 23 Supl, 2018, p. 187.

Top-down control and management of information on the Russian internet as part of maintaining internal stability

More or less since the turn of the century, one can observe the successive emergence and development of new forms of relatively stable regimes with authoritarian characteristics. These states are capable, to a far greater extent than the earlier, ossified authoritarianisms, of dealing with flexible borders, issues of free flow of information and other effects of increasing globalisation. These "hybrid," semi-democratic, or in other words, façade regimes tend to combine some formal democratic institutions with elements of authoritarian rule, leaving somewhat more space for some forms of free expression and free media than previous forms of closed authoritarianism allowed. These regimes are characterised by the skilful management of civil society institutions and even grassroots movements and initiatives that remain in opposition to power and its media presence.[18] They are extremely effective in managing the emergence and flow of information while accepting the lack of total control more characteristic of closed regimes. The façade of their operation is a severely limited democracy that is, in a sense, the key to participation in the global system which, to some extent, legitimises such a state externally and internally. Compared to closed authoritarianism, the new structures tend to be less systematic in their use of high-intensity coercion headed by brutal repression to maintain internal control and stability. Instead, the states in question prefer to enjoy the benefits of social engineering involving many subtle, quasi-legalistic and less obvious forms of control over society. Such measures, for example involving soft governance without resorting to traditional coercive measures, are less likely to risk global condemnation or undermine domestic support.[19]

It is interesting to note that states with highly constrained democratic mechanisms and institutions learn from each other's successes and failures, seeking to copy those policies that appear to mitigate the threat of internal instability. Numerous examples of revolutions in recent decades, such as the Arab Spring, have been recognised and analysed, and regimes with authoritarian characteristics, led by Russia, and in fear of destabilising the system, have adopted new laws and control techniques aimed at deterring and limiting the ability of activists to emulate protest movements observed in other states.[20]

It would seem that in many authoritarian states, the internet remains the last bastion of freedom of speech – and therefore represents, if not completely free, at least a freer space for the transmission of content than traditional information

[18] M. Majorek, S. Olczyk, M. Winiarska-Brodowska, *op. cit.*, p. 87.

[19] S. Levitsky, L. Way, *Competitive authoritarianism: Hybrid regimes after the Cold War*, Cambridge: Cambridge University Press, 2010, pp. 37–40.

[20] M. Majorek, S. Olczyk, M. Winiarska-Brodowska, *op. cit.*, p. 127.

providers. It can therefore be assumed that the internet is, by definition, much less restricted than is the case with traditional media, but that does not mean that it is not restricted. One has to come to terms with the fact that the total freedom of this medium is gone irretrievably. Almost since the beginning of the 21st century, countries with non-democratic features have tried to experiment with various control mechanisms directed towards new forms of communication. Already at that time, it was realised that the Internet, as yet little understood and researched, was becoming a space for arousing and intensifying social unrest. Thus, it was necessary to start implementing solutions to counteract this, although at the same time in violation of the ubiquitous and accepted position that the Internet should be a place free of state regulation. The universally accepted norms on the one hand, and the danger of internal destabilisation on the other, required the development of a multi-pronged approach to prevent potential protests. Consciously accepting the loss of some legitimacy was a necessary cost of maintaining internal stability. Initially, the management of information on the internet, categorised as the so-called first generation, was based on very coarse practices, which were basically limited to blocking sites and filtering published content by simply blocking or deleting content.[21] Then there are the more sophisticated methods, some of which were described earlier and involve legal restrictions, but these are not the most interesting in this aspect. Namely, pressure on editors of online publications, manipulation of their content, the introduction of a top-down and at the same time false message by the authorities, and relying on the growing popularity of blogs, vlogs and social channels, i.e. all the available benefits of the Web 2.0, come to the fore. What emerges, therefore, is a picture of a regime that relies on the façade institutions of democracy, i.e. it must, to some extent, be aware of the risks of internal destabilisation linked to the growing availability of new means of communication.[22] It is to be expected that any such power will seek to implement certain forms of information management on the internet, ranging from the most primitive to measures aimed at decentralising forms of interference with the message, building informal and semi-legal structures of management and control not only over content but also over users of the web.

Those wishing to disseminate messages unflattering to the authorities obviously use social media and other websites to publish material that cannot be posted in traditional media, and online newspapers are usually affected by less stringent censorship laws. However, as previously mentioned, increasingly governments in authoritarian countries are trying to restrict online content as well. One reason for this

---

21 R.J. Deibert, R. Rohozinski, "Liberation vs. Control: The Future of Cyberspace", *Journal of Democracy* vol. 21, no. 4, 2010, pp. 43–57.

22 J.A. Kerr, "Information, Security, and Authoritarian Stability: Internet Policy Diffusion and Coordination in the Former Soviet Region", *International Journal of Communication*, vol. 12, 2018, p. 3818.

is that online media are becoming more popular and online content is becoming a greater threat to the authorities. With internet surveillance and landing page blocking tools readily available, the authorities have more and more opportunities to control content and limit its dissemination.[23] Some signs of this, are easy to observe. For example, as already mentioned, the Russian authorities are in the habit of blacklisting websites containing sensitive content and, moreover, have introduced a law that requires bloggers to certify the factual accuracy of information on their blogs.[24]

The Russian model of media information management in the face of the conflict in Ukraine

An excellent illustration for the top-down management of information by the authorities is the indirect pressure exerted by the Russian authorities against the local, popular online newspaper *Lenta.ru*. It was known for its independent, reliable publications and was one of the most popular online resources in Russia. *Lenta* decided in March 2014 to publish a report on Ukraine, covering the current situation of the country including the Russian invasion of Crimea. Shortly after the aforementioned publication, the owner of the portal, Alexander Mamut, made a change in the position of editor-in-chief and, as an act of solidarity, a number of leading journalists resigned. Publicists working at the portal believe that this change was politically motivated and that the new chief executive no longer allows journalists as much freedom.[25]

It is worth noting at this point that the Russian model of information management is based on a two-faceted concept. In the first place, therefore, we have a total power-controlled media, in which the message is top-down imposed and the information provided has nothing to do with reliable journalism. And this branch is dominant in this state. Within the second area, let's call it the freedom area, there is a kind of safety valve, i.e. a certain amount of heavily marginalised media, which generate a more objective message. The media with the greatest reach, are ruthlessly controlled, while the less important ones have a degree of freedom to generate the message themselves. We should see this as a politically controlled process,

[23] M. Nekrasov, L. Parks, E. Belding, Limits to internet freedoms: Being heard in an increasingly authoritarian world, [in:] *Proceedings of the 2017 Workshop on Computing Within Limits (LIMITS '17)*, Assosiation for Computing Machinery: New York, 2017, pp. 120–122.

[24] N. Maréchal, "Networked authoritarianism and the geopolitics of information: Understanding Russian Internet policy", *Media and Communication*, vol. 5, no. 1, 2017, p. 32, https://doi.org/10.17645/mac.v5i1.808.

[25] M. Bodner, "Lenta.ru Editor Replaced After 'Extremism' Warning", *The Moscow Times*, 12 March 2014.

where members of the regime decide the fate of a huge number of media by assigning them to area one or area two, and then promoting and at the same time degrading them according to their impact on public opinion. In this type of situation, the authorities manage the media by assigning them different roles, on the one hand to the state-controlled media and on the other to the independent ones. While the role of the former is to present the news in a way that legitimises further authoritarian rule, the latter are used by the regime to demonstrate that its rule is in fact not as repressive as its critics claim.[26] The underlying assumption of power is therefore to guarantee just enough space for independent media activities to sustain the desired image of political freedom and respect for the rule of law without compromising its influence. Such a pattern could be seen, for example, during the invasion of Crimea, where the state-controlled media uncritically applauded the actions of the Russian regime, including those of the "green men,"[27] while less influential, previously marginalised outlets were allowed to post more critical comments.

