ISSN: 2957-2150

Czasopismo krajowego rejestru domen

Vol. I /2024

SPIS TREŚCI

Wstęp
Prof. Katarzyna Chałubińska-Jentkiewicz s. 3

Artykuły

1. Federico Borgonovo, Giulia Porrino, Propaganda Mission Command: a comparative social media analysis between the Badri Force 313 and the PMC Wagner, ss. 4-22. (19)
2. Monika Nowikowska, *Tożsamość cyfrowa jako prawo do dostępu do technologii, produktów i usług cyfrowych*, ss. 23-34. *(12)*
3. Federico Costantini, Francesco Crisci, Silvia Venier, Stefano Bistarelli, Ivan Mercanti Mercanti, Tackling disinformation in the UE with "truthster": technological design and DLT, ss. 35-49. (15)
4. Karolina Pięta, Dezinformacja jako narzędzie manipulacji w sieci, ss. 50-65. (16)
5. Krzysztof Kaczmarek, Ukryte zasoby Internetu a terroryzm, ss. 66-77. (12)
6. István Hoffman, *New challenges of local and regional public service provision: platforms and their cybersecurity issues*, ss. 78-88. *(11)*
7. Luka Martin Tomažič, Freedom of Expression on the Internet and National Security in Europe: Liberty and Basic Goods, ss. 89-104. (16)
8. Tal Pavel, *The Iranian Cyberattacks in Albania: Actors, Tactics, Targets*, ss. 105-123. *(19)*
9. Ekaterina Kuznetsova, Affordability of quality: case of Slovenian online shopping, ss. 124-144. (21)

Varia
Kazimierz Krzysztofek, HOMO GEPETENS. Człowiek i sztuczna inteligencja: karzeł na ramionach olbrzyma?, ss. 145-157. (13)

Debiuty
Mateusz Kozłowski, *Konteneryzacja - nowoczesna metoda utrzymywania usług*, ss. 158-170. *(13)*

Sprawozdania
Monika Balcerzak, *Sprawozdanie z corocznego spotkania Partnerów Rejestru domeny.pl*, ss. 171-174. (4)

Wstęp

Treść cyfrowa to nowy rodzaj dobra, które trzeba poddać analizie w różnych aspektach wymaganej ochrony. Ta zmiana wynika z nowego podejścia, kiedy na rynku usług cyfrowych, po raz pierwszy, regulację infrastruktury przyporządkujemy regulacji w zakresie zawartości cyfrowej. Dotychczas pojawiały się istotne pytania o granice podporządkowywania zawartości regulacjom dotyczącym infrastruktury, gdzie dominujące znaczenie miała kwestia konkurencyjności i bezpieczeństwa systemów wspierających usługi cyfrowe. Wydaje się, że nowym kierunkiem jest sytuacja odwrotna, kiedy to regulację infrastruktury przyporządkujemy regulacji w zakresie zawartości cyfrowej. Z wykorzystaniem takiego charakteru przyszłej regulacji powstaje obecna koncepcja ochrony tego, co wypełnia sieć internetową.

Pierwszy numer „dot.pl" stanowi próbę kompleksowego zestawienia różnych aspektów posługiwania się treścią cyfrową, która jest przedmiotem aktualnych i przyszłych regulacji prawnych. Czasopismo będzie przydatną pozycją zarówno dla środowiska rynku domen, jak i wszystkich praktyków, dla których kluczowe znaczenie ma świat cyfrowy. Dotyka zagadnień związanych z rozwojem nowych technologii, e-commerce, cyberprzestrzeni i sytuacji prawnej jednostki w świecie cyfrowym. Problemy poruszone w naszym czasopiśmie odnoszą się zarówno do zagadnień interesujących dla każdego użytkownika sieci, jak i podmiotów gospodarczych, których przedmiotem działania są szeroko definiowane usługi cyfrowe.

dr hab. Katarzyna Chałubińska-Jentkiewicz
Redaktor Naczelna

„dot.pl" - czasopismo Rejestru domeny .pl

Propaganda Mission Command: a comparative social media analysis between the Badri Force 313 and the PMC Wagner

Federico Borgonovo
ITSTIME (Italian Team for Security, Terroristic Issues & Managing Emergencies), Catholic University of the Sacred Heart,
ORCID: https://orcid.org/0000-0002-0028-6737
E-mail: federico.borgonovo@unicatt.it

Giulia Porrino
ITSTIME (Italian Team for Security, Terroristic Issues & Managing Emergencies), Catholic University of the Sacred Heart,
ORCID: https://orcid.org/0009-0007-8697-4787
E-mail: porrinogiulia@gmail.com

Abstract

Between 2021 and 2023 we have witnessed two major military operations, both relating to the field of hybrid conflict: the Taliban conquest of Afghanistan and the Russo-Ukrainian War. Two military units stood out, respectively, the Badri Force 313 and the PMC Wagner. Both units proved the existence of a strong propaganda component combined with operations conducted on the ground. This paper aims to highlight through two comparative case studies, the existence of a new parameter that joins the operational capacity, that is, Propaganda Mission Command. This tool has been observed within the respective digital ecosystems and has had serious tactical-strategic repercussions within

Received: 25.04.2024
Accepted: 24.05.2024
Published: 27.05.2024

Cite this article as:
F. Borgonovo, G. Porrino "Propaganda Mission Command: a comparative social media analysis between the Badri Force 313 and the PMC Wagner"

DOT.PL, no. 1/ 2024, 10.60097/DOTPL/189269

Corresponding author:
Federico Borgonovo
ITSTIME (Italian Team for Security, Terroristic Issues & Managing Emergencies), Catholic University of the Sacred Heart,
E-mail:
federico.borgonovo@unicatt.it

the combat theatres. The online communication of the two military apparatuses influenced recruitment, funding, and even the public's knowledge of the conflict. Finally, the use of propaganda in both these units contributed to the development of a new concept of *Auftragstaktik* that involves the communicative sphere. The existence of such a phenomenon should stimulate public and academic debates regarding the new nature of conflicts. Conflicts in which, as we observed, the propaganda/communication component is now indivisible from the military one and can result in remarkable operational and/or strategic advantages. The analysis of this hybrid tool is also meant to underline its difference from classic state propaganda. The two case studies show a different kind of "Propaganda Mission Command" that is framed within a military context, is related to "branded" units, and can shift the balance of conflicts towards one specific side through influence and psyops.

Keywords: PMC Wagner, Badri Force 313, Hybrid Warfare, Propaganda

Introduction

The final stages of the Taliban's conquest of Afghanistan and the recent Russian-Ukrainian (since its beginnings in 2014) war have highlighted the nature of hybrid conflicts, in particular the communicative aspect that can also be declined as propaganda. The paper focuses on the propaganda sphere of two specific military units, protagonists of the two conflicts: the Badri Force 313 and the PMC Wagner.

Starting from the binomial hybrid warfare-propaganda and the concept of Auftragstaktik, the authors theorised the concept of Propaganda Mission Command as a contemporary declination of Auftragstaktik focused on the propaganda-communication component and applied within today's hybrid warfare contexts.

The concept is then tested through the observation and analysis of the two military units, with particular attention to their reciprocal communication apparatus. The entire study is

based on a review of the relevant literature, data collection, and a content analysis of the propaganda material.

Finally, the authors made a comparison between the two military units. The rationale behind the choice of these two units lies in their great media impact and the diversity of the conflicts in which they operated. This last reason contains within itself the need to discover whether there are specific parameters characterising the application of propaganda in hybrid theatres of war.

Theoretical framework and literature review

The literature review is based on two clusters: the propaganda-communication component within the hybrid conflicts with a specific focus on its application by the Badri Force 313 and PMC Wagner, and finally the contemporary implementation of Auftragstaktik within hybrid warfare frameworks.

For instance, hybrid warfare as a method of war has its roots in the combat methods of former conflicts. In the past, different actors such as States and non-state entities, aimed to reach their political and military goals by implementing a mix of conventional and non-conventional, or irregular, methods such as misinforming world opinions or becoming a powerful force multiplier.

According to Munoz Musquera and Bachmann (2016), Hybrid Warfare may use elements taken from several methods and categories of warfare, such as irregular warfare, asymmetric warfare, and compound warfare.

The crucial element to underline is the fluidity, the capacity of adaptation to different scenarios and to a conflict "*in which states or non-state actors exploit all modes of war simultaneously by using advanced conventional weapons, irregular tactics, terrorism, and disruptive technologies or criminality to destabilize an existing order*"[1].

The main goals of hybrid campaigns are to create confusion, feed social divisions, and target critical vulnerabilities in terms of national security. In doing so, actors combine coercive and subversive measures, designed to be difficult to attribute because operating under a legal threshold. The specific characteristics of hybrid warfare identified by

[1] A. B. Munoz Mosquera et al., *Lawfare in Hybrid Wars: The 21st Century Warfare*, Journal of International Humanitarian Legal Studies, vol. 7, no. 1, 2016, pp. 63–87, https://doi.org/10.1163/18781527-00701008.

authors in previous years are a non-standard, complex, and fluid adversary combination of conventional and irregular methods and flexible use of mass communication for propaganda[2].

Part of the peculiar features characterizing hybrid threats have been detected by literature and have been widely discussed in the academic debate. Among them, it is possible to mention pervasive, diffuse, interconnected, and de-localised[3].

Firstly, "pervasive" is used to indicate the capacity to permeate different dimensions of social life, as it relates to security, economy, politics, and culture, for example, affecting both private actors and public institutions. Secondly, "diffused" stands for the ability to overcome not only the geographical boundaries (national and international) but also the temporal and sociocultural ones. The territorial element, or the loss of it, is a crucial element in the identification of hybrid warfare, explaining the attribution of "de-localized" as a specific feature of the phenomenon. It suggests that hybrid threats may take place at multiple levels in different areas of the world, waged by different actors, "*with diverse weapons, attributable, for instance, to different manifestation of power*"[4]. At last, "interconnected" highlights the peculiar consequences produced by hybrid threats. In a world characterized by its interconnectivity, an event occurring in a specific context inevitably produces repercussions beyond the boundaries of that context. In fact, according to Simons (2021), even though the informational and cognitive realms belong to the intangible world, they do affect events, processes, and outcomes in the tangible physical realm, and the current world's interconnectedness is enhanced even more the effects.

Over the last few years, the enormous technological developments on the media front have broadened the possibilities of increasingly expanding the horizons of hybrid warfare on the communication and propaganda side. The emergence of social media and the possibility of reaching an ever-wider audience to influence, have made it possible to transform narratives into real tools that can be used in the context of hybrid conflicts by a

[2] F. G. Hoffman, *Conflict in the 21st Century*, December 2007, 72.
[3] M. Maiolino, *Geopolitics of Information, Aids and Vaccinesmake Sense in the Framework of COVID-19and Hybrid Conflicts*, 2020, vol.12, no. 2.
[4] ibidem

plurality of actors, both state and non-state. In this landscape, propaganda becomes a fundamental tool in the implementation of hybrid warfare, given the necessity to control the population, inspire divisions among the rivals, and eliminate those who have different ideas and identities. Propaganda is intended as a deliberate effort made through mass media to shape public opinion. Such activities have evolved and exploded in modern times, thanks to new technologies and social media, and are conducted to achieve Hybrid Warfare objectives by a multitude of actors. Propaganda on social media has proved to be extremely effective since "*social media, which is made up of a multitude of trust-based networks, provides fertile ground for the dissemination of propaganda and disinformation, and the manipulation of our perceptions and beliefs"*[5]. The effectiveness of the Propaganda tool has made it appealing also to the Military side of Hybrid Warfare. As a result, the core of a military effort is now made not only of its kinetic side but also of communication and propaganda tactics implemented at both institutional and single army-unit levels.

The above definitions place the war in Afghanistan and the Russian-Ukrainian conflict in the category of hybrid conflicts. According to Farooq Yousaf & Moheb Jabarkhail, in 2021, the Taliban became a massive public-relation multi-lingual militant group efficiently fighting within the communicative sphere through social media propaganda, lawfare, and narrative[6]. Furthermore, the deployment of Badri Force 313 (formerly known as Badri Battalion 313) and its propaganda coverage by Haqqani mediatic houses[7], can be considered a hybrid war maneuver[8]. On the other side, the theoretical framework of Hybrid Warfare has been used by the US Army War College and other experts during the Afghan War defining the counterinsurgency strategies[9]. The Russo-Ukrainian war as far

---

[5] S. Svetok et al., *SOCIAL MEDIA AS A TOOL OF HYBRID WARFARE,* Riga, Latvia, NATO Strategic Communications Centre of Excellence, 2016.

[6] F. Yousaf et al., *Afghanistan's Future under the Taliban Regime: Engagement or Isolation?,* Journal of Policing, Intelligence and Counter Terrorism, vol. 17, no. 1, 2022, pp. 117–34, https://doi.org/10.1080/18335330.2021.1982139.

[7] M. G. Weinbaum et al., *The Tenacious, Toxic Haqqani Network*, 2021, 18.

[8] T. Joscelyn et al., *Taliban's Special Forces Outfit Providing "Security" at Kabul Airport,* FDD's Long War Journal, 2021, https://www.longwarjournal.org/archives/2021/08/talibans-special-forces-outfit-providing-security-at-kabul-airport.php.

[9] I. Käihkö, *The Evolution of Hybrid Warfare: Implications for Strategy and the Military Profession*, The US Army War College Quarterly: Parameters, vol. 51, no. 3, 2021, https://doi.org/10.55540/0031-1723.3084;

back as 2014[10], although hostilities had not yet broken out directly, also possessed all the characteristics of hybrid conflicts[11]. Even after 26 February 2022, these characteristics, again regarding the communicative sphere, were observed[12]. In particular, the case of the PMC Wagner is an example of a hybrid fighting unit deployed in different war realms including the propaganda realm.

Finally, the last part of the literature review is focused on the concept of *Auftragstaktik* and its application/adaptation within the hybrid war. The "*Auftragstaktik*" doctrine that "*allowed subordinate leaders independence to interpret the situation and execute actions that fulfilled the commander's intent rather than the letter of the order*"[13]. In other words, the single unit can therefore autonomously implement propaganda tactics and operations to achieve the commander's goal. The concept originally developed in 1869 by Gen. Helmuth von Moltke, Chief of the Prussian General Staff during the Franco-Prussian War[14], comes under the umbrella of the US armed forces under the definition of Mission Command and then fully adopted in 2019 with the ADP 6-0 Mission Command[15]. The definition states that in Auftragstaktik (Mission Command), commanders issue subordinates a defined objective and the necessary resources to accomplish the mission. Furthermore, subordinate commanders are then given the flexibility to plan and execute their mission within the higher commander's strategy. To operate effectively under this style of command requires a common approach to operations and subordinates who are specialized in their field and trained in independent decision-making[16]. This practice empowers single units' decision-making and decentralized

C. Bockstette, *Taliban and Jihadist Terrorist Use of Strategic Communication*, Connections: The Quarterly Journal vol. 08, no. 3, 2009, pp. 1–24, https://doi.org/10.11610/Connections.08.3.01.

[10] M. Galeotti, *The "Gerasimov Doctrine" and Russian Non-Linear War*, In Moscow's Shadows (blog), 6 July 2014, https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/.

[11] Saressalo and Huhtinen, *The Information Blitzkrieg — "Hybrid" Operations Azov Style*.

[12] F. Borgonovo, *Putin's Hybrid Army*, European Eye on Radicalization (blog), 7 April 2022, https://eeradicalization.com/putins-hybrid-army/.

[13] M. J. Gunther, *Auftragstaktik: The Basis for Modern Military Command?, 8 December 2012, 68.*

[14] R. A. Herrera, *The Auftragstaktik Infatuation*, MILITARY REVIEW, 2022, 14.

[15] Army Doctrine Publication, *Mission Command: Command and Control of Army Forces*. Washington DC: U.S. Government Publishing Office, 2019.