It follows from the above that, until some time ago, the internet remained in the realm of the less influential media, as numerous surveys indicated that the vast majority of Russians obtain their knowledge of events in Ukraine from media controlled by the authorities, namely state television channels. However, fearing that reliable information would not reach wider social groups and cause social unrest, the Russian authorities have taken steps to block public access to a large number of IP addresses on the pretext of fighting extremism and to put pressure on operators of social networking sites, such as Vkontakte, to close down anti-regime forums. The internet is increasingly seen as a destructive sphere that allows citizens to bypass state-controlled information providers. To further control the internet, the Russian National Guard, created to maintain internal security,[28] announced the creation of a new cyber-division dedicated to monitoring social media to identify "extremist" messages. The creation of this cell has been justified by an increase in the number of messages of a forbidden nature nevertheless this increase is due more to the increasingly broad definition of "extremism" used by the Russian authorities.[29]

---

[26] J.A. Dunn, "*Lottizzazione* Russian Style: Russia's Two-tier Media System", *Europe-Asia Studies*, vol. 66, no. 9, 2014, p. 1435, http://dx.doi.org/10.1080/09668136.2014.956441.

[27] M. Pokrzywińska, "'Zielone ludziki' w polityce zagranicznej Federacji Rosyjskiej w drugiej dekadzie XXI wieku", *Acta Politica Polonica*, no. 2, 2019, p. 48, https://doi.org/10.18276/ap.2019.48-04.

[28] N. Kusa, "Gwardia Narodowa Federacji Rosyjskiej jako element systemu bezpieczeństwa wewnętrznego Rosji", *Środkowoeuropejskie Studia Polityczne*, no. 1, 2017, pp. 156–158, https://doi.org/10.14746/ssp.2017.1.9.

[29] S. Sukhankin, "Russian National Guard: A New Oprichnina, 'Cyber Police' or Something Else?", The Jamestown Foundation, 21 March 2017, https://jamestown.org/program/russian-national-guard-new-oprichnina-cyber-police-something-else-2 [accessed: 18 March 2022].

The Russian blogosphere and social networks as a space for disinformation

Nowadays, it appears that social networks, personal blogs or news platforms claiming to be independent serve as a tool for manipulating the population by creating a public opinion favourable to the ruling political class. There is a group of individuals who, in exchange for financial remuneration, are prepared to spread through comments or posts favourable to the doings of their employer, which are often the ruling politicians. These types of people are called trolls, and their main task is to improve the image of power in cyberspace in order to hide or discredit those sources of information that reveal the true activities of those in power. Members of the so-called "army of trolls" operating for political purposes are a common phenomenon in Russia and beyond. A "troll cell" was recently discovered in Finland, and the Finnish authorities suspect that the source of funding is the Russian embassy in Helsinki. Putin has been using a host of trolls in his information war against Ukraine, following the annexation of Crimea and during conflicts with his eastern neighbours.[30] Trolling consisted of creating multiple blogs and fake accounts on major social networks (Vkontakte, Facebook, Twitter, etc.) and spreading pro-Kremlin messages. The strategy was to create a mix of news that would be difficult when trying to manipulate public opinion. This can be achieved by creating a flow of information through both non-political posts (such as fashion news or recipes) and political comments that are strictly created by editors and shared by trolls. One should therefore maintain a regular themed blog or fanpage, and occasionally weave in a political post about the fascism of the government in Kiev. The effect of these posts is achieved when readers of the blog and comments accept the posts, and subsequently click on likes and share this content further.

The reality is that we are dealing with hundreds of state-employed commentators on social and political life, whose main purpose is to negate posts unfavourable to the authorities and to slander the authorities. This is by no means done ostentatiously; years of cyber information warfare have perfected Russia's troll industry. The simple deletion of comments unfavourable to the authorities is in fact no longer necessary, because the trolls generate so much content that the designated comments are lost in a sea of support for the government. In the so-called content factory, we have people writing on a variety of topics and operating a variety of forums and blogs. At the end of 2016, the greatest emphasis was on creating sections dealing with Ukraine, where content undermining both Ukrainian statehood and the nation dominated,

[30] A. Eşanu, "Centrul de Telecomunicatii Speciale al R. Moldova l-a votat pe Plahotniuc primministru. Lista postacilor de partid", *Ziarul de Gardă*, 19 December 2015, https://www.zdg.md/stiri/centrul-de-telecomunicatii-speciale-al-r-moldova-l-a-votat-pe-plahotniuc-prim-ministru-lista-postacilor-de-partid [accessed: 25 April 2022].

successively discrediting the independent country. Separate sections, considered to be among the most prestigious, were dedicated to the US elections and foreign policy in general, where hired individuals pretended to be commentators from outside Russia, writing posts in English.[31] In this way, the reach of Russian trolls was wide and, over time, they gained more and more influence on the beliefs and worldview of internet users from all over the world. Such a wide and global influence would not have been possible without a perfectly contracted disinformation machine, built and perfected over the years.

The disinformation and manipulation of facts in this case takes place through a "snowball" effect, meaning that a given comment, seemingly harmless, is increasingly distributed to observers and friends on social networks. The whole process takes place naturally and the numerous shares lead to a strong embedding in the social media space and thus its credibility. It is worth mentioning that the work of these bloggers was and is illegal, as they were and are all unofficially employed and only receive their emoluments in cash. Thus, it is possible to qualify the activity of trolls as a clandestine activity born of initiatives designed and managed by specific state structures in order to build a distorted image of an alternative reality to achieve relative social stability.

In light of recent events in Ukraine, Russia has blocked the use of most social media on its territory. This included Facebook, Twitter and Instagram.[32] Of course, this blockade only affects less knowledgeable users, as the sites can still be used with an active VPN service. The attempt to cut the public off from the world's social networking resources is an act of desperation on the part of the Russian authorities, who, in the face of international ostracism, do not want to allow their citizens' perceptions to change at any cost. Among the biggest players, YouTube still remains, with a partial blockade of some functionalities. On the one hand, it is a window to the world for Russians, while on the other it is still a powerful propaganda tool in the hands of the Kremlin. From this, however, it follows that a simple cut-off from social networks at this stage makes little difference, as the successive work of creating an alternative reality by the authorities in the social media space has caused deep and perhaps irreversible social damage.

Conclusions

According to the above analyses, what emerges is a picture of a total degeneration of the role of the media, which, as a rule, in democratic systems are supposed to serve citizens, not the authorities. The news coverage here is so one-sided that, in

[31] F. Splidsboel Hansen, *Russian hybrid warfare: A study of disinformation*, Copenhagen: Danish Institute for International Studies, 2017, p. 22.

[32] K. Rutkowska, "Czy Rosja zabije YouTube?", Benchmark.co.uk, 19 March 2022, https://www.benchmark.pl/aktualnosci/youtube-rosja.html [accessed: 17 April 2022].

principle, it should be disqualified in terms of reliability. Most devastatingly, it does not necessarily contain untruths, but is truncated of relevant facts in such a way that it ultimately leaves the viewer with a certain mixture of emotions which, when juxtaposed with political preferences projected over the years, is itself a tool in the hand of power.

It is not uncommon for the regime-controlled media to ignore relevant facts, erasing them, as it were, from reality. Something that is unspoken does not exist, so in the minds of the vast majority of Russian citizens, if there is no talk of war, only of a special operation, it means there is no war. From this it follows that it is not always telling untruths that is harmful, it is just as destructive to be vague, or to omit important issues in silence. Nonetheless, this type of information management leads to the desired effect of sustained support for power. However, the most imaginative and effective method is disinformation. Disinformation understood as the spreading of false or fabricated information, or the distortion of facts through role reversal. The use of social media and the internet in general to spread this type of false information leads to a widespread belief in the veracity of the message, which has been reinforced by hundreds of shares and likes. This is by far the most powerful tool in the hands of the Russian authorities and it has contributed and will continue to contribute to the relative internal stability of the state, despite the deteriorating living conditions of the population and the international isolation of the country and its citizens.

References

Abramowitz M.J., "Press Freedom's Dark Horizon", Freedom House, https://freedomhouse.org/report/freedom-press/2017/press-freedoms-dark-horizon [accessed: 10 March 2022].

Babbie E., *The Basics of Social Research*, 4th ed., Belmont: Thomson Wadsworth, 2008.

Batorski D., Olcoń-Kubicka M., "Prowadzenie badań przez Internet – podstawowe zagadnienia metodologiczne", *Studia Socjologiczne*, no. 3, 2006, pp. 99–132.

Bodner M., "Lenta.ru Editor Replaced After ‚Extremism' Warning", *The Moscow Times*, 12 March 2014.

Deibert R.J., Rohozinski R., "Liberation vs. Control: The Future of Cyberspace", *Journal of Democracy*, vol. 21, no. 4, 2010, pp. 43–57.

Dunn J.A., "*Lottizzazione* Russian Style: Russia's Two-tier Media System", *Europe-Asia Studies*, vol. 66, no. 9, 2014, pp. 1425–1451, http://dx.doi.org/10.1080/09668136.2014.956441.

Eşanu A., "Centrul de Telecomunicatii Speciale al R. Moldova l-a votat pe Plahotniuc primministru. Lista postacilor de partid", *Ziarul de Gardă*, 19 December 2015, https://www.zdg.md/stiri/centrul-de-telecomunicatii-speciale-al-r-moldova-l-a-votat-pe-plahotniuc-prim-ministru-lista-postacilor-de-partid [accessed: 25 April 2022].

Galperin A., "Putting on Putin. Criticism gets creative at Russian Esquire", *Columbia Journalism Review*, March/April 2008, http://archives.cjr.org/short_takes/putting_on_putin.php [accessed: 11 March 2022].

Gentzkow M., Shapiro J.M., "Competition and Truth in the Market for News", *Journal of Economic Perspectives*, vol. 22, no. 2, 2008, pp. 133–154.

Hem M., *Evading the censors: Critical journalism in authoritarian states*, University of Oxford, 2014.

Hunt M., *Gorodskiye vesti*, 22 February 2006, http://blog.matthewhunt.com/2006/02/gorodskiye-vesti.html [accessed: 11 March 2022].

Karczewski E., "Destabilizacja bezpieczeństwa społecznego a problemy bezpieczeństwa wewnętrznego", *Przegląd Nauk o Obronności*, no. 3, 2017, pp. 247–255, https://doi.org/10.5604/01.3001.0012.9856.

Kateryнchuk P., "Russian Media Policy As A Factor Of Political Destabilization In Central And Eastern European Countries", *Eurolimes*, 23 Supl, 2018, pp. 185–198.

Kerr J.A., "Information, Security, and Authoritarian Stability: Internet Policy Diffusion and Coordination in the Former Soviet Region", *International Journal of Communication*, vol. 12, 2018, pp. 3814–3834.

Kusa N., "Gwardia Narodowa Federacji Rosyjskiej jako element systemu bezpieczeństwa wewnętrznego Rosji", *Środkowoeuropejskie Studia Polityczne*, no. 1, 2017, pp. 155–170, https://doi.org/10.14746/ssp.2017.1.9.

Levitsky S., Way L., *Competitive authoritarianism: Hybrid regimes after the Cold War*, Cambridge: Cambridge University Press, 2010.

Majorek M., Olczyk S., Winiarska-Brodowska M., *Cyberpolityka. Internet jako przestrzeń aktywności politycznej*, Warszawa: Texter, 2018.

Maréchal N., "Networked authoritarianism and the geopolitics of information: Understanding Russian Internet policy", *Media and Communication*, vol. 5, no. 1, 2017, pp. 29–41, https://doi.org/10.17645/mac.v5i1.808.

Nekrasov M., Parks L., Belding E., Limits to internet freedoms: Being heard in an increasingly authoritarian world, [in:] *Proceedings of the 2017 Workshop on Computing Within Limits (LIMITS '17)*, Assosiation for Computing Machinery: New York, 2017, pp. 120–122.

O'Neal L., "Yale Professor Talks Russian Propaganda in Ukraine", *The Emory Wheel*, 9 February 2015, http://emorywheel.com/yale-professor-talks-russian-propaganda-in-ukraine [accessed: 14 April 2022].

Pokrzywińska M., "'Zielone ludziki' w polityce zagranicznej Federacji Rosyjskiej w drugiej dekadzie XXI wieku", *Acta Politica Polonica*, no. 2, 2019, pp. 45–53, https://doi.org/10.18276/ap.2019.48-04.

"Russian federal censor adds Snapchat to government list of instant messengers without company's knowledge", Meduza Project, 10 August 2017, https://meduza.io/en/news/2017/08/10/the-first-major-western-instant-messenger-caves-to-russian-internet-censors-it-s-snapchat [accessed: 11 March 2022].

Rutkowska K., "Czy Rosja zabije YouTube?", Benchmark.pl, 19 March 2022, https://www.benchmark.pl/aktualnosci/youtube-rosja.html [accessed: 17 April 2022].

Skillen D., *Freedom of Speech in Russia: Politics and Media from Gorbachev to Putin*, London – New York: Routledge, 2017.

Splidsboel Hansen F., *Russian hybrid warfare: A study of disinformation*, Copenhagen: Danish Institute for International Studies, 2017.

Stier S., "Democracy, Autocracy and the News: The Impact of Regime Type on Media Freedom", *Democratization*, vol. 22, issue 7, 2015, pp. 1273–1295, https://doi.org/10.1080/13510347.2014.964643.

Sukhankin S., "Russian National Guard: A New Oprichnina, 'Cyber Police' or Something Else?" The Jamestown Foundation, 21 March 2017, https://jamestown.org/program/russian-national-guard-new-oprichnina-cyber-police-something-else-2 [accessed: 18 March 2022].

Wijayanto W., "Old Practice in a New Era: Rasa as the Basis of Self-Censorship in Kompas Daily Newspaper", *GSTF Journal on Media & Communications*, vol. 2, no. 2, 2015, pp. 66–74, https://www.globalsciencejournals.com/content/pdf/10.7603%2Fs40874-014-0019-0.pdf [accessed: 3 November 2017].

Top-down selection of information as an element of strategic information management in the event of a threat of internal destabilisation

Abstract

In many authoritarian countries, the Internet is an oasis of freedom of speech and the free transfer of knowledge – thus, if not completely free, then at least a more free space for transferring content than traditional information providers. Nevertheless, the total freedom of this medium has passed irretrievably. Use of social media and other websites to post material that cannot be posted on traditional media, and even online newspapers tend to be affected by less stringent censorship laws. However, this does not change the fact that contemporary authoritarian regimes are going so far as to interfere with social media, either by blocking access to content or by promoting false information. The conducted analysis is to show the mechanisms of top-down information management in order to lead to widespread disinformation and distortion of reality. In this respect, it is worth bringing up the actions of the Russian authorities in the context of the conflict in Ukraine and the possible opposition of the Russian society to the ongoing military operations.

Key words: information management, destabilisation, media, Russia, Ukraine

Varia

BEZPIECZEŃSTWO TEORIA I PRAKTYKA
SECURITY THEORY AND PRACTICE
e-ISSN 2451-0718
ISSN 1899-6264
2022
No. 2 (XLVII)
DOI: 10.48269/2451-0718-btip-2022-2-010

Krzysztof Waśniewski
PhD, Andrzej Frycz Modrzewski Krakow University
https://orcid.org/0000-0003-0076-4804

Anna Bałamut
PhD, Andrzej Frycz Modrzewski Krakow University
https://orcid.org/0000-0001-7300-7367

Transformation of the energy sector, environmental factors and national security in Poland: highlights from the Krynica Forum '22, Krynica-Zdrój, 19–21 October 2022

This paper selectively discusses the content of two conference panels held at the "Krynica Forum '22 – Growth and reconstruction" conference, which took place in Krynica Górska, Poland, from 19 until 21 October 2022.

The aim of the Krynica Forum was to work collectively on solutions for strengthening security, prosperity, social cohesion and the economic position of Poland and the countries of Central and Eastern Europe. Discussions were grouped into panels, which followed five thematic paths: "Security and geopolitics", "Change economy", "Energy and climate", "Future society" and "Health trends". The panel meetings gathered political leaders at many levels of government, business people, scientists and the media. The Kościuszko Institute was the host of the event, with Nowa Konfederacja as exclusive partner, and the local government of the Małopolskie Voivodeship as the titular partner. The conference received the support of other institutions and business entities, such as: Orlen S.A. as strategic partner, PGNiG

S.A., Małopolska Development Fund, Małopolska Regional Development Agency and Kraków Technology Park.