[16] Army Doctrine Publication.

execution across different battlefields proving that the practice of *Auftragstaktik* can be implemented on the contemporary communication-information-heavy battlefield[17].
Taking into consideration the two blocks of literature, we can enucleate the research question of the paper: Is it possible that the new hybrid conflicts have generated a new declination of the Auftragstaktik including the propaganda tool?

Case Studies and Methodology

The criteria that led to the selection of the Badri Force 313 and the PMC Wagner were threefold. Firstly, the hybrid nature of the conflicts in which they operated. Secondly, the media impact of the two units influenced the communicative and cognitive spheres of their respective conflicts. Thirdly the propaganda spread in the theatres of war of these two units is even more relevant since they are strongly marked by extremist ideologies linked to terrorist groups or extremist organizations. In particular, the Haqqani network, founder of the Badri Force is strictly linked to al-Qaeda [18] and the PMC Wagner networks consolidated across Europe among extreme right organizations[19]. And these make propaganda [20], especially the online component, one of their main weapons[21]. The two case studies were conducted through a content analysis of the propaganda material disseminated by the main social platforms related to the units.

Badri Force 313

The Taliban faction known as Network or Clan Haqqani has its military-propaganda apparatus[22]: the media house Manba al-Jihad is the mediatic apparatus that presented the Badri Battalion 313[23]. The connection between Manba and al-Qaeda was also

---

[17] M.J. Gunther, *Auftragstaktik: The Basis for Modern Military Command?*
[18] Weinbaum and Babbar, *The Tenacious, Toxic Haqqani Network*.
[19] M. Townsend, *Russian Mercenaries in Ukraine Linked to Far-Right Extremists*, 2022, https://www.theguardian.com/world/2022/mar/20/russian-mercenaries-in-ukraine-linked-to-far-right-extremists.
[20] A. V. Lieberman, *Terrorism, the Internet, and Propaganda*: *A Deadly Combination*, vol. 9 , 2017, pp. 31.
[21] M. Conway, *Determining the Role of the Internet in Violent Extremism and Terrorism: Six Suggestions for Progressing Research*, Studies in Conflict & Terrorism, vol. 40, no. 1, 2017, pp. 77–98, https://doi.org/10.1080/1057610X.2016.1157408.
[22] D. Rassler, *Multinational Mujahidin: The Haqqani Network between South Asia and the Arabian Peninsula,* Pan-Islamic Connections: Transnational Networks Between South Asia and the Gulf, Christophe Jaffrelot (ed.) and Laurence Louer, Oxford University Press, 2018), https://doi.org/10.1093/oso/9780190862985.003.0006.
[23] B. Roggio, *Taliban Promotes Its "Preparation for Jihad"*, FDD's Long War Journal, 14 August 2019, https://www.longwarjournal.org/archives/2019/08/taliban-promotes-its-preparation-for-jihad.php.

observed thanks to the data collection concerning the Badri Force as during the research, the official page of Manba al-Jihad was found within the Chirpwire platform, a well-known social media platform created and populated by Qaeda media houses [24].

The first reference to Badri 313 dates to 2020 with a video, compiled by Manba al-Jihad, entitled 'Badri Strike'. In the video, the suicide operation conducted in 2018 against the compound of the British oil company G4S is extolled, making explicit reference for the first time to a Taliban unit called Badri 313. The video shows how the attack was carefully planned and then carried out by a trained and specialised unit. The video once again confirms the tactical-ideological link to al-Qaeda; it shows a speech by Usadh Mohammad Yasir, a key figure in the alliance between the Taliban and al-Qaeda, praising the suicide operations carried out by Taliban special forces.

In May 2020, the Twitter (now X) channel of the Badri Battalion 313 unit was created. In April 2021, Manba al-Jihad disseminated photo reports of Taliban forces with advanced equipment and vehicles. The propaganda slant is no longer focused on martyrdom and the use of the suicide weapon, but instead focuses on training, technology, firepower, and the use of vehicles. The image produced shows a unit with an offensive set-up but with a propaganda slant closer to a Western special force. With this video, the foundations are laid for the process of 'distancing' from al-Qaeda to build a new image of the Taliban, starting with their soldiers. In the same year in July, the Haqqani media house published a second photo report; in this case, the Graduation of the Badri 313 Battalion is presented. Like the April photos, a special military unit with first-rate equipment is presented, but in this case, the brandification process is perfected. A universally recognisable military nomenclature ('Battalion') and a logo identifying the unit are shown. The Badri Battalion 313 is portrayed as a special unit increasingly similar to its Western counterparts and at the same time assumes its own identity that is recognisable from the outside. The propaganda operation is not limited to presenting the battalion but aims at appropriating or downplaying American military symbolism; the July photo reportage

[24] M. Lakomy, *Why Do Online Countering Violent Extremism Strategies Not Work? The Case of Digital Jihad*, Terrorism and Political Violence, 2022, pp. 1–38, https://doi.org/10.1080/09546553.2022.2038575.

features a photograph depicting Taliban soldiers in the act of hoisting the flag of the Afghan emirate, recalling the US seizure of Mount Suribachi on Iwo Jima in 1945 (figure 1).

***Figure 1**: Photo taken from the "Graduation Day"*

Directly linked to the Badri 313 Battalion is a Twitter page (already active since May 2020), within which we can distinguish two different propaganda productions before and after the conquest of Kabul. In the pre-conquest phase, updates from the front provided by Manba al-Jihad operators and pictures depicting the Badri 313 Battalion are disseminated. In the phase following the conquest of the capital, the page began to spread bulletins and photo reports on operations conducted directly by the unit, adding more and more visual elements specifically designed to create the external image of the battalion. An image that, even more than before, attempts to portray the Taliban as a militarily professional actor and, above all, capable of autonomously guaranteeing the security of its citizens. It is the need for security (from actors like IS and its Wilayah Khorasan) that pushes the Haqqani leadership to re-brand Badri Battalion 313, which changes its name to Badri Force 313 and transforms itself from a special assault battalion (figure 2) to a SWAT unit (figure 3) placed to defend nerve centres. At the same time, the Twitter page fueled the construction of the increasingly 'Western' image of Badri Force

313. The account's profile picture itself no longer showed a militiaman in camouflage with a covered face, but in June 2022 it shows well-equipped, and smiling soldiers can be seen as if they wanted to convey a sense of security and serenity (figure 4). Finally, the profile photo and banner were changed again and those now show a soldier with the Taliban Flag and the official symbols of the Taliban Emirate (figure 5).

***Figure 2**: first official logo of Badri 313*

***Figure 3:** second official logo of Badri 313*

***Figure 4:** Twitter page Badri 313 06/2022*

Figure 5: *Twitter page Badri 313 09/2022*

PMC Wagner

The PMC Wagner is an independent group of private mercenaries, but according to various testimonies, it would be a unit used by Russia in conflicts where the possibility of declaring oneself not involved (plausible deniability) is required[25]. Wagner has been regularly mentioned as a front for a Russian proxy war plan, particularly in Africa[26].

From the use of social media, we noticed a long-lasting and well-established online presence. The PMC maintains a considerable online presence with multiple Telegram channels, RuTube, YouTube, VKontakte (VK), and TikTok[27]. The core of the PMC Wagner propaganda apparatus is focused on promoting its ideology, fighting spirit, and recruiting new members. In its promotional videos, the PMC is portrayed as taking part in training,

[25] C. Rondeaux, *Decoding the Wagner Group: Analyzing the Role of Private Military Security Contractors in Russian Proxy Warfare,* New America, November 2019; N. Reynolds, *Putin's Not-So-Secret Mercenaries: Patronage, Geopolitics, and the Wagner Group*, Carnegie Endowment for International Peace, 2019; R. Parens, *The Wagner Group's Playbook in Africa: Mali,* Foreign Policy Research Institute, March 2022; J. Stanyard et al., *The Grey Zone Russia's Military, Mercenary and Criminal Engagement in Africa*', February 2023.

[26] ibidem

[27] G. Porrino, *Pro-Wagner Gaming Subculture: How the PMC Gamified Recruitment and Propaganda Processes,* Sicurezza, Terrorismo e Società, vol. 17, 2023.

and demonstrations, as well as combat. Given the hybrid nature of the PMC, the communication techniques adopted by the Wagner propaganda machine are aimed at recruitment, radicalization, and financing.

The symbolism of the PMC Wagner combines various neo-Nazi elements with the classical symbols tied to Russian nationalism. On PMC Wagner profiles on Telegram and VK, the mercenaries often published their images with the Russian Imperial Movement (RIM) flag, a white supremacist paramilitary group that the US designates as a terrorist organization (figure 6)[28]. Even the symbol of Rusich, a reconnaissance, sabotage, and assault group formed in 2014, directly attached to the PMC Wagner, shows the colors of the RIM flag with the Black Sun, an icon found on the floor of Wewelsburg Castle, the ideological and spiritual center of the SS since 1934 (figure 7). The main "uniting" factors of Rusich, a multi-national group that includes Poles, Norwegians, Bulgarians, and probably Serbs, are national socialism and adherence to native European faiths. We note how the ideological spectrum depicted in the PMC Wagner symbol is at once specific but broad enough to reach different communicative targets. In this spectrum, we find Russian nationalists, anti-Ukraine, white supremacists, and accelerationists.

Figure 6: *Frame of a video published on YouTube by a well-known Russian influencer in which two PMC Wagner mercenaries are interviewed. In the background the RIM flag 09/2023*

[28] A. Kruglova, *The Russian Imperial Movement, the War in Ukraine and the Future of Russian State*, 1 September 2023, https://www.icct.nl/publication/russian-imperial-movement-war-ukraine-and-future-russian-state.

Figure 7: *Rusich Symbol*

The PMC Wagner has built an impressive online propaganda apparatus that has further expanded the recruitment pool by tapping into international European far-right circuits. The network of far-right and alt-right actors in Europe, especially in North and Western Europe, thanks to football communities and mixed martial arts tournaments was linked to the recruitment apparatus of the PMC Wagner. The data collection shows that the content of propaganda varied before and after the outbreak of hostilities. Football ultras and drills in rooms adorned with neo-Nazi symbols during wartime were added to war bulletins, video messages from commanders, bank details, and crypto wallets for funding. Finally, the affirmation of a media house formed by PMC Wagner veterans, deployed also in Africa and the Middle East, was observed.

Among the actors in this network, we find several parallel units orbiting around the PMC Wagner as embedded support groups. Among them: Rusich; Española, a parallel battalion of Russian ultras led by Alexander Shum and with a special training centre near San Petersburg (figure 8); Serb members, active since the deployment in Syria. Those are linked with several ultras communities and Nidhogg, a little unit near the Scandinavian right-wing militia funded by an actual Wagner member[29].

[29] F. Borgonovo et al., *PMC Wagner and Allied Mercenaries, Aftermath of the March*, 26 June 2023, https://www.itstime.it/w/pmc-wagner-and-allied-mercenaries-aftermath-of-the-march-by-federico-borgonovo-giulia-porrino/.

What this network of supporters reveals is a spontaneous system of European far-right militarisation. In other words, a soft propaganda and training operation that opened the doors of PMC Wagner to the world of the European extreme right and to all those supporters willing to fight against Ukraine under ethnonationalism ideology (figure 9).

The functioning of the network was observed in the days immediately following the Russian invasion in February 2022. Following the Russian attack, the actors organised themselves as a spontaneous infrastructure to support operations in Ukraine. The network of groups and organisations, being already well structured, became active in a short time and immediately provided support for the recruitment, propaganda, and financing of the PMC Wagner. The network of far-right, alt-right, and supremacist actors rooted over the years organised itself as a spontaneous infrastructure to support operations.

Figure 8: *Espanol propaganda banner*

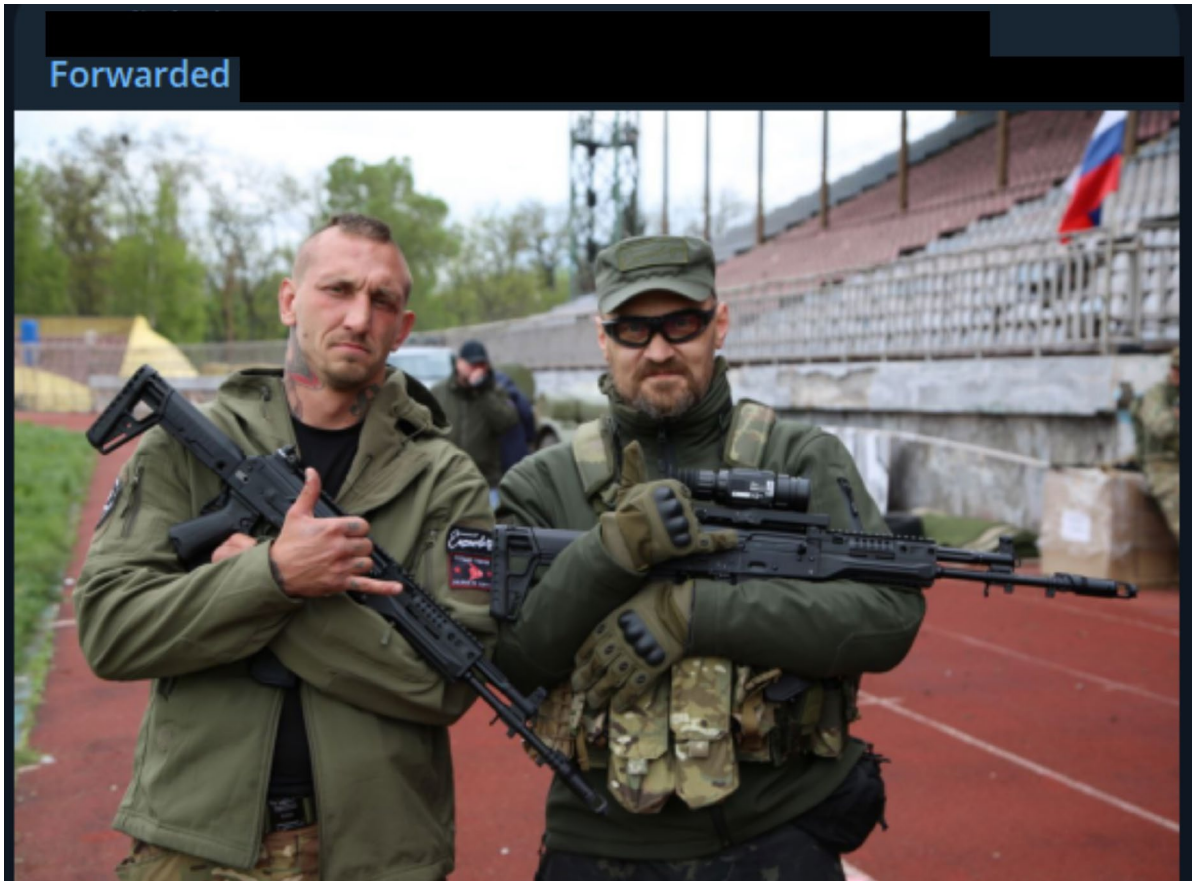


Figure 9: *Espanola fighters training with PMC Wagner mercenaries inside a football stadium (published on Telegram) 05/2023*

Comparison

Based on what has been gathered so far, it is possible to draw some elements from the comparison between the forms of propaganda observed in the two previous case studies. As for Badri 313, it is a military unit founded and created by the Haqqani network, by the media company Manba al-Jihad. The latter has not activated specific recruitment or financing systems related to propaganda, characterizing itself more in a demonstrative key. By this we mean the purpose of showing to the world, through Twitter channels, online sites, and ChirpWire, a special military unit that visually resembles Western ones, thus enhancing its affinities with military units considered elite. The aim was therefore almost entirely "*aesthetic*", that is military propaganda disconnected from the Taliban regime and other factions but aimed at underlining the professionalism and ability performed usually linked to the Western world. The *Auftragstaktik*, therefore, resides in the Haqqani network's characteristic of acting as a sort of Taliban Military Staff, thus

allowing Manba al-Jihad to implement its self-centred propaganda. At the same time, it is subservient to the Taliban's global communication strategy, aimed at showing their status and power both inside and outside the country.