The two panels being discussed were held on 20 October 2022, and were both focused on the national security of Poland in the context of technological change in the energy sector.

A brief outline of the scientific background seems useful before highlighting the content of the discussion panels. Poland is currently facing a contradiction in the national energy strategy: the need to comply with climate-friendly policies of the European Union has to be balanced against the imperative of energy security, with hard coal and lignite remaining the main sources of energy.[1] Even before the war in Ukraine, there was substantial evidence for the imperative of maintaining that difficult balance. Transition from coal to natural gas, thus to a cleaner fossil fuel, would significantly increase the hidden energy poverty in Polish households, as the providers of energy would transfer onto final users the amortisation of the corresponding investment in new assets.[2] The dependence of Poland on imported crude oil has been significant for decades and therefore has created a crucial threat to national security.[3] That dependence has been extending beyond just crude oil, into 42 key, 24 strategic and 17 critical minerals indispensable for the Polish economy.[4] Some research suggested that speeding up the transition to new technologies in the energy sector could improve the overall energy security of Poland.[5]

Strategies for technological change in the energy sector differ greatly among the member countries of the European Union. Geography, both physical and economic, seems to be the prime factor of those idiosyncrasies. In the case of Poland, assuring proper energy security is the key factor of success in effectively transforming the energy sector, whilst environmental and social factors are somehow instrumental.[6]

---

1 B. Igliński, M.B. Pietrzak, U. Kiełkowska *et al.*, 'The assessment of renewable energy in Poland on the background of the world renewable energy sector', *Energy*, vol. 261, 2022, 125319, https://doi.org/10.1016/j.energy.2022.125319.

2 L. Karpinska, S. Śmiech, 'Will energy transition in Poland increase the extent and depth of energy poverty?', *Journal of Cleaner Production*, vol. 328, 2021, 129480, https://doi.org/10.1016/j.jclepro.2021.129480.

3 J. Kamyk, A. Kot-Niewiadomska, K. Galos, 'The criticality of crude oil for energy security: A case of Poland', *Energy*, 220, 2021, 119707, https://doi.org/10.1016/j.energy.2020.119707.

4 K. Galos, K., E. Lewicka, A. Burkowicz *et al.*, 'Approach to identification and classification of the key, strategic and critical minerals important for the mineral security of Poland', *Resources Policy*, vol. 70, 2021, 101900, https://doi.org/10.1016/j.resourpol.2020.101900.

5 A. Aminpour, 'Energy security in Poland: Where the energy sector falls short and where it can go', *Georgetown Scientific Research Journal*, vol. 2, no. 1, 2022, pp. 7–13, https://doi.org/10.48091/gsr.v2i1.26.

6 R. Wisniewski, P. Daniluk, A. Nowakowska-Krystman, *et al.*, 'Critical success factors of the energy sector security strategy: The case of Poland', *Energies*, vol. 15, no. 17, 2022, 6270, https://doi.org/10.3390/en15176270.

Energy-related policies in Poland seem to be rooted in the imperative of national energy security rather than going towards quick transformation of the energy sector.[7] A series of mergers and acquisitions in the Polish energy sector seem to have been triggered as an institutional response at the level of business structures after the beginning of the war in Ukraine.[8]

The first of the two discussion panels summarised in this paper was titled "The resilience of Poland to the outcomes of Russian aggression in Ukraine – conclusions for the energy sector", and gathered three participants: Paweł Szczeszek (the CEO of TAURON Polska Energia), Robert Kuraszkiewicz (entrepreneur, columnist, former CEO of Bank Pocztowy) and Anna Bałamut, PhD (Assistant Professor at Andrzej Frycz Modrzewski Krakow University). The first issue discussed in that panel revolved around the thus far predominance of cheap natural gas from Russia as the core of technological change in the energy sector. That model has failed. How deep is the dependency of European countries on Russian gas? How was Poland prepared to face the present energy crisis? What is the connection between low-carbon economy and resilience to Russian energy blackmail?

In response to that line of discussion, Anna Bałamut stated that the progressive winding down of coal mining in Poland was short-sighted and obviously assumed the best-case scenario, without turbulence. We have been too slow at transitioning to distributed, renewable energy resources. Mr Paweł Szczeszek developed his commentary starting from the fact that successive Polish governments have been implementing climate-related agreements with a priority on energy security, when the cutting of emissions is maximised within the limits of proper energy security.

However, in the specific case of Poland, 1990 being taken as base year in climate-related agreements is a big problem. In 1990, the Polish economy was in deep recession after the transition from communism to market economy. The year 1990 is simply not representative of anything like a baseline state in the Polish industry. In a further development, Paweł Szczeszek asserted that climate-related agreements need to be specific and pragmatic to be implementable. Programmes such as "Fit for 55" in the EU are too general in that respect. As regards the current energy crisis, Paweł Szczeszek insisted that in 2022, those who had been importing cheap coal from Russia before the war in Ukraine have lost all their thus far accumulated gains. In that context, it is worth noting that for the last seven years, Polish state-owned companies have been buying coal from domestic mines, not from Russia.

---

7 K. Rabiej-Sienicka, T.J. Rudek, A. Wagner, '*Let it Flow*, *Our Energy* or *Bright Future*: Socio-technical imaginaries of energy transition in Poland', *Energy Research & Social Science*, vol. 89, 2022, 102568, https://doi.org/10.1016/j.erss.2022.102568.

8 J. Toborek-Mazur, K. Partacz, M. Surówka, 'Energy security as a premise for mergers and acquisitions on the example of the multi-energy concern PKN Orlen in the face of the challenges of the 2020s', *Energies*, vol. 15, no. 14, 5112, https://doi.org/10.3390/en15145112.

As regards renewable sources and their relative importance, Paweł Szczeszek argued that investment in the distribution and storage of energy is crucial for the practical utility of the renewable energy sources, probably even more important than investment in the generation capacity based on those sources. In photovoltaics, we need to be realistic. The nominally provided peak capacity in photovoltaic installations are not realistic. When synchronising photovoltaic installations with the power grid, it is more realistic to plan for average capacity or even for the minimum one.

For his part, Robert Kuraszkiewicz contended that the war in Ukraine was virtually impossible to predict a few years ago, and thus it was impossible to take that war into account in long-term energy policies. Independently from both the war and the drive towards low carbon emissions, a dual technological revolution is going on, namely that which is digital-electricity related. The global economy progressively focuses on electricity as the directly useful form of energy, to the expense of heat or natural gas. The war in Ukraine has demonstrated how dependent Poland is on Russian coal. Compared to other European countries, Poland derives an exceptionally large proportion of its thermal energy from coal. From Robert Kuraszkiewicz's perspective, Europe needs to develop sources of energy other than fossil fuels simply because we do not have sufficient domestic reserves of fossil fuels. Renewable sources of energy are one possible option in that respect. The intermittence of their power supply is an attribute, not a drawback. We simply need to adapt to that attribute. In the context of technological change, Robert Kuraszkiewicz remarked that Poland is lagging behind significantly as regards the technology of power distribution and storage.

That first issue discussed in the panel opened on the question: what kind of stable, non-intermittent source of energy, other than fossil fuels, is best for Poland from the perspective of near future? In that thread, the dominant voice seems to have been that of Paweł Szczeszek. He claimed that two strands of investment are of capital importance in the Polish energy sector: renewables and nuclear. We should keep investing in renewable sources of energy. It is important to develop small modular reactors (SMR) based on nuclear energy. TAURON, together with KGHM Polska Miedź S.A., is initiating such a project. For now, the technology of SMR is too expensive for industrial use. On the other hand, supplies in nuclear fuel are a strategic issue if we want to invest in SMR. However, with that long perspective in mind, Poland still heavily relies on local systems of central heating, attached to local thermal power plants, and, therefore, we still need coal.

The second energy-related panel held on the same day, 20 October 2022, was titled "Transformation of the energy sector and national security", hosting Krzysztof Wojczal (lawyer, geopolitical analyst, columnist), Karol Wolff (Head of Strategy and Strategic Projects at PKN Orlen S.A.), and Arkadiusz Sekściński (Deputy CEO of PGNiG S.A., in charge of development projects). The discussion started

around the question of how technological change in the energy sector can help the national security of Poland. This thread of debate seems to have been dominated by Krzysztof Wojczal, who warned that deficits in the supply of natural gas will make Germany consume and import a lot of electricity. Poland will have to compete against Germany as a buyer in the market of electricity. The Baltic Pipe project, i.e., natural gas from Norway, is an improvement as regards the energy security of Poland, and yet it is another case of an imported energy source, as well as another piece of critical infrastructure, exposed to attacks. We should develop our own, domestic sources of energy in Poland, independent of imports. Furthermore, we should invest in our capacity to export energy. Taking on the issue of energy security from another angle, Krzysztof Wojczal propounded that Poland needs to develop better connections between the domestic power grid and those in other countries. That will improve both our capacity to export energy and to import it. Poland should actively build influence in Ukraine, also in the perspective of energy security.

The second thread developed in that panel revolved around the possible ways of speeding up technological change in the Polish energy sector, with a particular focus on accelerating the implementation of nuclear. Karol Wolff claimed that we need to combine an efficient response to a dual challenge. We need a generation-long transformation in our energy sources, and a much more immediate transformation towards greater energy security. A combination of renewables and nuclear seems to be the right response to that dual challenge. Both assure low carbon emissions and independence in energy supply. Small modular reactors (SMR) will find their first practical applications in the powering of industrial plants, as they can supply both electricity and industrial heat. There is a chance to have such first applications in Poland by 2030. Orlen S.A. has created an affiliated company oriented towards both renewables and SMR.

Further discussion in the panel focused on the role of renewable energy sources (RES) in transforming the energy sector in Poland, with the provocative question: why do we have such a small share of RES in the Polish energy mix? Karol Sekściński argued that transition towards renewables is ongoing in Poland: Orlen S.A. is developing offshore windfarms in a PLN 140 billion project. Still, new drillings for natural gas are being developed into exploitation in Poland. Further in his statement, Karol Sekściński asserted that local communities need to be consulted regarding investment in the energy sector, and this is just one step. Projects in the energy sector require extensive preparation, inclusive of realistic business plans. That facilitates effective implementation, which, incidentally, is just as important as setting strategic goals. Drifting slightly onto another topic, Karol Sekściński pointed out the importance of developing biogas installations. We have too little capacity in that field in comparison with the amount of biogas we generate.

The discussion reported in this paper seems to show an underlying common thread as regards energy security, namely the importance of diversity in the sources of energy. Combining a core power infrastructure based on non-intermittent sources with a broader network of distributed energy resources (e.g. solar, wind, biogas) seems to be the best solution. At the core, progressive transition from fossil fuels towards nuclear appears as the soundest strategy.

Reports

BEZPIECZEŃSTWO TEORIA I PRAKTYKA
SECURITY THEORY AND PRACTICE
e-ISSN 2451-0718
ISSN 1899-6264
2022
No. 2 (XLVII)
DOI: 10.48269/2451-0718-btip-2022-2-011

Adam Jabłoński

Associate Professor PhD, President of the Board of the Southern Railway Cluster

Marek Jabłoński

Associate Professor PhD, Vice President of the Board of the Southern Railway Cluster

Dirk-Ulrich Krüger

President of ERCI – European Railway Clusters Initiative ASBL

Veronica Elena Bocci

Vice President of ERCI – European Railway Clusters Initiative ASBL

Report on the Workshop of the European Network of Railway Clusters ERCI from the perspective of safety in EU rail traffic, Marina di Carrara, Tuscany, 20–22 June 2022 Workshop topic: Strengthening European value chains for industrial companies

With dozens of railway companies from all over Europe, several hundred participants from various enterprises and only one railway cluster from Poland – in Marina di Carrara, Carrara, in Tuscany, the first meeting of the joint task forces "Cybersecurity on railways" and "Multimodal logistics" operating within the European Railway Clusters Initiative (ERCI) took place.

The ERCI is a leading meta-cluster of the railway industry in Europe, bringing together 16 innovative clusters from 17 European countries (Italy, Poland, France, Great Britain, Spain, Turkey, Denmark, Belgium, Sweden, Croatia, Slovenia, Serbia, Bosnia and Herzegovina, Montenegro, North Macedonia, Austria, Germany). Together, it combines the ideas and interests of over 2,000 small and medium-sized companies in the industry.

Among the founding members of the ERCI, apart from the clusters from Germany, France and Italy, there is one Polish cluster – OTTIMA plus Ltd. / Southern Railway Cluster. The meeting on behalf of the Polish cluster was attended by Associate Professor PhD Adam Jabłoński (President of the Management Board) and Associate Professor PhD Marek Jabłoński (Vice President of the Management Board).

The meeting in Tuscany was combined with a workshop under the slogan: "The Blockchain Made Easy for SMEs and European Value Chains".

Blockchain is an innovative database concept that is not stored on a central server but is a network of equivalent replicas. Each of them may be owned by all interested system participants.

The meeting created access to the knowledge and technology transfer of European partners in the railway industry, which was a breakthrough in the constantly developing railway market in Europe. This is the first event of its kind to address a "very hot" topic in recent times: Blockchain technology, which is an extremely important driver of innovation. Companies from various parts of Europe talked about how the use of blockchain technology looks in practice.

Blockchain as a key technology for the European railway sector

As noted during the workshop in Italy – Blockchain is and will be a key technology for the railway sector as it introduces a new approach to data-based processes. This unlocks a very wide and varied application potential, with benefits in terms of performance, safety, security, sustainability and railroad operations.

It therefore becomes fundamental to fully understand the technology that can implement benefits for any organisation. For this purpose, during the three-day workshop, more than 20 speeches by representatives from clusters and railway companies from all over Europe were given.

The event was opened by the ERCI Management Board – Veronica Elena Bocci (DITECFER, Italy) and Dirk-Ulrich Krüger (Rail S., Germany), who, after a short introduction, announced the first speaker, Giorgio Pizzi (Ministry of Sustainable Infrastructure and Transport / ENISA TRANSSEC – Italy). During his speech, "Cybersecurity in Railways: What has been achieved? What remains to be done?" he emphasised in particular that rail networks are part of public transport systems, which

are in turn a complex and closely interconnected network. Giorgio Pizzi noted that such a configuration could give an attacker the opportunity to launch a coordinated attack, undermining the stability of society and the economy. The consequences of these attacks on such critical infrastructures can spread from one system to another, causing disruption.

Presentation by Prof. Filippo Zatti (University of Florence) turned out to be extremely interesting – the author presented blockchain technology as a kind of open, distributed digital ledger that can efficiently and quickly record transactions between parties. Blockchain technology is based on a common IT platform focused on distributed data storage using an algorithm. Encrypted data ensures transmission security and limited access for third parties.

The following topics were discussed in subsequent speeches:

- "Railway freight and multimodal logistics: How to tackle gaps from a value chain perspective – Ignasi Gómez-Belinchón (In-Move by Railgrup – Spain), Aristarco Tomás (Tenalach Consulting – Spain),
- "Building EU leadership in blockchain technology: The European Commission's blockchain strategy – Q&A" – Pierre Marro (European Commission – DG CNECT – Belgium),
- "Discovering blockchain technology: the fundamentals – Q&A", Prof. Filippo Zatti (University of Florence – BABEL – Italy),
- "Blockchain-enabled virtual coupling of automatic train operation" – M. Ganesan (Alstom – India),
- "Digital automatic coupling of rolling stock in a freight train and the enabling role of blockchain" – Francesco Lucisano (Co.El.Da. Software – Italy), Guido Ancarani (DITECFER – Italy),
- "Exchange of information in TEN-T Logistics Corridors: I Rail Project and eFTI platforms perspectives" – Marco Mattiocco (Excise, Customs and Monopoles Agency – Italy),
- "Blockchain-enabled ports: the experience of the "PLANET" H2020 project and blockchain interoperability" – Harris Niavis (Inlecom – Belgium), Claudio Salvadori (NGS – New Generation Sensors – Italy),
- "What skills for blockchain: the "CHAISE" blueprint alliance of the EU and training available" – Pietro Azzara (Italia 4 Blockchain – Italy),
- "The STARS blockchain network: How we got here and what our goals are" – Conversation between Veronica Elena Bocci (DITECFER / STARS project – Italy) and Fabio Gatti (Apuana SB / STARS project – Italy).