As far as the PMC Wagner is concerned, on the other hand, it has set up its online propaganda apparatus without any intermediary and without resorting to media houses, unlike what was found for Badri 313. PMC Wagner has its channels, also in the light of its genesis as a voluntary unit. This allows it to have its channels whose purpose is not just to implement propaganda aimed at showing off its capabilities. On the contrary, a more complex purpose emerges which also includes financing, recruitment, and radicalization. It is a paramilitary unit that is ideologically well-deployed and well-rooted in far-right Western European networks.

In light of what has been found, therefore, it emerges that on the one hand, there is experimentation of Propaganda Mission Command with extreme flexibility and independence by both leaders and individual military units and at the same time experimentation of a form of tense propaganda to show warfare. On the other hand, there is an effective implementation of Wagner's tactics, tools, and individual communicative propaganda initiatives, which implemented the Auftragstaktik in a complete and all-encompassing form for military reasons. This is due in particular to the very nature of PMC Wagner as a private military company unofficially framed in the army but at the same time characterized by a hybrid nature, that is, capable of incorporating the most diverse shades of war spheres. Also, in light of the foregoing in terms of changing the nature of conflicts in a hybrid key, the communication and propaganda sphere stands out, in particular, to fight by attracting recruits and funding at the same time.

Conclusions

The nature and forms through which conflicts manifest and develop are undergoing profound change, now revealing the characteristics of Hybrid Warfare that the doctrine has long identified and debated. These processes of hybridization of the conflict are now firmly placed alongside the military component of other forms of conflict, which insinuate themselves through the legal loopholes that are the result of a determination of war that has now profoundly changed. This allows a plethora of actors, both state and non-state,

to use the countless recent technological transformations to conduct hostile actions of various kinds.

Among the most relevant possibilities in the course of this research, there is the use of propaganda no longer as an ancillary tool of military action, but as an autonomous form of warfare and a weapon in its own right. In conducting this analysis, the focus was concentrated on two specific actors who are of particular interest due to their peculiar characteristics and the scenarios in which they operate, namely the Badri Force 313 and the PMC Wagner. The comparative analysis of the two units reveals the use of Propaganda Mission Command with different purposes and means. The Badri force set up a muscular propaganda based on the use of aesthetics and aimed at targeting the West. PMC Wagner (and its alliance system) in addition to reporting news from the conflict engaged in massive online and offline recruitment campaigns. The materials found on the social platforms make it possible to appreciate the specificity of this new form of conflict management, now full of a hybrid nature as in the present cases in which the two actors considered were involved. In addition, their extremist nature is also relevant (see Table 1). The propaganda conducted in the war theatres considered by these two units allows us to appreciate the extremist nature of these two units. In addition, their extremist ideologies are linked in a more or less structured form to extremist groups which now make propaganda and the communicative sphere one of their main weapons. This phenomenon is of even greater interest in the framework of studies on the nature of conflicts and the future of warfare as it underlines on the one hand the ramification of propaganda activity that benefits from technological innovations to reach an ever-wider audience and provide increasingly sophisticated content. On the other hand, the contribution highlights the fragmentation of propaganda as far as its authors are concerned, and the use made of it. Indeed, the role of non-state actors is increasingly emerging, not necessarily linked to state authorities in the Weberian sense of the term, who play no longer a marginal role in the framework of modern conflicts, exploiting propaganda as an autonomous and independent tool of warfare.

Table 1: *Propaganda mission command categorization*

Unit	Type of unit	Social Media	Ecosystem	Affiliation	Propaganda	Symbology
Badri Force 313	Special operation force	Multiple platforms linked to the institutions	Centralized and institutional	Haqqani network and government	Muscular Propaganda	Jihadism and al-Qaeda
Wagner PMC	Private military company	Multiple platforms linked to soldiers, influencers, and leadership	Decentralized and semi-institutional	Yevgeny Prigozhin	Recruitment propaganda	Neonazism and Russian right-wing extremism

References

Army Doctrine Publication. 'Mission Command: Command and Control of Army Forces'. Washington DC: U.S. Government Publishing Office, 2019.

Bockstette, Carsten. 'Taliban and Jihadist Terrorist Use of Strategic Communication'. *Connections: The Quarterly Journal* 08, no. 3 (2009): 1–24. https://doi.org/10.11610/Connections.08.3.01.

Borgonovo, Federico. 'Putin's Hybrid Army'. *European Eye on Radicalization* (blog), 7 April 2022. https://eeradicalization.com/putins-hybrid-army/.

Borgonovo, Federico, and Giulia Porrino. 'PMC Wagner and Allied Mercenaries, Aftermath of the March', 26 June 2023. https://www.itstime.it/w/pmc-wagner-and-allied-mercenaries-aftermath-of-the-march-by-federico-borgonovo-giulia-porrino/.

Conway, Maura. 'Determining the Role of the Internet in Violent Extremism and Terrorism: Six Suggestions for Progressing Research'. *Studies in Conflict & Terrorism* 40, no. 1 (2 January 2017): 77–98. https://doi.org/10.1080/1057610X.2016.1157408.

Galeotti, Mark. 'The "Gerasimov Doctrine" and Russian Non-Linear War'. *In Moscow's Shadows* (blog), 6 July 2014. https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/.

Gunther, MAJ Michael J. 'Auftragstaktik: The Basis for Modern Military Command?', 8 December 2012, 68.

Herrera, Ricardo A. 'The Auftragstaktik Infatuation'. *MILITARY REVIEW*, 2022, 14.

Hoffman, Frank G. 'Conflict in the 21st Century':, December 2007, 72.

Joscelyn, Thomas, and Bill Roggio. 'Taliban's Special Forces Outfit Providing "Security" at Kabul Airport'. FDD's Long War Journal, 22 August 2021. https://www.longwarjournal.org/archives/2021/08/talibans-special-forces-outfit-providing-security-at-kabul-airport.php.

Käihkö, Ilmari. 'The Evolution of Hybrid Warfare: Implications for Strategy and the Military Profession'. *The US Army War College Quarterly: Parameters* 51, no. 3 (25 August 2021). https://doi.org/10.55540/0031-1723.3084.

Kruglova, Anna. 'The Russian Imperial Movement, the War in Ukraine and the Future of Russian State', 1 September 2023. https://www.icct.nl/publication/russian-imperial-movement-war-ukraine-and-future-russian-state.

Lakomy, Miron. 'Why Do Online Countering Violent Extremism Strategies Not Work? The Case of Digital Jihad'. *Terrorism and Political Violence*, 17 March 2022, 1–38. https://doi.org/10.1080/09546553.2022.2038575.

Lieberman, Ariel Victoria. 'Terrorism, the Internet, and Propaganda: A Deadly Combination' 9 (2017): 31.

Maiolino, Marco. ‘Geopolitics of Information, Aids and Vaccinesmake Sense in the Framework of COVID-19and Hybrid Conflicts.Pdf’ 12, no. 2 (2020).

Munoz Mosquera, Andres B., and Sascha Dov Bachmann. ‘Lawfare in Hybrid Wars: The 21st Century Warfare’. *Journal of International Humanitarian Legal Studies* 7, no. 1 (14 March 2016): 63–87. https://doi.org/10.1163/18781527-00701008.

Parens, Raphael. ‘The Wagner Group’s Playbook in Africa: Mali’. Foreign Policy Research Institute, March 2022.

Porrino, Giulia. ‘Pro-Wagner Gaming Subculture: How the PMC Gamified Recruitment and Propaganda Processes’. *Sicurezza, Terrorismo e Società* 17 (2023).

Rassler, Don. ‘Multinational Mujahidin: The Haqqani Network between South Asia and the Arabian Peninsula’. In *Pan-Islamic Connections: Transnational Networks Between South Asia and the Gulf*, edited by Christophe Jaffrelot and Laurence Louer, 0. Oxford University Press, 2018. https://doi.org/10.1093/oso/9780190862985.003.0006.

Reynolds, Nathaniel. ‘Putin’s Not-So-Secret Mercenaries: Patronage, Geopolitics, and the Wagner Group’. Carnegie Endowment for International Peace, 2019.

Roggio, Bill. ‘Taliban Promotes Its “Preparation for Jihad” | FDD’s Long War Journal’, 14 August 2019. https://www.longwarjournal.org/archives/2019/08/taliban-promotes-its-preparation-for-jihad.php.

Rondeaux, Candace. ‘Decoding the Wagner Group: Analyzing the Role of Private Military Security Contractors in Russian Proxy Warfare’. New America, November 2019.

Saressalo, Teemu, and Aki-Mauri Huhtinen. ‘The Information Blitzkrieg — “Hybrid” Operations Azov Style’. *The Journal of Slavic Military Studies* 31, no. 4 (2 October 2018): 423–43. https://doi.org/10.1080/13518046.2018.1521358.

Stanyard, Julia, Thierry Vircoulon, and Julian Rademeyer. ‘The Grey Zone Russia’s Military, Mercenary, and Criminal Engagement in Africa’, February 2023.

Svetoka, Sanda, Anna Reynolds, and Linda Curika. *SOCIAL MEDIA AS A TOOL OF HYBRID WARFARE*. Riga [Latvia]: NATO Strategic Communications Centre of Excellence, 2016.

The Telegraph, Foreign. ‘Taliban Mocks US by Recreating the Famous Picture of Soldiers Raising the Stars and Stripes on Iwo Jima’. *The Telegraph*, 26 August 2021. https://www.telegraph.co.uk/world-news/2021/08/26/taliban-mocks-us-recreating-photograph-key-second-world-war/.

Townsend, Mark. ‘Russian Mercenaries in Ukraine Linked to Far-Right Extremists’, 20 March 2022. https://www.theguardian.com/world/2022/mar/20/russian-mercenaries-in-ukraine-linked-to-far-right-extremists.

Weinbaum, Marvin G, and Meher Babbar. ‘The Tenacious, Toxic Haqqani Network’, 2021, 18.

Yousaf, Farooq, and Moheb Jabarkhail. ‘Afghanistan’s Future under the Taliban Regime: *Engagement or Isolation?*’ *Journal of Policing, Intelligence and Counter Terrorism* 17, no. 1 (2 January 2022): 117–34. https://doi.org/10.1080/18335330.2021.1982139.

„dot.pl" - czasopismo Rejestru domeny .pl

Tożsamość cyfrowa jako prawo do dostępu do technologii, produktów i usług cyfrowych

Monika Nowikowska
ASzWoj, Wydział Prawa i Administracji
Al. gen. Chruściela Montera 103, 00-910, Warszawa, Polska
ORCID: https://orcid.org/0000-0001-5166-8375
E-mail: monika.nowikowska@gmail.com

Streszczenie

Zmiany społeczne związane z rozwojem nowych technologii stymulują procesy demokratyczne, stanowią przestrzeń do osiągania różnych celów gospodarczych, jak również mogą dotyczyć sfery funkcjonowania człowieka, także jego praw i wolności. Przedmiotem przeprowadzonych badań jest wskazanie nowych obszarów regulacyjnych, wpływających na prawa jednostki. Artykuł ma na celu przybliżenie ewolucji tożsamości cyfrowej w Internecie oraz wyzwań dla jej ochrony wynikających z rozwoju nowych technologii. Hipoteza badawcza zakłada, że tożsamość cyfrowa stanowi nowe prawo, pozwalające na realizację uprawnień jednostki w sieci. Prawo do tożsamości cyfrowej wyraża się w prawie do dostępu do technologii, produktów i usług cyfrowych. W pracy wykorzystano metody: historyczną, egzegezy tekstu prawnego oraz indukcyjną i dedukcyjną. Do weryfikacji tej hipotezy zastosowano przegląd literatury przedmiotu oraz aktów

Received: 26.11.2024
Accepted: 05.12.2024
Published: 05.12.2024

Cite this article as:
M. Nowikowska, "Tożsamość cyfrowa jako prawo do dostępu do technologii, produktów i usług cyfrowych"

DOT.PL, no. 1/ 2024,
10.60097/DOTPL/196891

Corresponding author:
Monika Nowikowska
ASzWoj, Wydział Prawa i Administracji
E-mail:
monika.nowikowska@gmail.com

unijnych, regulujących zagadnienie tożsamości cyfrowej. Zamiarem autorki niniejszego artykułu było także uporządkowanie obszaru pojęciowego. W artykule podjęto próbę zdefiniowania pojęcia „tożsamości cyfrowej" oraz ustalenia jego relacji z takimi pojęciami jak: „tożsamość internetowa", „tożsamość online", „e-tożsamość".

Słowa kluczowe: tożsamość cyfrowa, społeczeństwo informacyjne, usługi cyfrowe, nowe technologie

Digital identity as the right to access digital technologies, products and services

Abstract

Social changes associated with the development of new technologies stimulate democratic processes, provide a space for achieving various economic goals, as well as can affect the sphere of human functioning, including his rights and freedoms. The subject of the conducted research is to identify new regulatory areas, creating new rights of the individual. The article aims to provide an overview of the evolution of digital identity on the Internet and the challenges to its protection arising from the development of new technologies. The research hypothesis is that digital identity is a right, allowing the realization of the individual's rights in the network. The right to digital identity is expressed in the right to access digital technologies, products and services. The paper uses the following methods: historical, exegesis of the legal text, and inductive and deductive. To verify this hypothesis, a review of the literature on the subject and EU acts regulating the issue of digital identity was used. It was also the intention of the author of this article to organize the conceptual area. The article attempts to define the concept of „digital identity" and to establish its relationship with such concepts as: „internet identity", „online identity", „e-identity".

Keywords: digital identity, information society, digital services, new technology

Wstęp

Rozwój nowych technologii powoduje, że coraz większa część życia codziennego wielu ludzi przenosi się do internetu. Podczas korzystania z serwisów bankowych, urzędowych. medycznych, zakupów on-line, używana jest tzw. cyfrowa tożsamość. Cyfrowy świat staje się naturalnym środowiskiem współczesnego człowieka. Na przestrzeni kilku ostatnich lat ekosystem cyfrowych usług zaufania znacząco się rozwinął. Dostrzegając rosnącą rolę usług w sieci, także na szczeblu Unii Europejskiej, wprowadzane są zmiany legislacyjne zakładające wysoki stopień harmonizacji na poziomie ustawodawstw krajowych.

W ostatnim okresie na gruncie dokumentów unijnych pojawiło się pojęcie „tożsamości cyfrowej". **Brak jest legalnej definicji tego pojęcia. W literaturze przedmiotu podkreśla się, że** każdy człowiek posiada tożsamość, na podstawie której buduje fundamenty swojej indywidualnej godności[30]**.** M. Flis pojęcie tożsamości definiuje jako „zbiór wyobrażeń, sądów, przekonań, które konstruuje podmiot wobec samego siebie, czyli układ autodefinicji aktora społecznego"[31]. Termin ten wiąże się z zespołem cech, które pozwalają zidentyfikować, rozpoznać daną osobę. Ustalenie czyjejś tożsamości polega na rozpoznaniu specyficznych cech danej osoby, które odróżniają tę osobę od innych[32]. Tożsamość jednostki jest relatywna względem tożsamości innych jednostek.

Tak rozumianą tożsamość można porównać do pojęcia „wizerunku". Przez wizerunek rozumie się cechy, które pozwalają zidentyfikować jakąś osobę jako określoną jednostkę fizyczną. Są to dostrzegalne, fizyczne cechy człowieka, tworzące jego wygląd i pozwalające na identyfikację osoby wśród ludzi[33]. Zarówno podstawową funkcją tożsamości, jak i wizerunku, jest identyfikowanie osoby na podstawie posiadania określonej liczby atrybutów. Na tak rozumiane definicje składają się dwa elementy:

---

[30] M. Domańska, *Zakaz dyskryminacji ze względu na więcej niż jedno zabronione kryterium*, Warszawa 2019, s. 63.