The first day of the workshop ended with "roundtable" talks on open points about blockchain usage and key lessons. The interviews were attended by: Giorgio Pizzi, Luigi Rucher, Pietro Azzara, Federica Montaresi, Thomas Ostertag and Fabio Gatti. Veronica Elena Bocci was the moderator of the conversation.

The second day of the workshop was mainly focused on the search for new blockchain use cases in railway and multimodal logistics. Veronica Elena Bocci made presentations from stakeholders on blockchain use cases in their organisations.

Nicola Gramegna (EnginSoft – Italy) and Martin Holland (Prostep – Germany) presented ways to gain the potential of blockchain technology integration. Annabelle Sion (Polymeris – France) and Maximin Mair (DeconX – Italy) answered questions about the use of blockchain technology to track materials used in production processes, supporting sustainable development.

During the speech entitled "Blockchain for condition monitoring", John Euston (University of Birmingham – UK) emphasised that remote condition monitoring (RCM) technologies benefit the rail industry by improving its availability, safety and asset reliability. The RCM system enables the detection and diagnosis of failures in damaged assets, preventive maintenance, and the avoidance of breakdowns, costly breakdowns and delays.

In the following speeches, the participants of the meeting from Italy and Spain made their presentations.

- "Blockchain for traceability in logistics – Q&A" – Marcos Icardó (Usyncro – Spain),
- "Untapped potentials from integrating technologies: Blockchain and IoT – DEMO – Q&A" – Leonardo Fabbri (Elfi Electronics – Italy),
- "Untapped potentials from integrating technologies: Blockchain and artificial intelligence; blockchain and digital twin; overview of more possible use cases; funding opportunities – Q&A" – Veronica Elena Bocci, Guido Ancarani (DITECFER – Italy).

Veronica Elena Bocci and Guido Ancarani (DITECFER – Italy) presented how to use the potential of integrated technologies: Blockchain and artificial intelligence. Most possible use cases and funding opportunities have been reviewed.

The next part of the workshop was about practical work with blockchain technology. Fabio Gatti (Apuana SB – Italy) demonstrated how to register a transaction on the STARS blockchain network. Participants representing railway companies and clusters from all over Europe were divided into international groups of several people and together they performed exercises aimed at, among other things, identification of the use cases for blockchain technology and key data, and the benefits resulting from them.

Blockchain is one of the fastest growing technologies. The meeting of the member companies of the European network of ERCI clusters and the solutions presented by them in this area confirm this fact. The workshop helped understanding of the challenges facing this solution. These include, undoubtedly, the issue of improving security. The wide range of potential applications of this technology opens up new possibilities, which, however, must be fully understood in order to be able to fully use them safely.

To sum up, it should be noted that during this important conference, bilateral meetings were held between cluster management boards and their members. On behalf of Poland, Associate Professor PhD Adam Jabłoński, and Associate Professor PhD Marek Jabłoński actively participated in these meetings, especially in terms of comparing the presented solutions in Europe to the solutions operating in Poland. This also concerned the ability to dynamically transfer modern technologies supporting the increase in the level of rail traffic safety to Poland and the analysis of their implementation in the conditions of the operational and investment processes, which are currently very multidimensional in Poland.

BEZPIECZEŃSTWO SECURITY
TEORIA I PRAKTYKA THEORY AND PRACTICE
e-ISSN 2451-0718 2022
ISSN 1899-6264 No. 2 (XLVII)
DOI: 10.48269/2451-0718-btip-2022-2-012

Andrzej Kazimierski
Chief Editor of the quarterly *KontrolerINFO*

New safety challenges: 21st International Congress on Internal Control, Internal Audit, Anti-Corruption, and Anti-Fraud, Krakow, Andrzej Frycz Modrzewski Krakow University, 29–30 September 2022

On 29–30 September 2022, the 21st International Congress on Internal Control, Internal Audit, Anti-Corruption, and Anti-Fraud took place.[1] The Congress was held in the auditorium of the Andrzej Frycz Modrzewski Krakow University, a long-standing partner of the Polish Institute of Internal Control (PIIC), the organizer of the Congress, after two years of forced online organisation (due to the COVID-19 pandemic). The Congress was attended by almost 200 people. It is the only event of its kind in Poland. The overarching aim of this regular international meeting is to share experiences and gather knowledge on the issues, challenges, and prospects facing auditors, internal controllers, and professionals involved in corporate risk management, prevention, and detection of economic fraud and corruption, as well as in *governance* and *compliance*.

This year's proceedings were officially opened by PIIC heads Piotr Grzybowski and Ireneusz Jabłoński, and the Chairman of the PIIC Advisory Board Rafał Krzemień. Associate Professor Klemens Budzowski, the rector of the Andrzej Frycz Modrzewski Krakow University, spoke on behalf of the University, and Angelika

[1] The *KontrolerINFO* quarterly has assumed media patronage of the Congress.

Bodziony-Durych, the General Director of the Małopolskie Province Office in Krakow spoke on behalf of the Małopolskie Province Governor Łukasz Kmita.

As those who attended this year's Congress said, direct contact with speakers is a very different experience to an online conference watched on a computer screen. It allows getting again the full and true values that this type of event provides. The two-day Conference focused on the most important issues and problems related to internal control in its broadest sense.

During the first day, the attendees discussed, among other things, the introduction of *compliance*: How can it be implemented in the overall organisational systems of various entities without limiting their competitiveness? Agata Lauruk, the Compliance Officer and Data Protection Officer at the STS Group, sought to answer this question. In her opinion, to make this happen, *compliance* must focus not on checking people, but on developing the organisation in question.

When analysing the problems of the GDPR regime, which has been in place in Poland for 6.5 years, Joanna Karczewska – recognised as one of the 100 most important women working in the field of cyber security in Europe[2] – summarised the current situation as deplorable. Indeed, the GDPR is implemented in such a way that, instead of protecting citizens from surveillance by artificial intelligence, actually facilitates it. According to Karczewska, the blame for this situation lies with lawyers, especially those working for the Tech Giants. They have overcome the restrictions imposed by the GDPR, while they continue to be a difficulty for small entities.

In their presentations, Piotr Błaszczeć of LOCOS, a PIIC expert, Mateusz Chrobok, a cyber security, AI, and start-up consultant, Maciej Orzechowski, the president of AIA Concept, and Sławomir Szydłowski of Enigma, discussed problems related to the protection of companies and their data from intrusions related to the use of artificial intelligence, which is now becoming one of the most important problems for data security systems in organisations. New professions will soon emerge, such as artificial intelligence auditor and artificial intelligence surveillance system administrator. However, artificial intelligence can also be used to improve the functioning of an organisation and the level of satisfaction of the people within it. This, too, is a task for the internal control system.

Punishable mismanagement – this was another thematic block presented on the first day of the Congress. Issues related to this topic were presented by Martyna Pawłowska and Jakub Pawłowski of the Pawłowscy-Partners law firm, and Grażyna Felisiak, the president of Sfera Biznesu. In their presentations, they stated that it is very easy to be accused of the offence of mismanagement (Article 296 of the Penal Code), for example because of the purchase (even unintentionally) of low-quality or

[2] *Hacking gender barriers: Europe's top cyber women*, Brussels: Women4Cyber Foundation, 2022, https://women4cyber.eu/roadmap-of-actions/100-women-in-cybersecurity-book [accessed: 24 October 2022].

defective goods, or because of a contract or settlement that turns out to be detrimental to the company over a period of time, which is an offence punishable by three months to five years in prison. According to Grażyna Felisiak, who has worked in accounting for 30 years, in her work she has yet to find an organisation that has not in some way violated Article 296 of the Penal Code. Preventing this type of situation is one of the tasks facing internal control.

Auditing, business security, whistleblowers, AML (anti-money laundering), AI (artificial intelligence), corruption, and ethics – these were the topics of the second day of the Congress. In their presentations, these topics were presented by Anna Wojciechowska – a lawyer, Alexander Ruehle – a co-founder and the CEO of zapliance GmbH, Krzysztof Andrejczuk – the Director of the Internal Audit Office at PSE SA, Paweł Sawicki – the head of the Legal and Compliance Department at the Kopeć & Zaborowski law firm, Paweł Cybulski – a former Deputy Minister of Finance, a deputy head of the National Revenue Administration, a PIIC expert, Robert Rzepiński – a security coordinator at Energa SA, Marek Czechowski – the President of Mark Data Protection, and Dr. Rainer Lenz – the head of Corporate Audit Services at SAF-Holland SE, who spoke online about the future of the profession of auditor.

Krzysztof Andrejczuk, when speaking in his presentation titled 'How effective internal audit can support company managers' about cyber security in a company, said that today one should no longer ask oneself if there will be a cyber attack against that company, but when it will happen and how to prepare for it. This is where an audit can help by providing the company with information about possible risks. Unfortunately, a very large number of organisations still do not have a full internal audit function, including 25 per cent of the companies listed on the WSE in the mWIG40 index and one in the WIG20.

These considerations were addressed by Robert Rzepiński in his presentation titled 'Security analysis in business – old and new challenges'. He stated, among other things, that effective protection of classified information in organisations was becoming an increasing problem. The security schemes adopted to date are no longer impregnable, as there are now increasingly frequent attempts to breach these systems for political reasons (e.g. sanctions imposed on Russia) or due to societal changes (triggered by the COVID-19 pandemic). Therefore, all elements of security – those related both to artificial intelligence and to humans themselves – need to be examined more closely and every element needs to be analysed.

In his presentation titled 'Current issues in anti-money laundering. A report on Europe and the world', Paweł Cybulski clearly stated that today crimes can be committed from anywhere in the world – there are no borders or barriers in this respect. An example is the Polish cooperative bank robbed of PLN 1.5 billion by the Colombian mafia. Criminals like it very much when there are fixed due diligence procedures

in place in an organisation, because such procedures are easier to breach and use for extortion and theft.

One of the major issues raised at the Congress was whistleblowers, their role in the functioning of organisations, and their protection. This topic was discussed by Paweł Sawicki in his presentation titled 'Designing and implementing whistleblower channels – guidance for the private and public sectors'. As he stated, if a company that is obliged to implement whistleblower protection rules does not have adequate procedures in place, the company faces criminal liability – the exceptions being small companies with up to 50 employees and communes/municipalities with fewer than 10,000 residents. A whistleblower's report must be accepted within 7 days and feedback must be given within 3 months. Another important point is that no proposed law will protect whistleblowers and their jobs. Ultimately, it is the employer who decides about the protection of whistleblowers.

The Diploma of Honour, awarded by the Polish Institute of Internal Control for special contributions to the development of audit, control, and the prevention of fraud and corruption in Poland, was given to, among others, the Małopolskie Province Governor Łukasz Kmita, Paweł Cybulski, Elżbieta Majchrowska – the Rector's representative for postgraduate studies at the Andrzej Frycz Modrzewski Krakow University, a coordinator of training projects co-financed by the European Social Fund, Joanna Karczewska, and Rafał Patoła – the Deputy Director for Administration and Economics at the National Institute of Public Health – National Institute of Hygiene.

In his speech, Łukasz Kmita said:

> This is an important distinction for me. As a matter of principle, I insist on high standards, including the transparency of the administration's actions and the integrity of each activity that makes up the various tasks. This is also what I expect from everyone I work with. I always emphasise that a properly conducted audit is an important management tool for improving service levels. This is why I do not believe in "sham" and unprepared audits - and unfortunately I have had to deal with many such audits, including ones conducted by members of the parliament. The auditor also needs to be prepared for the audit activities. In my opinion – and this is my principle – everyone should carried out his or her duties as if they were always going to be audited, and therefore in full transparency and to the best of his or her knowledge. I would like to thank the Polish Institute of Internal Control for the award. For me, this confirms not only that I have taken the right direction as the Governor of the Małopolskie Province, but also that my daily work and the way I do it have been recognised by experts. Many thanks to all the staff at the Province Office who ensure these high standards on a daily basis.

The organisers of the Congress also honoured individuals who had made a special contribution to its organisation and to the success that it proved to be this year.

BEZPIECZEŃSTWO TEORIA I PRAKTYKA SECURITY THEORY AND PRACTICE
e-ISSN 2451-0718
ISSN 1899-6264
2022
No. 2 (XLVII)
DOI: 10.48269/2451-0718-btip-2022-2-013

Mirosław Kwieciński

Associate Professor, Andrzej Frycz Modrzewski Krakow University
https://orcid.org/0000-0001-6917-5501

5th Original Multidisciplinary Scientific Seminar *Modus Securitas*: "Determinants of the effectiveness of state and business security management – concepts, models, approaches, practice, visions, and research results", Senator Manor in Zakrzów, 18–20 September 2022

On 18–20 September 2022, the 5th Original Multidisciplinary Scientific Seminar *Modus Securitas* entitled "Determinants of the effectiveness of state and business security management – concepts, models, approaches, practice, visions, and research results" was held at the Senator Manor in Zakrzów in the Makowski Beskid. The initiator and organiser of the seminar was, as in previous years, Mirosław Kwieciński, PhD, an Associate Professor at the Andrzej Frycz Modrzewski Krakow University and at the Carpathian State College in Krosno. The seminar was organised in cooperation with the Economic Intelligence Institute Foundation in Krakow.

The sessions of the 5th edition of the seminar focused on four topics:

1) Doctrinal actions that weaken the security of the state and businesses by flattening citizens' incomes and reducing entrepreneurs' profits, as well as by causing a significant inflationary impulse and a decomposition of alternatives in social life. Has the spectre of Agenda 2030 already become a reality in Poland?

2) A leap forward in the centralisation of the economic and social life. Does the drive to curtail citizens' freedoms by increasing the importance of the central budget, reducing the role of local government, and increasing surveillance set a new, universally applicable standard for the functioning of the state?
3) The urgent need for a dynamic development of a methodological and tool-based concept for managing the resilience of state and business organisations. Is there not a lack of contemporary inspiration for the increased dynamism of the actions undertaken to restore the axiological and normative order, as well as the reproductive function of the young Polish intelligentsia?
4) The nature, causes and consequences of dysfunctions in the methodological order of the research in social sciences and the possibilities of overcoming them.

The subject matter covered, which continues to be of great interest, attracted 24 participants. The academic community was represented by persons from academic institutions in Warsaw, Krakow, Wrocław, Poznań, Upper Silesia, Opole, Bielsko-Biała, Jelenia Góra, Nowy Sącz, and Krosno. The main purpose of the session, as in previous editions, was to discuss selected current issues relating to the determinants of effective state and business security management.

The attention of the participants in the inaugural lecture focused on the important problem of the theory and practice of security management. The 5th edition of the seminar was opened by Łukasz Furman, PhD, an Associate Professor at the UTH (Helena Chodkowska University of Technology and Economics in Warsaw), who presented a paper titled "The financial security of companies in the current economic reality". It was an extremely interesting presentation of the current financial condition of Polish companies, taking into account some of the consequences of the systemic changes in the area of taxes. The participants of the seminar showed great interest in the issues discussed.

The next part of the seminar was the discussion held during the 1st session on the following topic: "Challenges for security management processes in the face of the changes necessitated by the introduction of the ill-conceived concept of the so-called Polish Deal."[1] The proceedings were chaired by Prof. Kazimierz Perechuda from the Wrocław University of Economics and Iwona Gawron, PhD, from the Applied Sciences Academy in Nowy Sącz.