[31] M. Flis (red.) *Etyczny wymiar tożsamości kulturowej, Studia z antropologii społecznej*, Warszawa 2004, s. 30.

[32] K. Chałubińska-Jentkiewicz, M. Nowikowska, *Bezpieczeństwo, tożsamość, prywatność – aspekty prawne*, Warszawa 2020, s. 60.

[33] Zob. M. Poźniak-Niedzielska, J. Szczotka, *Prawo autorskie. Zarys problematyki*, Warszawa 2020, s. 229; M. Poźniak-Niedzielska, *Ograniczenie praw autorskich do wizerunku, korespondencji i źródeł in*formacji [w:] *Prawo autorskie i prawa pokrewne. Zarys wykładu*, M. Poźniak-Niedzielska (red.), Bydgoszcz 2006, s. 133; E. Wojnicka, *Prawo do wizerunku w ustawodawstwie polskim*, „Zeszyty Naukowe Uniwersytetu Jagiellońskiego PWiOWI 1990, nr 56, s. 107; M. Nowikowska, *Prawo do wizerunku i prawo adresata korespondencji*, [w:] *Prawo własności intelektualnej. Teoria i praktyka*, J. Sieńczyło-Chlabicz (red.), Warszawa 2021, s. 315-316.

zespół cech (atrybutów) jednostki oraz rozpoznawalność. W aspekcie cech pozwalających odróżnić jednostkę od innych osób R. Coomaraswamy trafnie podkreśla, że tożsamość nie jest ze swej istoty niezmienna, bowiem jest kompozytem składającym się z wielu samodzielnych, często konkurujących, sprzecznych i podlegających transformacji kryteriów. Dlatego tożsamość często ulega zmianom, również w odpowiedzi na reakcję, czy zmienność ideologii i pod wpływem doświadczeń życiowych[34]. Jako przykład specyficznych cech, które kształtują tożsamość jednostki można wskazać miejsce i datę urodzenia, kolor włosów, numer dowodu osobistego, numer PESEL. Niektóre z tych cech nigdy się nie zmieniają, jak np. data urodzenia, jednak część z nich, może ulec zmianie, np. numer dowodu osobistego.

Wraz z rozwojem technologii cyfrowej pojawiły się także takie pojęcia, jak „tożsamość on-line" i „tożsamość cyfrowa", „e-tożsamość". Brak legalnych definicji omawianych pojęć sprawia, że obowiązek konstruowania ich znaczenia ciąży w głównej mierze na doktrynie i judykaturze.

Przez „tożsamości on-line", rozumie się całokształt indywidualnych cech, które użytkownik wykazuje w społeczności internetowej, będąc na stronach internetowych. Jako przykład można wskazać posługiwanie się prawdziwymi danymi (np. imię i nazwisko), pseudonimem lub awatarem (obraz graficzny) podczas korzystania np. z forów internetowych czy sieciowych gier internetowych. Tak rozumiana tożsamość on-line stanowi odzwierciedlenie użytkownika w sieci.

„E-tożsamość" to cyfrowy odpowiednik dokumentu tożsamości, który składa się z zestawu danych, potwierdzających on-line tożsamość użytkownika. Rozwiązania takie są stosowanie przykładowo w sektorze bankowym, pozwalając na dokonywanie czynności on-line, np. zaciąganie kredytów bankowych.

Natomiast przez „tożsamość internetową" rozumie się zespół cech jednostki, które pozwalają ją odróżnić od innych użytkowników w Internecie, np. na portalach społecznościowych, takich jak Facebook, Instagram lub LinkedIn. Tożsamość internetowa tworzy się w wyniku dokonywania codziennych czynności, takich jak zakupy

---

[34] R. Coomaraswamy, *Identity within: Cultural Relativism, Minority Rights and the Empowerment of Women*, **„The George Washington International Law Review", 2002, vol. 34, no. 3, s. 484 i n.**

bądź płatności on-line, rejestrowanie się na wielkich platformach VoD (*video on demand*), jak np. Netflix, HBO Max, Amazon Prime Video.

„Cyfrowa dekada”

Dostrzegając rosnącą rolę internetu w życiu współczesnego człowieka, ustawodawca unijny akcentuje potrzebę podniesienie skuteczności w wykonywaniu publicznych i prywatnych usług związanych z szeroko pojętym handlem elektronicznym na terytorium Unii Europejskiej, a także ułatwienie w użytkowaniu usług internetowych o charakterze transgranicznym. Ma temu służyć prawo obywateli UE do tożsamości cyfrowej, która może zwiększyć dostęp użytkownika do usług publicznych i prywatnych w Internecie. Istotnym celem, jakim kieruje się ustawodawca unijny, jest nadanie szczególnych atrybutów, będących rozwiązaniem z zakresu tożsamości elektronicznej, które powinny zanotować wzrost zdolności, wydajności oraz osiągnąć wysoki poziom zaufania w całej Unii Europejskiej, zarówno w sektorze prywatnym, jak i w sektorze publicznym, w związku z koniecznością identyfikacji i uwierzytelnienia użytkowników przy zapewnieniu wysokiego poziomu bezpieczeństwa. Dalszej analizie poddano podstawowe dokumenty prawne, w których w ostatnim czasie zaakcentowano potrzebę szybkiego rozwoju transformacji cyfrowej.

W „Europejskiej deklaracji praw i zasad cyfrowych w cyfrowej dekadzie”[35] z 23 stycznia 2023 r., proklamowanej przez Parlament Europejski, Radę i Komisję, podkreślono że transformacja cyfrowa ma wpływ na każdy aspekt życia[36]. Oferuje ona znaczne możliwości poprawy jakości życia, wzrostu gospodarczego oraz zrównoważonego rozwoju. Stąd, transformacja cyfrowa stanowi dla UE wyzwanie aby określić, w jaki sposób prawa podstawowe, stosowane w normalnym życiu, powinny być wdrażane w świecie internetowym.

W Deklaracji podkreślono, że transformacja cyfrowa musi odbywać się przy uwzględnieniu pięciu podstawowych zasad. Po pierwsze, nie powinna ona pociągać za

[35] Wspólne deklaracje Parlament Europejski, Rada, Komisja Europejska „Europejska deklaracja praw i zasad cyfrowych w cyfrowej dekadzie” (Dz.U. C 23 z 21.01.2023 r. s. 1) – dalej Deklaracja.
[36] Do wcześniejszych inicjatyw w zakresie rozwoju cyfrowego należą: „Deklaracja z Tallina w sprawie administracji elektronicznej”; „Deklaracja berlińska w sprawie społeczeństwa cyfrowego i administracji cyfrowej opartej na wartościach”; „Deklaracja lizbońska – celowa demokracja cyfrowa”.

sobą ograniczania praw. Po drugie, to, co jest nielegalne poza internetem, jest również nielegalne w internecie. Po trzecie, transformacja cyfrowa musi pozostawać bez uszczerbku dla „polityk niecyfrowych", takich jak dostęp do kluczowych usług publicznych poza internetem. Po czwarte, transformacja cyfrowa musi odbywać się z zapewnieniem pełnej zgodności z prawami podstawowymi, takimi jak ochrona danych, prawo do prywatności, niedyskryminacja i równouprawnienie płci. Po piąte, konieczne jest zapewnienie neutralności technologicznej, neutralności sieci oraz wiarygodności i inkluzywności[37].

Analiza postanowień Deklaracji pozwala stwierdzić, że Unijna wizja transformacji cyfrowej ukierunkowana jest na człowieka. W rozdziale 1 pkt 1 Deklaracji wskazano, że w transformacji cyfrowej w Unii Europejskiej najważniejszy jest człowiek. Technologia powinna służyć i przynosić korzyści wszystkim ludziom mieszkającym w UE oraz umożliwiać im w pełni bezpieczną realizację ich aspiracji przy jednoczesnym poszanowaniu ich praw podstawowych. Za podstawowy cel w Deklaracji postawiono zapewnienie poszanowania w internecie praw jednostek i wartości uznanych w prawie UE. Technologia powinna być wykorzystywana do łączenia ludzi, a nie do ich dzielenia. Powinna sprzyjać sprawiedliwemu i integracyjnemu społeczeństwu oraz sprawiedliwej i inkluzywnej gospodarce w UE[38].

Na szczególną uwagę zasługuje wyrażona w Deklaracji zasada inkuzywności. Zakłada ona, że transformacja powinna być korzystna dla wszystkich, zapewniać równość płci oraz obejmować w szczególności osoby starsze, osoby mieszkające na obszarach wiejskich, osoby z niepełnosprawnościami lub osoby marginalizowane, podatne na zagrożenia lub pozbawione praw obywatelskich. Powinna również propagować różnorodność kulturową i językową. W Deklaracji wskazano również, że ważnym

[37] Inkluzywność to koncepcja, która zakłada tworzenie środowiska, w którym każdy człowiek – bez względu na tożsamość, płeć, zdolności, pochodzenie i cechy – jest akceptowany i doceniany. Jest to podejście, które dąży do eliminacji barier i dyskryminacji, a także do promowania równości, różnorodności i integracji we wszystkich aspektach życia społecznego, edukacyjnego, zawodowego i kulturowego: http://akademiaintelektu.org/Inkluzywność - co to oznacza i dlaczego jest tak ważna? - Akademia Intelektu - nowoczesne centrum edukacji (dostęp: 25.11.2024 r.).

[38] M. Nowikowska, *Digital identity on the internet – challenges and threats*, [w:] Wielowymiarowość cyberbezpieczeństwa, J. Żylińska, K. Huczek, K. Borkowski (red.), Warszawa 2024, s. 25 i n.

elementem w transformacji cyfrowej jest infrastruktura. Wszyscy obywatele UE powinni mieć dostęp do przystępnej cenowo i szybkiej łączności cyfrowej.

W Deklaracji *expressis verbis* odniesiono się również do zagadnienia tożsamości cyfrowej. W rozdziale 2 pkt 7 Deklaracji podkreślono, że każdy powinien mieć dostęp online do kluczowych usług publicznych w UE. Istotne jest zapewnienie obywatelom UE możliwości dobrowolnego skorzystania z dostępnej, bezpiecznej i godnej zaufania tożsamości cyfrowej, która pozwala na dostęp do szerokiego wachlarza usług online. Bardzo ważne jest wspieranie płynnego, bezpiecznego i interoperacyjnego dostępu w całej UE do cyfrowych usług publicznych zaprojektowanych z myślą o skutecznym zaspokajaniu potrzeb obywateli, w tym w szczególności do cyfrowych usług zdrowotnych i opiekuńczych, dostępu do elektronicznej dokumentacji medycznej.

Z punktu widzenia tożsamości cyfrowej ważne jest zapewnienie bezpieczeństwa oraz ochrona prywatności i danych osobowych[39]. W rozdziale V Deklaracji poświęconym bezpieczeństwu wskazano, że każdy powinien mieć dostęp do technologii, produktów i usług cyfrowych, które z założenia są bezpieczne, gwarantują ochronę prywatności, aby zapewnić wysoki poziom poufności, integralności, dostępności i autentyczności przetwarzanych informacji[40]. Założenie to obejmuje wymogi w zakresie cyberbezpieczeństwa dla produktów wprowadzanych do obrotu na jednolitym rynku cyfrowym. W pkt. 17 Deklaracji podkreślono ponadto, że każdy ma prawo do prywatności i do ochrony swoich danych osobowych. Ochrona ta obejmuje kontrolę sprawowaną przez ludzi nad tym, w jaki sposób ich dane osobowe są wykorzystywane i komu są udostępniane[41].

Innym istotnym dokumentem w obszarze rozwoju tożsamości cyfrowej jest program Rady „Droga ku cyfrowej dekadzie”[42] opisujący transformację cyfrową UE do 2030 r.

---

[39] M. Nowikowska, *Identity Theft. Protection of Personal Data in Cyberspace*, [in:] Digital well-being – a concern for the quality of life, L. Tafaro, I. Laki, I. Florek (eds.), Warsaw-Budapest 2023, s. 154.
[40] Zob. K. Chałubińska-Jentkiewicz, M. Nowikowska, *Bezpieczeństwo, tożsamość, prywatność*..., s. 41.
[41] Zob. K. Chałubińska-Jentkiewicz, M. Nowikowska, *Artificial Intelligence v. Personal Data*, „Polish Political Science Yearbook”, 2022, vol. 51(3), p. 185; M. Safjan, *Ochrona danych osobowych – granice autonomii i informacji*, [w:] Ochrona danych osobowych, M. Wyrzykowski (red.), Warszawa 1999, s. 9; M. Nowikowska, *Personal Data Protection in the Context of the Act on the National Cybersecurity System*, [in:] Cybersecurity in Poland. Legal Aspects, K. Chałubińska-Jentkiewicz, F. Radoniewicz & T. Zieliński (eds.), Springer Cham 2022, s. 171.
[42] “Program Droga ku cyfrowej dekadzie” z 8 grudnia 2022 r.: https://www.consilium.europa.eu/pl/infographics/digital-decade/ (dostęp: 19.08.2024).

Określono w nim cele cyfrowe oparte na czterech głównych punktach: 1) umiejętności cyfrowe, 2) infrastruktura cyfrowa, 3) cyfryzacja przedsiębiorstw i 4) usług publicznych). Podstawowym celem UE do 2030 r. jest stworzenie inkluzywnego środowiska cyfrowego ukierunkowanego na człowieka. W Programie wskazano, że w 2019 r. około 56% osób w wieku od 17-74 lat posiadało podstawowe umiejętności cyfrowe. UE wyznaczyła do 2030 r. wzrost tego wskaźnika do poziomu 80%. Podobnie do 2030 r. UE chce zapewnić 100% dostęp do infrastruktury, tj. zagwarantowania w każdym obszarze (miejskim i wiejskim) połączeń gigabitowych i dostępu łączności 5G. W Programie wskazano także, że w 2020 r. 60% obywateli korzystało z identyfikacji elektronicznej. Za cel UE stawia sobie podwyższenie tego wskaźnika do poziomu do 80% wszystkich obywateli UE.

11 kwietnia 2024 r. Parlament Europejski i Rada przyjęły rozporządzenie 2024/1183 w sprawie zmiany rozporządzenia (UE) nr 910/2014 w odniesieniu do ustanowienia europejskich ram tożsamości cyfrowej[43] (tzw. eIDAS 2). W punkcie 5 preambuły wskazano, że obywatele powinni mieć prawo do tożsamości cyfrowej, która podlega ich wyłącznej kontroli i która umożliwia im korzystanie ze swoich praw w środowisku cyfrowym oraz uczestnictwo w gospodarce cyfrowej. Ramy tożsamości cyfrowej powinny przyczyniać się do bardziej zintegrowanej cyfrowo Unii poprzez zmniejszanie barier cyfrowych między państwami członkowskimi i umożliwianie obywatelom Unii czerpania korzyści z cyfryzacji, przy jednoczesnym zwiększaniu przejrzystości i ochrony ich praw.

Ustawodawca unijny na mocy eIDAS 2 wprowadził Europejskie Portfele Tożsamości Cyfrowej (ang. *The EU Digital Wallet*, EUDIW**)**. Portfel tożsamości cyfrowej jest produktem i usługą, które umożliwiają użytkownikowi przechowywanie danych dotyczących tożsamości, danych uwierzytelniających i atrybutów powiązanych z jego tożsamością, dostarczanie ich na żądanie stronom ufającym oraz wykorzystywanie ich do uwierzytelniania online i offline na potrzeby usługi. Przykładem tożsamości cyfrowej jest elektroniczny dowód osobisty, paszport, czy prawo jazdy. Europejską tożsamość cyfrową można wykorzystywać zarówno online, jak i offline, w publicznych i prywatnych usługach w całej UE[44].