[1] The 'Polish Deal' is a systemic change introduced by the government of the Republic of Poland from 1 January 2022 to ensure the implementation of a plan to rebuild the Polish economy after the COVID-19 pandemic. It is intended to reduce social inequalities, bring beneficial tax changes for 20 million Poles (including raising the tax-free amount to PLN 30,000) and create better living conditions for all citizens. However, the legislation that was introduced proved ill-conceived, contained many inconsistencies, and lacked comprehensiveness, which was poorly received by citizens, especially the middle class and entrepreneurs. The plan – which has been undergoing constant modification since July 2022 – continues to generate a great deal of controversy as well as concern, particularly over tax calculation issues.

The following papers were presented as part of the panel:

- "Reducing the role of local government in the new economic realities. A crisis management perspective" – Katarzyna Sienkiewicz-Małyjurek, PhD, an Associate Professor at the Silesian University of Technology in Gliwice;
- "The threats of a dysfunctional safety culture in rail transport" – Adam Jabłoński, PhD, an Associate Professor at the WSB University in Poznań (Chorzów Branch);
- "Entrepreneurs in the state defence planning and crisis management. The legal status as of 2022" – Border Guard col., ret., Mirosław Hakiel, Economic Intelligence Institute Foundation in Krakow.

The issue of the diversity of security issues in the face of the current conditions was continued during the 2nd session titled "An attempt at a social and systemic diagnosis and a description of the consequences of the implementation of the ill-considered concept of the so-called Polish Deal. A context leading to the necessary implementation of organisational resilience", which was chaired by Janusz Ziarko, PhD, an Associate Professor at the Andrzej Frycz Modrzewski Krakow University, and Daria Hołodnik, PhD, from the Opole University of Technology. The attention of the participants was drawn to the following papers:

- "A failed revolution? Has there been an attempt to replace the elites in Poland? A communication disaster or a camouflaged intentional change?" by Jadwiga Mazur, PhD, University of Security in Poznań, an Associate Professor at the Pedagogical University of Krakow;
- "The police and secret services vs. ethics and law" by Ryszard Bełdzikowski, PhD, from the Higher School of Administration in Bielsko-Biała;
- "Operationalisation of the management of data processing security in the Internet of Things environment as a way to strengthen the resilience of organizations" by Prof. Kazimierz Perechuda and Krzysztof Hauke, PhD, from the Wrocław University of Economics;
- "The establishment of the State Intelligence System in the structure of the executive branch of government of the Republic of Chile as a source of inspiration for the cultural change in the Polish secret services" by Krzysztof Passella, M.A. from the Economic Intelligence Institute Foundation in Krakow.

The presentations concluded with a lively discussion on various aspects of the implementation of the concept of resilience management in contemporary organisations.

The next session was organised as a methodological workshop on the concepts of state and business security management. The proceedings of this session were chaired by Jadwiga Mazur, PhD, University of Security in Poznań, an Associate Professor at the Pedagogical University of Krakow, and Wojciech Topczewski, PhD, from the Karkonosze University of Applied Sciences in Jelenia Góra. The following papers were presented:

- "The methodology of soft systems in solving public security and public order problems" by Janusz Ziarko, PhD, an Associate Professor at the Andrzej Frycz Modrzewski Krakow University;
- "Smart security: a model for the strategiometry of security management using mobile technologies" by Wojciech B. Cieśliński, PhD, an Associate Professor at the University of Health and Sport Sciences in Wrocław;
- "Detection of the operation of non-dual network power in the wine production business" by Daria Hołodnik, PhD.

As during the previous sessions, the papers inspired a lively discussion, thus enriching the output of the proceedings of the seminar.

The session was concluded with a panel discussion titled "Applicability of the concept of organisational resilience in the public sector and business – opportunities and threats", which was chaired by Marek Dudek, PhD, an Associate Professor at the AGH University of Science and Technology in Kraków, and Dariusz Fatuła, PhD, an Associate Professor at the Andrzej Frycz Modrzewski Krakow University. The heated and facts-based discussion among the representatives of the academic and business communities on the definition of the principles of implementation of the concept of organisational resilience led to the following conclusions:

- a need to focus on creative problem-solving in the face of a diversity of circumstances;
- a need for permanent preparation of organisations' structures, exercises, and simulations, which involves some necessary investments;
- implementation of cognitive processes by collecting and processing information;
- a need to motivate people to exhibit desirable behaviour; and
- seeking out and surrounding oneself with smart people who are capable of showing the weaknesses of the organisation and present constructive criticism, which indicates a key role of staff selection.

The 5th edition of the seminar was appreciated by the participants and fully confirmed the need for scientific meetings and discussions. The participants emphasised its high level, both scientific and expert knowledge-related, and the need to continue the seminar next year. To this end, a steering committee was set up by the participants to organise the future sessions.

BEZPIECZEŃSTWO SECURITY
TEORIA I PRAKTYKA THEORY AND PRACTICE
e-ISSN 2451-0718 2022
ISSN 1899-6264 No. 2 (XLVII)

Publication ethics

OUR CODE OF CONDUCT AND BEST PRACTICE GUIDELINES
The Andrzej Frycz Modrzewski Krakow University Publishing House (Oficyna Wydawnicza KAAFM) observes the principles and guidelines that have been developed by the Committee on Publication Ethics (COPE) in the Codes of Conduct and Best Practice Guidelines.

DUTIES AND RESPONSIBILITIES OF THE EDITOR
The Editor shall

- make sure that the publishing ethics is duly observed and shall take all the available and appropriate measures to prevent plagiarism, abuse and other unfair practices, including ghostwriting and/or guest authorship;
- decide which papers will be published, based on the opinions expressed by the editorial board, and the relevant reviews provided by external reviewers who have been duly appointed for this purpose (for more information, go to the Information for Authors tab);
- evaluate the materials submitted for publication in accordance with an agreed and transparent procedure;
- upon taking a decision to publish, consider exclusively the original nature of the submitted material, its overall academic value, and its significance for the development of research in Poland and worldwide; no commercial aspects or fees paid for publication shall have an impact on this decision;
- refrain from disclosing any information to third parties concerning the materials submitted for publication;
- have the right to withdraw a given publication after it has been published if there is evidence to prove a possible lack of reliability or falsification of research data, plagiarism, or a breach of the editorial ethics, as well as where major methodological flaws have been made.

DUTIES AND RESPONSIBILITIES OF THE AUTHOR
The Author shall

- familiarise him/herself with the principles of publishing ethics that have been set by the Editor, as well as the procedure applied for qualifying materials

submitted for publication, the principles of cooperation of the Editor and the Author, and any other technical guidelines provided;
- have the right to submit for publication only his/her individual and original texts. All borrowings, quotes/citations, tables and comments/notes used in the text should be followed by a relevant reference/footnote;
- provide a reliable and accurate description of the studies conducted, and an impartial interpretation of the research findings obtained;
- provide detailed information about the contribution of individual authors where a material that has been submitted for publication has multiple authors;
- enclose a relevant bibliography that includes all the publications that have been used throughout the preparation of the material;
- in the event that major flaws and/or discrepancies are revealed in his/her text, without undue delay notify the Editor of this fact in order to allow for corrections of these mistakes at the editing stage.

DUTIES AND OBLIGATIONS OF THE SCIENCE EDITOR OF A JOINT STUDY
The Science Editor shall
- decide which materials will be published in the joint study that has been proposed by him/her;
- bear responsibility for observing the principles of publishing ethics and the overall academic value of the publishing house;
- in the event of suspected plagiarism or falsification of research data by any of the Authors, take necessary decisions to withdraw the text from the joint study and notify the Editor thereof;
- make certain that the persons who have contributed to the creation of a joint study have accepted and acknowledged its form, once the editing process conducted by the Editor has been completed.

DUTIES AND OBLIGATIONS OF THE REVIEWER
The Reviewer shall
- carry out an impartial assessment of the material submitted for publishing;
- if need be, point to the relevant books or papers connected to the subject matter of the text that have not been quoted or referred to by the author;
- report to the Editor any and all major similarities of the reviewed text with other works;
- not be allowed to use and enjoy the reviewed text for the purposes related to his/her individual benefits; s/he shall not assess the text in the event of a possible conflict of interest with the author either;
- submit his/her review within the agreed deadline, adding a statement that there is no conflict of interest with the author;
- evaluate the materials submitted for publishing in line with an established and transparent procedure.