[43] Dz.U. UE L, 30.04.2024.
[44] http:// digital-strategy-ec.europa.eu/pl/policies/eudi-wallet-implementation (dostęp: 23.02.2024).

Wskazuje się, że wdrożenie ram europejskiej tożsamości cyfrowej może przynieść następujące korzyści:

- każda osoba, która ma prawo do otrzymania krajowego dokumentu tożsamości, ma również prawo do posiadania tożsamości cyfrowej uznawanej w całej UE;
- portfel tożsamości stanowi prosty i bezpieczny sposób na kontrolowanie tego, jakie informacje chcemy podać serwisom, które udostępniają usługi i wymagają udostępnienia informacji;
- tożsamość cyfrowa, dostępna za pośrednictwem cyfrowych portfeli w aplikacjach mobilnych na telefony komórkowe oraz na innych urządzeniach, ma na celu umożliwienie potwierdzenie tożsamości online i offline, przechowywanie i wymianę informacji przekazanych przez urzędy, np. imię, nazwisko, data urodzenia, obywatelstwo, przechowywanie i wymianę informacji pochodzących z wiarygodnych źródeł prywatnych oraz wykorzystywanie tych informacji do udowodnienia swojego prawa, np. do pobytu, pracy lub studiów w danym państwie członkowskim[45].

Podsumowując powyższe można stwierdzić, że Unijna droga do transformacji cyfrowej obejmuje w szczególności suwerenność cyfrową, poszanowanie praw podstawowych, praworządności i demokracji, włączenie społeczne (poprzez zapewnienie łączności, edukację cyfrową, szkolenia, uczciwe i sprawiedliwe warunki pracy, dostęp do cyfrowych usług publicznych online), zrównoważony rozwój, bezpieczeństwo, poprawę jakości życia, dostępność usług oraz poszanowanie praw i aspiracji wszystkich osób. Oprócz korzyści, jakie daje tożsamość cyfrowa, niesie ona z sobą także wiele wyzwań i zagrożeń. Wiąże się ona również z licznymi wyzwaniami, wśród których najważniejsze jest bezpieczeństwo w Internecie.

Tożsamość cyfrowa jako prawo obywatela do dostępu do technologii, produktów i usług cyfrowych

Ustawodawca unijny w rozporządzeniu 2024/1183 w pkt 5 posłużył się zwrotem „prawa obywateli do tożsamości cyfrowej", które stanowi warunek *się qua non*

[45] https:// commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity (dostęp: 15.04.2024).

wykonywania praw w środowisku internetowym. Prawo do tożsamości cyfrowej wyraża się w prawie do dostępu do technologii, produktów i usług cyfrowych. Tożsamość cyfrowa w społeczeństwie informacyjnym staje się kluczowym elementem, który pozwala jednostce na interakcję z usługami i produktami online[46]. Można uznać, że tożsamość cyfrowa stanowi zestaw informacji i danych, które identyfikują jednostkę w przestrzeni cyfrowej, a jej posiadanie staje się niezbędne do korzystania z produktów i usług w sieci.

Tożsamość cyfrowa staje się kluczowym elementem, który decyduje o dostępie do produktów i usług w sieci. Aby prawo to mogło być zrealizowane, niezbędny jest dostęp do technologii. Osoby, które nie mają dostępu do odpowiednich technologii, np. internetu, mogą zostać wykluczone z dostępu do usług wymagających tożsamości cyfrowej.

Ponadto należy stwierdzić, że tożsamość cyfrowa pełni rolę „klucza", który otwiera drzwi do produktów i usług w cyfrowym świecie. Aby uzyskać ten dostęp, użytkownik musi przejść proces weryfikacji swojej tożsamości. Jako przykład można wskazać dostęp do usług bankowych. Bank, przed umożliwieniem dostępu do konta, przelewów czy transakcji online, będzie wymagał uwierzytelnienia tożsamości użytkownika.

Podsumowanie

Tożsamość cyfrowa jest kluczowym elementem współczesnej rzeczywistości cyfrowej, umożliwiającym dostęp do produktów i usług, za pośrednictwem nowych technologii. Identyfikacja tożsamości cyfrowej pozwala nam udowodnić, kim jesteśmy w sieci. Analiza dokumentów unijnych pozwala stwierdzić, że ustawodawca określa tożsamość cyfrową jako prawo obywatela do realizowania się w środowisku internetowym, które pozwala jednostce na interakcję z usługami i produktami online. Wskazuje się, że identyfikacja cyfrowa pomaga zaoszczędzić czas i uprościć interakcje. Różni dostawcy prywatni i publiczni oferują obecnie różne środki identyfikacji cyfrowej, z różnym stopniem wiarygodności i bezpieczeństwa. Ustawodawca Unijny, dostrzegając zalety zharmonizowano we wszystkich państwach członkowskich modelu portfela

[46] K. Markiewicz, *Rozwój społeczeństwa informacyjnego*, [w:] Bezpieczny rozwój społeczeństwa informacyjnego, E. Szczepaniuk, M. Gawlik-Kobylińska, J. Werner, Warszawa 2016, s. 177; J. Dzierżyńska-Mielczarek, *Rynek mediów w Polsce*, Warszawa 2018, s. 75.

tożsamości cyfrowej, wskazuje, że rozwiązanie to umożliwi użytkownikom cyfrowe udowodnienie, kim są, a jednocześnie zapewnią im pełną kontrolę nad tym, jakie dane udostępniają, aby utożsamiać się z usługami internetowymi.

Przeprowadzone rozważania wskazują, że pojęcie tożsamości cyfrowej jest zagadnieniem złożonym. Z jednej strony tożsamość cyfrowa staje się nieodzownym atrybutem funkcjonowania jednostki w cyberprzestrzeni. Z drugiej, niesie ze sobą wiele zagrożeń. Przed ustawodawstwem unijnym stoi wiele wyzwań. Chcąc rozwijać ramy europejskiego portfela tożsamości cyfrowej i dostrzegając korzyści płynące z nowych technologii, równocześnie należy wprowadzać mechanizmy, które będą skutecznie zabezpieczać i chronić jednostkę w sieci.

Bibliografia

Chałubińska-Jentkiewicz K., Nowikowska M., *Artificial Intelligence v. Personal Data*, „Polish Political Science Yearbook" 2022, vol. 51(3).

Chałubińska-Jentkiewicz K., Nowikowska M., *Bezpieczeństwo, tożsamość, prywatność – aspekty prawne*, Warszawa 2020.

Coomaraswamy R., *Identity within: Cultural Relativism, Minority Rights and the Empowerment of Women*, **„The George Washington International Law Review" 2002, vol. 34, no. 3.**

Domańska M., *Zakaz dyskryminacji ze względu na więcej niż jedno zabronione kryterium*, Warszawa 2019.

Dzierżyńska-Mielczarek J., *Rynek mediów w Polsce*, Warszawa 2018.

Flis M. (red.) *Etyczny wymiar tożsamości kulturowej, Studia z antropologii społecznej*, Warszawa 2004.

Markiewicz K., *Rozwój społeczeństwa informacyjnego*, [w:] *Bezpieczny rozwój społeczeństwa informacyjnego*, E. Szczepaniuk, M. Gawlik-Kobylińska, J. Werner, Warszawa 2016.

Nowikowska M., *Digital identity on the internet – challenges and threats*, [w:] *Wielowymiarowość cyberbezpieczeństwa*, J. Żylińska, K. Huczek, K. Borkowski (red.), Warszawa 2024.

Nowikowska M., *Identity Theft. Protection of Personal Data in Cyberspace*, [in:] *Digital well-being – a concern for the quality of life*, L. Tafaro, I. Laki, I. Florek (eds.), Warsaw-Budapest 2023.

Nowikowska M., *Personal Data Protection in the Context of the Act on the National Cybersecurity System*, [in:] *Cybersecurity in Poland. Legal Aspects*, K. Chałubińska-Jentkiewicz, F. Radoniewicz & T. Zieliński (eds.), Springer Cham 2022.

Nowikowska M., *Prawo do wizerunku i prawo adresata korespondencji*, [w:] *Prawo własności intelektualnej. Teoria i praktyka*, J. Sieńczyło-Chlabicz (red.), Warszawa 2021.

Poźniak-Niedzielska M., *Ograniczenie praw autorskich do wizerunku, korespondencji i źródeł in*formacji [w:] *Prawo autorskie i prawa pokrewne. Zarys wykładu*, M. Poźniak-Niedzielska (red.), Bydgoszcz 2006.

Poźniak-Niedzielska M., Szczotka J., *Prawo autorskie. Zarys problematyki*, Warszawa 2020.

Safjan M., *Ochrona danych osobowych – granice autonomii i informacji*, [w:] *Ochrona danych osobowych*, M. Wyrzykowski (ed.), Warszawa 1999.

Wojnicka E., *Prawo do wizerunku w ustawodawstwie polskim*, „Zeszyty Naukowe Uniwersytetu Jagiellońskiego PWiOWI 1990, nr 56.

Wspólne deklaracje Parlament Europejski, Rada, Komisja Europejska „Europejska deklaracja praw i zasad cyfrowych w cyfrowej dekadzie” (Dz.U. C 23 z 21.01.2023 r. s. 1).

„dot.pl" - czasopismo Rejestru domeny .pl

Tackling disinformation in the EU with "Truthster": technological design and DLT

Federico Costantini
University of Udine, Department of Law, Via Treppo 18, 33100 Udine (IT),
ORCID: https://orcid.org/0000-0003-2168-5523
E-mail: federico.costantini@uniud.it

Francesco Crisci
University of Udine, Department of Economics, Via Tomadini 30/A, 33100 Udine (IT),
ORCID: http://orcid.org/0000-0003-2563-9612
E-mail: francesco.crisci@uniud.it

Silvia Venier
Institute of Law, Politics, Development (DIRPOLIS), Scuola Superiore Sant'Anna,
E-mail: silvia.venier@santannapisa.it

Stefano Bistarelli
Department of Computer Science, University of Perugia,
ORCID: https://orcid.org/0000-0001-7411-9678
E-mail: stefano.bistarelli@unipg.it

Ivan Mercanti
Department of Computer Science, University of Perugia,
ORCID: https://orcid.org/0000-0002-9774-1600
E-mail: ivan.mercanti@unipg.it

Received: 08.04.2024
Accepted: 19.05.2024
Published: 27.05.2024

Cite this article as:
F. Costantini, F. Crisci, S. Venier, S. Bistarelli, I. Mercanti, "Tackling disinformation in the EU with "Truthster": technological design and DLT"

DOT.PL, no. 1/ 2024,
10.60097/DOTPL/189285

Corresponding author:
Federico Costantini,
University of Udine, Department of Law, Italy
E-mail:
federico.costantini@uniud.it

Abstract

Tackling disinformation is crucial for the development of the Information Society. To do this, it is necessary to empower journalists in the production of trustworthy information, and to nurture an economic ecosystem centred on the secure circulation of content. In this

contribution we present an interdisciplinary approach that aims (1) to find a balance between freedom of expression and other fundamental rights (e.g., privacy and data protection), (2) to develop business models driven by the production of genuine content, and (3) to exploit the potential of distributed ledger systems to provide media certification.

Keywords: Blockchain, TruBlo, Fake news, Trust, Freedom of expression, Journalism

Introduction[47]

An overview: From "truth" and "authority" to "trustworthiness" and "governance".

Truth is a basic human need from a threefold perspective: (1) individually, as a matter of a personal spiritual quest, (2) socially, as a base for trusted personal and economic relations, and (3) politically, as an inevitable requirement for consent in the fair exercise of public power. Conversely, disinformation is as old as human society. In this sense, as regards interpersonal relations, it might be recalled that in the culture of ancient Greece – the cradle of western civilization – popular rumour (*Pheme*) was already distinguished from slander (*Sychophantia*) and malice (*Diabolé*, which was embodied as a goddess). As for the institutional aspect, the exploitation of misleading information has always been valued as an asset, both in critical times – from the Chinese classic *The Art of War* we can quote the imperishable statement "*all warfare is based on deception*"[48] – and as a privileged tool for the ordinary exercise of power by a sovereign.[49]

As we know the Information Society[50] means that the transmission of messages and the broadcasting of news is achieving unprecedent speed and magnitude.[51] The uptake in the

[47] This contribution is the result of joint research of the co-authors. Individual contributions can be attributed as follows: F. Costantini, par. 1 and 5, S. Venier, par. 2, F. Crisci, par. 3, S. Bistarelli and I. Mercanti, par. 4.
[48] S. Tzu, *The art of war* (VI-V b.C.), chapter one.
[49] N. Machiavelli, *De Principatibus* (1514).
[50] J. R. Beniger, *The control revolution: technological and economic origins of the information society,* Cambridge, Mass.: Harvard University Press, 1986.
[51] J. Gleick, *The information: a history, a theory, a flood*, 1st ed. New York: Pantheon Books, 2011.

mass media (the printed press, radio, and television) caused the creation of new enterprises (mass media companies), new marketplaces (advertising) and new professional figures (journalists), while allowing unparalleled concentration in the control of public opinion. As worldwide dictators learned to master the art of media censorship and manipulation,[52] democratic regimes cherished freedom of expression as a means to protect trust in social relations, fair competition among enterprises and fundamental rights of citizens. On the latter aspect, it is noteworthy that continuous efforts are being made by jurisprudence and scholars to update legal concepts and to find the appropriate balance between freedom of expression and other fundamental rights (reputation, privacy, authorship and so on).[53]

The advent of the Internet disrupted the paradigm which had lasted since the end of the eighteenth century. In this sense, the decision by the US Supreme Court in the case of "ACLU / RENO" – in which the Internet was described as "*a wholly new medium of worldwide human communication*"[54] – is symbolic of the foundation of "cyberlaw",[55] the law governing the Internet.[56] In fact, since an indefinite set of heterogeneous resources (e.g. data, services, and applications) is available, is flowing continuously throughout the world and is instantaneously accessible, neither a "centralized" nor a "distributed" approach is feasible for regulating the newly discovered digital continent. For the first of these approaches, the obvious main risk is censorship, which can be perpetrated by private (service providers) as well as public actors (governmental agencies or bodies). Concerning the second, the risk is a global Babel, which leads inevitably to echo chambers, social instability, and institutional uncertainty. Conversely, a "decentralized" approach seems suitable, despite the difficulties in implementing such an approach,[57] because of its flexibility and resilience. It is no coincidence that the same approach was

[52] H. Arendt, *The origins of totalitarianism*, 1st ed. New York: Harcourt, 1951.
[53] S. D. Warren et al., *The Right to Privacy*, "Harvard Law Review 4", no. 5, 1890.
[54] American Civil Liberties Union, Janet Reno, Supreme Court of the United States No. 96–511, 19 March 1997 – 26 June 1997.
[55] L. Lessig, *Code and other laws of cyberspace*, New York: Basic Books, 1999.
[56] M. C. Kettemann, *The Normative Order of the Internet. A Theory of Rule and Regulation Online*, London, Oxford University Press, 2020.
[57] V. Buterin, *The Meaning of Decentralization;* "Medium", 2017). https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274.

chosen by the Internet pioneers for the network architecture which became today's Internet.[58]

Currently, almost thirty years after the decision in the ACLU / RENO case, and after a further wave of innovation in ICT (e.g. social media), it seems that not only does the concept of truth need to be revisited according to new epistemic perspectives, but also that legal provisions alone are inadequate to enforce truth, or even to safeguard it. On the one hand, the concept of "trustworthiness" seems to be more theoretically grounded,[59] flexible[60] and future-proof[61] than that of "truth". On the other, concerns about trustworthiness in communication are strengthened by the exploitation of the potentials of new technologies (e.g. artificial intelligence and "deep fakes").[62] In tackling such issues, legislators at every level have started to adopt a softer approach to regulation, introducing complex governance systems that include three basic components: (1) traditional legal provisions, which offer a uniform framework of general and abstract rules;[63] (2) business models allowing economic sustainability (costs of maintenance and transactions); and (3) a technological infrastructure, combining the general rules of law with the design of an ecosystem that is intended to make resources virtual and to automate processes.[64]

From a theoretical perspective, it seems today that such a model of governance – with the combination of the three components mentioned above – is the most suitable method for regulating a decentralized set of interdependent human communities which rely on a,

---

[58] P. Baran, *On Distributed Communications Networks*, "RAND Corporation papers", Santa Monica, California, 1962.

[59] E. Gettier, *Is Justified True Belief Knowledge?,* "Analysis", 23, no. 6, 1963.

[60] N. Luhmann, *Vertrauen: ein Mechanismus der Reduktion sozialer Komplexitaet*, "Soziologische Gegenwartsfragen", N. F., Stuttgart: F. Enke, 1968.

[61] S. O. Funtowicz et al., *Uncertainty and quality in science for policy*, "Theory and decision library", Series A. Philosophy and methodology of the social sciences, Dordrecht; Norwell: Kluwer Academic Publishers, 1990.

[62] M. Coeckelbergh, *Democracy, epistemic agency, and AI: political epistemology in times of artificial intelligence*, "AI Ethics", 2022, https://doi.org/10.1007/s43681-022-00239-4, https://www.ncbi.nlm.nih.gov/pubmed/36466152.

[63] U. Pagallo et al., *The middle-out approach: assessing models of legal governance in data protection, artificial intelligence, and the Web of Data*,"The Theory and Practice of Legislation", 2019, https://doi.org/10.1080/20508840.2019.1664543.

[64] M. Craglia et al., *Digitranscope. The governance of digitally-transformed society,* Luxembourg: UR 30590 EN, Publications Office of the European Union, 2021. https://publications.jrc.ec.europa.eu/repository/handle/JRC123362;
A. Theodorou et al., *Towards ethical and socio-legal governance in AI*,"Nature Machine Intelligence", 2, no. 1, 2020, https://doi.org/10.1038/s42256-019-0136-y.

likewise decentralized, worldwide network to survive and flourish as peacefully as possible. This approach is adopted even at the EU level, as confirmed by many recently adopted (e.g. the Digital Markets Act[65] and the Digital Services Act[66]), or soon to be enacted (e.g. the "AI Act"[67] and the "Cyber Resilience Act"[68]), provisions.

Tackling online disinformation in the EU: A holistic approach

The fact that our democratic societies depend strongly on the ability to produce, share and consume trustworthy information from a wide variety of sources is particularly acknowledged by the European Commission, which – in its Communication on *Tackling online disinformation: a European approach* – has defined disinformation as "*verifiably false or misleading information that is created, presented and disseminated for economic gain or to intentionally deceive the public, and may cause public harm. Public harm comprises threats to democratic political and policy-making processes as well as public goods such as the protection of EU citizens' health, the environment or security*".[69] While, on the one hand, democracy in Europe rests on the existence of free and independent media, on the other, ICT is profoundly changing the way in which traditional and new media produce and distribute information, and the ways in which users are engaged in the dissemination of information. In other words, it is not only governments and digital platforms, but each media creator, who is in the forefront of the battle against disinformation, and every user can be held hostage by propaganda.

In order to address this issue, the EU institutions released a *Code of Practice on Disinformation* in 2018,[70] and this was revised in 2022 with the *EU Strengthened Code of*

[65] Regulation (EU) 2022/1925 of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act), OJ L 265, 12.10.2022, p. 1–66, ELI: http://data.europa.eu/eli/reg/2022/1925/oj

[66] Regulation (EU) 2022/2065 of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act), OJ L 277, 27.10.2022, p. 1–102, ELI: http://data.europa.eu/eli/reg/2022/2065/oj

[67] Proposal for a Regulation laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain union legislative acts, COM/2021/206 final https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52021PC0206

[68] Proposal for a Regulation on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020, COM/2022/454 final, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022PC0454.

[69] COM(2018) 236 final, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018DC0236.

[70] https://digital-strategy.ec.europa.eu/en/library/2018-code-practice-disinformation.

Practice on Disinformation.[71] The aim of this initiative is to encourage stakeholders to adopt a set of measures to empower content creators and users by ensuring the safe design of the architecture of their systems and by providing them "*with tools to assess the provenance and edit history or authenticity or accuracy of digital content*". We can argue that this document confirms that an approach resulting from the combination of legal provisions, economic balances and technological tools is valued as a viable strategy even in this specific field. However, designing an abstract model, despite the positive reception, and even wide adoption, by stakeholders, is not sufficient to eradicate disinformation, because of the different causes, the many modes, the heterogeneous actors, and the impact of this phenomenon. For this reason, the EU is committed to fostering the development of new methods and tools to contain the spread of disinformation, and to financing research and innovation projects.[72]

Outline of the contribution: Presenting the "TRUTHSTER" project

In this contribution we present the background research for the "TRUTHSTER" project which, in our view, can be considered to be not only an example of the actions put in place by the EU aimed at tackling disinformation but also a paradigm for the approach adopted by the EU institutions.[73] Indeed, as we will explain below, we envisage an ecosystem composed of three pillars: (1) a set of legal rules deriving from both legislation and private agreements, (2) a sustainable business model based on an "open innovation" paradigm, and (3) a digital platform based on distributed ledger technologies which is intended to avoid, *by design*, both a centralized monopoly over media production and a lack of control of its circulation. Furthermore, our driving concept is that trustworthiness in information can be better pursued by empowering individual media creators in their effort to build trust in their own professionality. Hence, the practical outcome of TRUTHSTER is a tool – a mobile application – which, it is intended, will integrate a "proof of validity" of digital media generated from a journalist's device before it is shared, and will focus on content

[71] https://digital-strategy.ec.europa.eu/en/library/2022-strengthened-code-practice-disinformation.
[72] Joint Communication, Action Plan against Disinformation, JOIN/2018/36 final, https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:52018JC0036.
[73] L. Floridi, ed., *The Onlife Manifesto. Being Human in a Hyperconnected Era*, Open Access , Cham: Springer International Publishing, 2015.

whose creation process requires interaction with another human actor (mainly video interviews, audio recordings, and photos). In the process, a customized disclosure notice, containing the terms and conditions regulating the media release, would automatically be sent to the interviewee, thus acknowledging her/his fundamental rights (primarily, privacy).

In the following paragraphs we will address each pillar separately. In section 2 we give the outline of the legal framework, focusing on the specific concerns that media creators – primarily journalists, influencers, and digital entrepreneurs in general – need to address when balancing freedom of entrepreneurship and of expression with rights to privacy and data protection. In section 3 we briefly describe the proposed business model and in section 4 we provide an overview of the technologies to be deployed. At the end we offer a few final remarks.

The legal pillar: Balancing rights and protecting their core

Fundamental rights represent the overall architecture that underpins information sharing in our democratic societies. In particular, the right of freedom of expression represents the cornerstone of the activity of journalists.[74] Indeed, according to the European Convention on Human Rights (ECHR), journalists, as well as NGOs, bloggers and scholars, are the "watchdogs" of public opinion, thus benefiting from special protection (Article 10 ECHR). Consequently, public authorities are not allowed to restrict the freedom to investigate, and to report and comment on, all matters of public interest.[75] In order to obtain this increased protection, journalists are expected to comply with the duties and responsibilities connected with their role. For instance, while the ECHR states that journalists are not required to verify official sources in reporting news released by them, the professional responsibility of journalists entails a requirement to validate information to a reasonable extent before releasing it publicly. In the case of an interview

[74] As recognised by the Universal Declaration of Human Rights (article 19), the European Convention on Human Rights (article 10) and the Charter of Fundamental Rights of the European Union (article 11).

[75] On the role of the press, see e.g. ECtHR in Affaire Campos Dâmaso C. Portugal, § 30; on academic researchers see Başkaya and Okçuoğlu v. Turkey [GC], §§ 61-67; on the role of bloggers and popular users of social media as watchdogs, see e.g. ECtHR *Magyar Helsinki Bizottság v. Hungary* [GC], § 168.

published in a newspaper, however, some differences have been drawn between the transcription of the interviewee's statement and the journalist's own declarations.[76]

As observed above, freedom of expression needs to be balanced with others fundamental rights. This balance becomes more difficult in the digital realm, since on the Internet, as stated by the ECtHR, it is not only that the risks are generally considered to be higher than those related to the traditional press,[77] but also that a new kind of threat has emerged, thus requiring new remedies. This is confirmed by the "right to be forgotten", which can be claimed only against online search engines and media web archives[78] and not against newspapers and the traditional media in general. Furthermore, the fact that fundamental rights are embodied not only in international treaties and legislation but also in secondary sources of law creates interpretative nuances and exceptions, increasing uncertainty for professionals, and thus *de facto* hindering their freedom. As we know, Regulation (EU) 679/2016 (henceforth the "GDPR")[79] establishes specific rights for data subjects and obligations for data processors and controllers. Interestingly, pursuant to Article 85 GDPR and Recital 153, Member States are entitled to provide derogations or exemptions – which must be notified to the EU Commission – to adapt the application of data protection in the field of journalistic production. Pursuant to this clause, for example, the Data Protection Supervisor in Italy has enacted a "*Professional Code*" for journalists,[80] according to which a reporter is required to disclose her or his qualification when collecting news in order to benefit from the exemption from Articles 13 and 14 of the GDPR (the duty to provide information to a data subject). The perverse consequence of this measure, whose aim was to simplify practical duties, is that the status of journalists is weakened since, once they release information – and share, once for all, the personal

---

[76] See Case of Kącki v. Poland § 52.

[77] See ECtHR, Guide on data protection (2022), para 369 ff, available at https://rm.coe.int/guide-data-protection-eng-1-2789-7576-0899-v-1/1680a20af0

[78] See in particular the groundbreaking judgment of the Court of Justice of the EU (CJEU) in Google Spain (2014), Case 131/12 Google Spain SL and Google Inc. v Agencia Espanola de Proteccio´n de Datos (AEPD) and Mario Costeja Gonza´lez v AEPD. See also ECtHR, Guide on data protection (2022), para 280-282.

[79] Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, in OJ L 119, 4.5.2016, p. 1–88, ELI: http://data.europa.eu/eli/reg/2016/679/oj.

[80] Regole deontologiche relative al trattamento dei dati personali nell'esercizio dell'attività giornalistica" (G.U. del 4 gennaio 2019, n. 3), https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9067692

data they collect – they are exposed to legal claims concerning media authorship, consent, personal image and so on, without having any means of defence.

In general, when media reports directly involve persons of interest (e.g., in an interview), their consent for using their personal data or their personal image (e.g., protected materials) can represent a critical requirement, since field reporters are inclined to avoid the practical inconvenience of collecting a documented expression of will (particularly if this is expected to be on paper). Currently, professional media creators lack effective protection to ensure (1) the genuine nature of information sources, (2) the integrity of the content that is produced, and (3) compliance with legal requirements (laws, bylaws, and professional codes of practice) throughout the process of collecting and publishing information. On their part, those who are directly involved in the production of content (e.g., respondents in interviews) are unable to control their own data once the news is spread, or are unaware of their own rights or are incapable of exercising them, or, often, lack the capacity to raise legal claims and request restoration.

The design concepts of the TRUTHSTER application are aimed at addressing such legal issues; specifically: (1) the interview should not be released without the consent of the interviewee; (2) it should be easy for the interviewer to request the consent of the interviewee; (3) the certification of the media content should be activated by the same simple gesture of the interviewee as that by which her/his consent is expressed; (4) the certification of the media content should include any relevant data (embedded as metadata), and should be performed by a decentralized platform to avoid censorship or manipulation; and (5) the documentation of the interaction and of the certification should be available for both the interviewer and the interviewee.

The economic pillar: Entrepreneurial innovation

The project proposes a formula for entrepreneurial innovation that seeks to go beyond the traditional distinctions of the innovation process, underpinning innovation in the dimension of cultural entrepreneurship (the evolution of the digital media creation

culture).[81] The proposed business model feeds an alternative socio-cultural dimension into the dominant professional and work models in the traditional news media sector. It is possible to trigger, or at least to nurture, processes of institutional and organizational change in the traditional formulas for the organization of work (in the information chain and in the functioning of newsrooms) and in the management of the journalistic profession.

The characteristic aspects of the TRUTHSTER project's business solution are the concept of entrepreneurial innovation (new organizational forms and innovative business models designed in a coherent manner) and the use of platforms as "relational infrastructures" based on the "participatory culture" of data journalism as a social and cultural phenomenon. Likewise, in the digital maker movement, "Arduino"[82] is at the same time (1) a digital prototyping board (a "digital artefact"), (2) an entrepreneurial model focused on entrepreneurial learning and entrepreneurial innovation practices, and (3) a collective platform for creatives and innovators who are focused on the community and culture of digital makers.

In short, the solution envisaged by the TRUTHSTER project, in terms of its business model and organizational design, is economically sustainable only if its "participatory" dimension and its "membership" mechanism simultaneously feed the three components of the ecosystem: (1) the continuous production of open source applications and tools (especially by professional developers and people from the world of academic entrepreneurship); (2) the adoption of such tools to feed the cultural dimension of the data journalism movement; and (3) the development of the platform as an online community of creatives and innovators around the convergence of technologies such as blockchain and artificial intelligence in news media.

The technological pillar: The need for a decentralized platform

The implications of blockchain technologies in the field of human rights have drawn the attention of scholars. On the one side, blockchain promises to facilitate freedom of

[81] M. Goyanes et al., *Value and Intelligence of Business Models in Journalism*, "Journalistic Metamorphosis: Media Transformation in the Digital Age", SBD, vol.70, 2020, pp. 171-184.
[82] https://www.arduino.cc.

expression and to balance this with the protection of the rights to privacy and data protection.[83] However, because of its own decentralized and immutable structure, blockchain may also hamper some limbs of the above-mentioned rights, for instance with respect to ensuring the accountability of data controllers and the full enjoyment of the right to access, modify and delete personal data. Some recommendations to governments, private actors in the digital sectors and stakeholders have been provided by EU national Data Supervisors[84] and by NGOs.[85]

The opportunity offered by blockchain to provide a decentralized system for the validation of content and a clear chain of custody can be relevant in the field of journalism, and several models have been proposed so far.[86] According to Harrison and Leopold, "[*b*]*y providing greater transparency into the lifecycle of content, blockchain could offer a mechanism to restore trust in our digital ecosystem*".[87] Indeed, blockchain can track and verify the origin of news and visual content, as demonstrated by the "News Provenance Project" of the *New York Times* and IBM.[88] Some media corporations and news agencies have started to develop blockchain-based solutions to address specific concerns such as copyright infringements (WordProof[89]), to certify press releases (ANSA check[90]), and

---

[83] *G. Zyskind et al., Decentralizing Privacy: Using Blockchain to Protect Personal Data*, paper presented at the 2015 IEEE Security and Privacy Workshops, 21-22 May 2015.

[84] Commission Nationale Informatique et libertés (CNIL), Blockchain. Solutions for a responsible use of the blockchain in the context of personal data (2018), available at https://www.cnil.fr/sites/default/files/atoms/files/blockchain_en.pdf
For a discussion, see Sonia Daoui et al, GDPR, Blockchain and the French Data Protection Authority: Many Answers but Some Remaining Questions (2018), available at https://stanford-jblp.pubpub.org/pub/gdpr-blockchain-france/release/1

[85] Article 19, Blockchain and Freedom of Expression, 2019, pp. 37-38, available at https://www.article19.org/wp-content/uploads/2019/07/Blockchain-and-FOE-v4.pdf

[86] B. Kim et al., *Journalism Model Based on Blockchain with Sharing Space*,"Symmetry-Basel", vol. 11, no. 1, 2019, https://doi.org/https://doi.org/10.3390/sym11010019;
F. Jurado et al., *Tracking News Stories Using Blockchain to Guarantee their Traceability and Information Analysis*, "International Journal of Interactive Multimedia and Artificial Intelligence" , vol. 6, no. 3, Sep 2020, https://doi.org/10.9781/ijimai.2020.06.003;
M. Sintes-Olivella et al., *Blockchain at the service of quality journalism: the Civil case*, "Profesional De La Informacion", vol. 29, no. 5, 2020, https://doi.org/ARTN e290522 10.3145/epi.2020.sep.22;
L. Teixeira et al., *A New Approach to Crowd Journalism Using a Blockchain-Based Infrastructure*, "Momm 2020: The 18th International Conference on Advances in Mobile Computing & Multimedia, 2020, https://doi.org/10.1145/3428690.3429159.

[87] Kathryn Harrison et al., *How Blockchain Can Help Combat Disinformation*, "Harward Business Review", 2021, https://hbr.org/2021/07/how-blockchain-can-help-combat-disinformation.

[88] https://www.newsprovenanceproject.com.

[89] https://wordproof.com.

[90] https://www.ansa.it/sito/static/ansa_check.html.

even to certify online content for forensic purposes (LegalEye[91]). Furthermore, blockchain-based solutions can offer a different monetization system and incentivize high quality content with smart contracts, which may be used to automate payments for content that has been verified according to predefined quality standards. Smart contracts may represent an alternative to payments that derive from click-at-all-costs models, which are often driven by sensationalized (when not completely fake) content.

We believe that blockchain technology may serve as one of these technical solutions, as it offers a mechanism to enhance trust in the information shared. It can ensure that providers of information are verified and that users' rights can be exercised, as it can securely store the timestamps of a publication and certify the provenance of news stories, thus increasing the reputation of legitimate content producers. Furthermore, smart contracts offer a new, simplified, and automated tool to boost the value chain of trusted information, since they can regulate how information can be created, shared, and consumed (e.g., by managing copyright validation and micropayments).

Our solution is based on three main components: (1) a mobile and web interface for the interviewer, (2) a cloud-ready backend server, and (3) a web app for the interviewee. The user experience is described below. The interviewer will use her/his mobile device to log into the TRUTHSTER application, which identifies her/him and the device itself, after a preliminary KYC procedure. The user is allowed to insert the personal data (e.g. name, address, and contact details) of the interviewee and to configure the legal framework regulating the digital content (including privacy and media release options chosen by the interviewee) before the content is generated. Once the content is recorded, the interviewee is requested (e.g. by an SMS sent to her/him or through scanning a QR code) to interact with the interviewer.

This interaction triggers four events: (1) the calculation of the hash of the file (together with metadata included by the user, such as the identity of the interviewee, and metadata that is recorded automatically, such as the GPS position of the device), (2) the transmission of such data (in a human comprehensible format) to the interviewee for

[91] https://www.legaleye.it.

future reference (e.g. GDPR notice), (3) the upload of the file into a cloud server,[92] and (4) the storage of the hash and metadata on a decentralized platform, which is provided by Alastria,[93] an open-source and permissioned[94] blockchain platform. At the end of the process, the interviewer is notified of its completion.[95] The interface is enriched by other functionalities, such as a navigable history of the interviews stored in the database and other practical tools.

Conclusion

While blockchain is not only a technological innovation but undoubtedly also a social phenomenon, its practical benefits and disadvantages are still under discussion, with "pros" and "cons" which depend on the context of the application (and this context is very wide, ranging from cryptocurrencies to supply chain validation). In our project, the use of a blockchain platform offers the supreme advantage that it allows the theoretical background (the need for decentralized governance to support the trustworthiness of the media) to be aligned with legal requirements (the challenge of protecting fundamental rights in the digital realm) and with sustainability concerns (the interest of the single media creator as a design requirement). In the coming months we are planning to release a White Paper both to showcase the outcome of our research and to demonstrate the validity of our tenets.

Acknowledgement

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No 957228 (see https://www.trublo.eu/ for details).

Reference

Arendt, Hannah. *The Origins of Totalitarianism.* 1st ed. New York: Harcourt, 1951.

[92] MongoDB, https://www.mongodb.com. MongoDB is a document database that builds highly available and scalable internet applications. Its flexible schema is popular among development teams using agile approaches.
[93] https://alastria.io/.
[94] Thanks to Alastria ID, only authorized people (registered interviewers) are allowed to write in the blockchain.
[95] Thanks to the Node.js server that notifies the user when the process is complete.

Baran, Paul. *On Distributed Communications Networks*. Rand Corporation Papers. Santa Monica (California): RAND, 1962.

Beniger, James R. The Control Revolution: Technological and Economic Origins of the Information Society. Cambridge, Mass.: Harvard University Press, 1986.

Buterin, Vitalik. "The Meaning of Decentralization." Medium, 2017. https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274.

Coeckelbergh, Mark. "Democracy, Epistemic Agency, and Ai: Political Epistemology in Times of Artificial Intelligence." *AI Ethics* (Nov 22 2022): 1-10. https://doi.org/10.1007/s43681-022-00239-4. https://www.ncbi.nlm.nih.gov/pubmed/36466152.

Craglia, Massimo, Henk Scholten, Marina Micheli, Jiri Hradec, Igor Calzada, Stevens Luitjens, Jaap Boter, and Marisa Ponti. *Digitranscope. The Governance of Digitally-Transformed Society*. Luxembourg: UR 30590 EN, Publications Office of the European Union, 2021. doi:10.2760/503546. https://publications.jrc.ec.europa.eu/repository/handle/JRC123362.

Floridi, Luciano, ed. *The Onlife Manifesto. Being Human in a Hyperconnected Era*, Open Access. Cham: Springer International Publishing, 2015.

Funtowicz, Silvio O., and Jerome R. Ravetz. *Uncertainty and Quality in Science for Policy*. Theory and Decision Library. Series A. Philosophy and Methodology of the Social Sciences. Dordrecht; Norwell: Kluwer Academic Publishers, 1990.

Gettier, Edmund. "Is Justified True Belief Knowledge?". *Analysis* 23, no. 6 (1963): 121-23.

Gleick, James. *The Information: A History, a Theory, a Flood*. 1st ed. New York: Pantheon Books, 2011.

Goyanes, M., M. Rodriguez-Castro, and F. Campos-Freire. "Value and Intelligence of Business Models in Journalism." [In English]. *Journalistic Metamorphosis: Media Transformation in the Digital Age* 70 (2020): 171-84. https://doi.org/10.1007/978-3-030-36315-4_13.

Harrison, Kathryn, and Amelia Leopold. "How Blockchain Can Help Combat Disinformation." *Harward Business Review* (2021-07-19 2021). https://hbr.org/2021/07/how-blockchain-can-help-combat-disinformation.

Jurado, F., O. Delgado, and A. Ortigosa. "Tracking News Stories Using Blockchain to Guarantee Their Traceability and Information Analysis." [In English]. *International Journal of Interactive Multimedia and Artificial Intelligence* 6, no. 3 (Sep 2020): 39-46. https://doi.org/10.9781/ijimai.2020.06.003.

Kettemann, Matthias C. The Normative Order of the Internet. A Theory of Rule and Regulation Online. London: Oxford University Press, 2020.

Kim, B., and Y. Yoon. "Journalism Model Based on Blockchain with Sharing Space." [In English]. *Symmetry-Basel* 11, no. 1 (Jan 2019). https://doi.org/https://doi.org/10.3390/sym11010019.

Lessig, Lawrence. *Code and Other Laws of Cyberspace*. New York: Basic Books, 1999.

Luhmann, Niklas. *Vertrauen: Ein Mechanismus Der Reduktion Sozialer Komplexitaet*. Soziologische Gegenwartsfragen, N. F. Stuttgart: F. Enke, 1968.

Machiavelli, Niccolò. *De Principatibus*. 1514.

Pagallo, Ugo, Pompeu Casanovas, and Robert Madelin. "The Middle-out Approach: Assessing Models of Legal Governance in Data Protection, Artificial Intelligence, and the Web of Data." *The Theory and Practice of Legislation* (2019): 1-25. https://doi.org/10.1080/20508840.2019.1664543.

Sintes-Olivella, M., E. Xicoy-Comas, and E. Yeste-Piquer. "Blockchain at the Service of Quality Journalism: The Civil Case." [In Spanish]. *Profesional De La Informacion* 29, no. 5 (Sep-Oct 2020). https://doi.org/ARTN e290522 10.3145/epi.2020.sep.22.

Teixeira, L., I. Amorim, A. U. Silva, J. C. Lopes, and V. Filipe. "A New Approach to Crowd Journalism Using a Blockchain-Based Infrastructure." [In English]. *Momm 2020: The 18th International Conference on Advances in Mobile Computing & Multimedia* (2020): 170-78. https://doi.org/10.1145/3428690.3429159.

Theodorou, Andreas, and Virginia Dignum. "Towards Ethical and Socio-Legal Governance in Ai." [In en]. *Nature Machine Intelligence* 2, no. 1 (2020-01 2020): 10-12. https://doi.org/10.1038/s42256-019-0136-y.

Tzu, Sun. *The Art of War*. VI-V b.C.

Warren, Samuel D., and Louis D. Brandeis. "The Right to Privacy." *Harvard Law Review* 4, no. 5 (1890): 193-220.

Zyskind, G., O. Nathan, and A. Pentland. "Decentralizing Privacy: Using Blockchain to Protect Personal Data." Paper presented at the 2015 IEEE Security and Privacy Workshops, 21-22 May 2015.

„dot.pl" - czasopismo Rejestru domeny .pl

Dezinformacja jako narzędzie manipulacji w sieci

Karolina Pięta
Katolicki Uniwersytet Lubelski im. Jana Pawła II,
Katedra Socjologii Bezpieczeństwa i Kryminologii,
Instytut Nauk Socjologicznych, Polska
ORCID: https://orcid.org/0000-0002-9036-8276
E-mail: Karolina.pieta@kul.pl

Received: 08.11.2024
Accepted: 15.11.2024
Published: 18.11.2024

Cite this article as:
K. Pięta, „Dezinformacja jako narzędzie manipulacji w sieci"

DOT.PL, no. 1/ 2024,
10.60097/DOTPL/196011

Corresponding author:
Karolina Pięta
Katolicki Uniwersytet Lubelski
im. Jana Pawła II
E-mail: Karolina.pieta@kul.pl

Streszczenie

Na przestrzeni ostatnich lat obserwujemy *intensywny postęp cyfryzacji i informatyzacji. Rozwój Internetu stworzył przestrzeń w obszarze komunikowania się oraz ułatwił proces przekazywania informacji. Fundamentalnym elementem bezpieczeństwa oraz poczucia braku zagrożenia jest przekazywanie treści zgodnych z prawdą. Coraz częściej jednak można spotkać się z informacjami fałszywymi, które stają się narzędziem manipulacji i dezinformacji w celu błędnego informowania opinii publicznej o różnych ważnych kwestiach życia społecznego. Celem artykułu jest ukazanie problemu dezinformacji jako narzędzia manipulacji, przedstawienie technik dezinformacji które wykorzystywane są w cyberprzestrzeni oraz wskazanie jak skutecznie walczyć z dezinformacją w sieci. Problemem badawczym jest próba odpowiedzi na pytanie czy dezinformacja stanowi*

narzędzie manipulacji użytkownikami w sieci? Metoda badawcza wykorzystana w niniejszym artykule to analiza danych zastanych (desk research) w oparciu o literaturę przedmiotu i dostępne źródła internetowe.

Słowa kluczowe: *dezinformacja, manipulacja, techniki dezinformacji, Internet, cyfryzacja*

Disinformation as a tool of manipulation on the Internet

Abstract

Over recent years, we have observed intensive progress in digitization and computerization. The development of the Internet has created space for communication and facilitated the process of transmitting information. A fundamental element of security and the feeling of lack of threat is providing truthful content. However, more and more often we come across false information, which becomes a tool of manipulation and disinformation in order to falsely inform the public about various important issues of social life. The aim of the article is to present the problem of disinformation as a tool of manipulation, present disinformation techniques that are used in cyberspace and indicate how to effectively fight disinformation online. The research problem is an attempt to answer the question whether disinformation is a tool for manipulating users on the Internet? The research method used in this article is the analysis of existing data (desk research) based on the subject literature and available Internet sources.

Keywords: *disinformation, manipulation, disinformation techniques, Internet, digitization*

Wstęp

Rewolucja cyfrowa, a więc intensywny rozwój informatyzacji, nowoczesnych technologii, oraz szybki postęp technologiczny i cyfryzacja, pozwoliły na ukształtowanie się społeczeństwa informacyjnego, w którym główną rolę odgrywa przede wszystkim wiedza i informacja. Społeczeństwo informacyjne w literaturze przedmiotu definiowane jest jako

społeczeństwo, w którym informacja jest kluczowym elementem społeczno-ekonomicznej działalności i zmian[96]*, jako formacja społeczno-gospodarczą, w której produktywne wykorzystanie zasobu jakim jest informacja oraz intensywna pod względem wiedzy produkcja odgrywają dominującą rolę*[97] *lub jako społeczeństwo, które informacje wytwarza, przechowuje, przekazuje, pobiera i wykorzystuje*[98]*. Powyższe definicje pozwalają zauważyć istotność jaką odgrywa przekaz informacji oraz proces dzielenia się wiedzą w codziennym życiu jednostek w obszarze społecznym, ekonomicznym, kulturowym czy politycznym. Na przestrzeni lat, wraz z rozwojem społeczeństwa informacyjnego, powszechny dostęp do informacji stał się jednym z warunków poczucia bezpieczeństwa, a sama informacja zaczęła być chroniona niczym dobro materialne*[99]*. Obecnie informacja stanowi jeden z odwiecznych składników otaczającego nas świata. Mimo, że informacja jest najmniej namacalna najbardziej ulotna, w dobie ciągle trwającej rewolucji informacyjnej to jednak uznawana jest za główną siłą napędową rozwoju gospodarczego i przede wszystkim postępu cywilizacyjnego*[100]*.*

Obecna rewolucja cyfrowa znacząco wpływa na to, w jaki sposób komunikujemy się i dzielimy informacjami. Przeniesienie masowej komunikacji do sieci gdzie realizuje się większość ludzkich potrzeb prowadzi jednak do wielu zmian i wyzwań, zarówno tych pozytywnych, jak i negatywnych. Komunikacja przez Internet pozwala w prosty, szybki i efektywny sposób, wymieniać informacje z ludźmi na całym świecie. Za pomocą zdjęć, filmów czy wiadomości głosowych informacje przekazywane są w znacznie atrakcyjniejszej formie niż innymi środkami przekazu. Ponadto, miejsca takie jak czaty, fora dyskusyjne czy portale społecznościowe stwarzają możliwości wypowiedzi na

---

96 M. Casey, *Europejska polityka informacyjna. Wyzwania i perspektywy dla administracji publicznej*, Toruń 2001, s. 34.

97 H. Kubicek, *Möglichkeiten und Gefahren der „Informationsgesellschaft"* (cyt. za) M. Goliński, *Społeczeństwo informacyjne: problemy definicyjne i problemy pomiaru*, „Dydaktyka Informatyki", 2004, s. 47.

98 A. W. Tomaszewska, *Społeczeństwo informacyjne – pojęcie, pomiar i stopień rozwoju w Polsce*, [w:] P. Urbanek, *Ekonomia i zarządzanie w teorii i praktyce. Tom 6. Determinanty konkurencyjności przedsiębiorstw, regionów, gospodarek,* Łódź 2013, s. 301.

99 P. Chmielecka, *Zjawisko dezinformacji w komunikacji politycznej na przykładzie imigrantów z Ukrainy – zarys problemu* [w:] D. Boćkowski, E. Dąbrowska-Prokopowska, P. Goryń, K. Gorynia (red.), *Dezinformacja – Inspiracja – Społeczeństwo. Cybersecurity,* Białystok 2022, s. 63.

100 A. M. Kamińska, *Internetowe narzędzia komunikacji, czyli jak zapanować nad chaosem informacyjnym*, „Nowa Biblioteka. Usługi, Technologie Informacyjne i Media", 2017, nr 4 (27), s. 19.

określony temat, wystawiania komentarzy[101] czy dzielenia się doświadczeniami oraz pogłębiania własnej wiedzy. Pozwala to zauważyć, że Internet, jako medium komunikacyjne, sprzyja nawiązywaniu i utrwalaniu kontaktów międzyludzkich oraz ułatwia i przyspiesza przepływ informacji.

Wraz z szerokimi możliwościami jakie oferuje Internet w przepływie informacji, wiedzy i komunikacji warto zwrócić uwagę na coraz popularniejszy problem dezinformacji w sieci, a więc celowe rozpowszechniania treści niezgodnych z prawdą w celu zaburzenia przekazu informacyjnego dla osiągnięcia własnych korzyści. W ostatnich latach zauważono coraz częstsze wykorzystywanie zjawiska dezinformacji w różnego rodzaju środkach masowego przekazu, zwłaszcza jako narzędzia manipulacji, szczególnie przy wykorzystaniu Internetu. Portale społecznościowe, strony internetowe czy fora stanowią idealne miejsce do rozpowszechniania nieprawdziwych informacji, co zaczęto dostrzegać jako poważne zagrożenie zarówno dla społeczeństwa, jak i demokracji[102], gdyż w procesie informacyjnego komunikowania medialnego kluczowe wydaje się być skrupulatne oddzielenie faktów od komentarzy[103], czyli informacji od opinii. Pozwala to odbiorcom na samodzielne formułowanie wniosków na podstawie prezentowanych informacji. Niestety nie zawsze jest to proste do rozróżnienia. Celem artykułu jest ukazanie problemu dezinformacji jako narzędzia manipulacji w sieci, przedstawienie wybranych technik dezinformacji w Internecie oraz wskazanie jak skutecznie walczyć z dezinformacją w dzisiejszym społeczeństwie informacyjnym. W niniejszym artykule postawiono następującą hipotezę badawczą, że dezinformacja w znaczący sposób jest wykorzystywana jako narzędzie manipulacji w sieci. W celu jej weryfikacji zastosowano metodę badawczą jaką jest analiza danych zastanych (desk research) w oparciu o literaturę przedmiotu i dostępne źródła internetowe.

Dezinformacja jako narzędzie manipulacji

101 *Ibidem*.
102 Por. N. Szymańska, *Dezinformacja jako narzędzie manipulacji medialnej,* „Roczniki Studenckie Akademii Wojsk Lądowych", 2023, nr 7, s. 39.
103 *Encyklopedia psychologii*, Wyd. 1, Warszawa 1998, s. 126.

Dezinformacja definiowana jest jako proces celowego i błędnego informowania[104], w którym przekazywana informacja jest nieprawdziwa i brakuje jej rzetelnych oraz prawdziwych treści[105]. Dezinformacja to zjawisko podobne do kłamstwa, ponieważ polega na składaniu fałszywych twierdzeń z zamiarem wprowadzenia w błąd, oszukania lub zmylenia. Charakteryzuje się brakiem prawdomówności i często jest kojarzona z prawdziwymi wydarzeniami. Może jednak wystąpić również w czasie pokoju lub działań wojennych. Dezinformacja może być skierowana do określonej lub wyimaginowanej grupy odbiorców i może zawierać fałszywe lub wprowadzające w błąd stwierdzenia, a także sensacyjne nagłówki mające na celu przyciągnięcie uwagi[106]. Zasadniczym założeniem interpretacyjnym pojęcia dezinformacji jest jej celowość, a więc ostrożne i celowe manipulowanie informacjami w taki sposób, aby odbiorca nie był w stanie prawidłowo ocenić sytuacji. W konsekwencji może to prowadzić do podejmowania przez odbiorców błędnych decyzji na podstawie fałszywych przesłanek. W niektórych przypadkach dezinformacja może przyjąć formę niezamierzoną, co może prowadzić do powstania błędnych interpretacji lub wyciągania fałszywych wniosków z przekazanych informacji przez odbiorcę[107].

Dezinformacja często postrzegana jest jako działanie pomiędzy jednorazowym wprowadzaniem w błąd a ciągłym wpływaniem na opinię publiczną. Wprowadzanie w błąd może być czynnością jednorazową, pragmatyczną i impulsywną, gdzie głównym celem jest osiągnięcia zamierzonego efektu w krótkim czasie poprzez wykorzystanie różnych środków masowego przekazu do wmówienia nieprawdziwych informacji określonej grupie odbiorców. W tym przypadku dezinformacja jest przygotowana w sposób profesjonalny i jest prowadzona systematycznie. Z kolei wpływanie, które może wydawać się mniej zorganizowane i oportunistyczne ma na celu budowanie przede wszystkim długofalowego przekazu, który kształtuje percepcję społeczną w sposób subtelny, ale skuteczny. W tym przypadku dezinformatorzy działają zgodnie z określonym

---

104 A. Markowski, *Wielki słownik poprawnej polszczyzny* (cyt. za) K. Chałubińska-Jentkiewicz, *Dezinformacja jako akt*
agresji w cyberprzestrzeni, "Cybersecurity and Law", 2021, nr 5(1), s. 13.

105 S. Dubisz (red.), *Uniwersalny słownik języka polskiego*, T. 1, Warszawa 2003, s. 60.

106 M. Hetmański, *Społeczny charakter informacji* [w:] B. Chyrowicz (red.), *Społeczeństwo informatyczne. Szansa czy zagrożenie?*, Lublin 2003, s. 10-25.

107 Por. M. Wrzosek, *Dezinformacja jako komponent operacji informacyjnych*, Warszawa 2005, s. 8.

harmonogramem dążąc w sposób skrupulatny do zmiany poglądów, przekonań lub zachowań jednostek, przez co stają się szkodliwi[108] *dla opinii publicznej w kontekście wolności słowa i demokracji. Warto zaznaczyć, że dezinformacja może mieć wymiar strategiczny lub taktyczny*[109]*. Głównym celem wymiaru strategicznego jest systematyczne rozpowszechnianie fałszywych sygnałów informacyjnych albo fabrykowanie przekazu, aby uzyskać nieprawdziwy obraz sytuacji, skutkujący błędną jej oceną. Natomiast jeśli chodzi o dezinformację taktyczną to w swoich założeniach jest ona zbliżona, ale nie tożsama, do wprowadzenia w błąd. Ma ona wciąż walor celowej działalności o charakterze planowym, chociaż jej horyzont czasowy należy rozpatrywać raczej w wymiarze miesięcy niż lat.*[110]

Ze względu na fakt, iż głównym zadaniem dezinformacji jest celowa próba obalenia ogólnie przyjętych koncepcji prawdy[111]*, to stanowi ona idealne narzędzie manipulacji opinią publiczną we wszystkich aspektach życia społecznego. Manipulacja uznawana za celowe procedury i mechanizmy, które umożliwiają sterowanie zarówno myślami, emocjami jak i zachowaniami innych ludzi, którzy nie zdają sobie w pełni lub częściowo z tego sprawy*[112] *może nieść spore konsekwencje w dokonywaniu decyzji przez osoby będące pod wpływem manipulatora. Zwłaszcza, że manipulacja będąca zazwyczaj skrytym działaniem, narzuca także jednostkom lub grupom fałszywy obraz pewnej rzeczywistości*[113]*. Internet bez wątpienia stanowi idealną przestrzeń do manipulacji podmiotami życia społecznego za pomocą działań dezinformacyjnych dotyczących zarówno aspektów społecznych, gospodarczych, kulturowych, jak i politycznych. Należy pamiętać, że niemal wszystko co mówimy, piszemy lub wstawiamy do Internetu, może być odebrane jako działanie manipulacyjne przez innego użytkownika sieci. Z tego też względu istotne wydaje się dążenie w swoich internetowych relacjach do szczerej i otwartej*

108 A. Januszko-Szakiel, *Dezinformacja jako narzędzie manipulacji świadomością* [w:] J. Aksman (red.), *Manipulacja: pedagogiczno-społeczne aspekty*, Kraków 2010, s. 211.

109 K. Żarna, *Wybrane przykłady dezinformacji podczas kampanii wyborczej do Rady Narodowej Republiki Słowackiej w 2023 roku*, "Politeja", 2024, nr 1 (88/2), s. 158.

110 T. Kacała, *Dezinformacja i propaganda w kontekście zagrożeń dla bezpieczeństwa państwa,* „Przegląd Prawa Konstytucyjnego", 2015, nr 2 (24), s. 52.

111 D. McQuail, *Teoria komunikowania masowego* (cyt. za) T. Goban-Klas (red.), *Cywilizacja medialna: geneza, ewolucja, eksplozja,* Warszawa 2007, s. 211.

112 H. Hamer, *Psychologia społeczna*, Warszawa 2005, s. 211.

113 A. Lepa, *Świat manipulacji (*cyt. za) J. Nagi, *Manipulacja jako narzędzie dezinformacji*, „Resovia Sacra", 2019, nr 26, s. 298.

komunikacji, aby choć w małym stopniu zniwelować ryzyko, że nasze wypowiedzi zostaną uznane za manipulacyjne. Zwłaszcza, że manipulacja dotyczy przede wszystkim nie środków, lecz relacji między nadawcą i odbiorcą, a ujawniać się może zarówno w konkretnych zachowaniach jak i działaniach[114]. W konsekwencji manipulacja poprzez dezinformację w znaczny sposób może wpłynąć na ludzi w odniesieniu do ich postaw, wierzeń czy poglądów, co tym samym może prowadzić do fałszywych przekonań, które będą wpływać w sposób trwały na jednostkę.

Wybrane techniki dezinformacji z internecie

Platformy mediów społecznościowych obecnie uznawane są za kluczowe źródła rozpowszechniania dezinformacji, bowiem, w odróżnieniu od portali informacyjnych i profesjonalnych serwisów prasowych, nie działa w nich kontrola sprawdzania udostępnianych komunikatów. Liczba informacji, które pojawiają się na głównym feedzie użytkowników, sprzyja jedynie pobieżnemu przeglądaniu tytułów, bez dokładnego wczytywania się w treść[115], a tym bardziej w weryfikację źródeł. Z tego względu działania o charakterze dezinformacyjnym w przypadku mediów społecznościowych nie muszą być wcale tak trudne. Mimo wszystko należy pamiętać o tym, że aby informacja fałszywa mogła uchodzić za informację sfabrykowaną, która pozwoli na manipulację i dezinformację opinii publicznej, powinna charakteryzować się cechami informacji użytecznej. Do takich cech można zaliczyć między innymi: dokładność – jeśli informacja ma być wartościowa, to musi być dokładna, aby mogła dostarczyć wiarygodnego odzwierciedlenia rzeczywistości; aktualności – należy pamiętać, że użyteczna informacja mająca znamiona dezinformacji powinna być aktualna, a więc powinna być dostępna wtedy, kiedy może być podstawą odpowiednich działań zarządzającego nią. Nie musi to wcale oznaczać, że powinna być dostępna szybko, ponieważ aktualność jest funkcją sytuacji, w jakiej znajduje się zarządzający, a więc sam użytkownik; kompletność – informacja przekazywana do opinii publicznej powinna być kompletna i dostarczać odbiorcy wszelkich potrzebnych mu faktów i szczegółów. Obraz sytuacji powinien być

---

114 J. Bralczyk, *Manipulacja językowa* [w:] Z. Bauer, E. Chodziński (red.), *Dziennikarstwo i świat mediów*, Kraków 2000, s. 249.

115 J. Balcewicz, *Fake News – Dezinformacja w świecie nowych mediów*, NASK Cyber Policy, https://cyberpolicy.nask.pl/fake-news-dezinformacja-w-swiecie-nowych-mediow/, [dostęp dn. 31.10.2024 r.].

pełny i klarowny, aby informacja mogła być użyteczna. Jeśli natomiast informacja jest niepełna, zarządzający nią może sobie wyrobić niedokładny lub zniekształcony obraz rzeczywistości, co może szybko zostać zdemaskowane przez opinię publiczną i potraktowane jako informacja nierzetelna i sfabrykowana; odpowiedniość – informacja odpowiednia to informacja użyteczna dla odbiorcy w zależności od jego konkretnych potrzeb i warunków.[116]

Internet jako przestrzeń pozwalająca na łatwą i szybką komunikację w sieci, jest narażony na szereg działań o charakterze dezinformacyjnym swoich odbiorców, które mogą przybierać różne formy i rodzaje. Do najpopularniejszych technik dezinformacji wykorzystywanych w sieci zalicza się negocjację faktów (nieprawda nie do stwierdzenia) – głoszenie oczywistej nieprawdy, jednak przy założeniu, że nie ma świadków i nie ma sposobu na to, aby ustalić prawdę oraz odwrócenie faktów – jednak odwrócenie i negacja faktów to metody niezbyt często obecnie stosowane, gdyż dziś o wiele trudniej ukryć niektóre fakty przed opinią publiczną[117].

Zdecydowanie częściej natomiast spotykane są takie formy dezinformacji, jak:

- *mieszanie prawdy i kłamstwa – metoda ta stosowana jest w przypadku, gdy opinia publiczna jest już poinformowana o tym, co zaszło w rzeczywistości społecznej, lecz nie zna dokładnie wszystkich szczegółów;*
- *modyfikacja motywu i okoliczności – metoda polegająca na zasugerowaniu odbiorcom takiego motywu i takich okoliczności działania, które są w stanie wywołać w opinii publicznej przekonanie o wyższości bądź większej słuszności sposobu myślenia/postępowania jednej ze stron;*
- *rozmycie – polegające na tzw. „zalaniu" głównej i prawdziwej informacji przez dużą liczbę faktów nieistotnych dla danej sytuacji;*
- *kamuflaż – polega na drobiazgowym opisaniu zaistniałej sytuacji po to, aby zakryć główną informację;*

116 R. Bielawski, B. Grenda, P. Majdan, *Wieloaspektowa ewaluacja wykorzystania mediów społecznościowych na potrzeby kierowania SBN RP (ewaluacji ryzyka cyberzagrożeń BN)* (cyt. za) M. J. Wachowicz, *Ujęcie teoretyczne pojęcia dezinformacji,* Wiedza Obronna, 2019, T. 266-267, nr 1-2, s. 248.

117 R. Bielawski, B. Grenda, P. Majdan, *Wieloaspektowa ewaluacja wykorzystania mediów społecznościowych na potrzeby kierowania SBN RP (ewaluacji ryzyka cyberzagrożeń BN)* (cyt. za) M. J. Wachowicz, *Ujęcie teoretycznepojęcia dezinformacji,* Wiedza Obronna*, 2019, T. 266-267, nr 1-2, s. 248.*

- *interpretacja – jest to metoda stosowana w sytuacji, kiedy faktom nie da się zaprzeczyć, odwrócić ich, rozmyć lub zakamuflować, ale można je omówić, używając odpowiednich słów, które wywołują negatywne lub pozytywne skojarzenia opinii publicznej;*
- *generalizacja – to proces, w którym na podstawie jednego lub kilku przypadków stara się rozszerzyć wnioski na szerszą grupę osób. Głównym celem generalizacji jest pokazanie, że dany fakt lub zdarzenie, które może wydawać się wyjątkowe lub nietypowe, w rzeczywistości ma miejsce w szerszym kontekście i nie jest to odstępstwo od normy.*
- *ilustracja – metoda polegająca na użyciu konkretnego przypadku lub faktu jednostkowego w celu zobrazowania oraz lepszego zrozumienia szerszych zjawisk społecznych. Metoda ta często wykorzystywana jest w takich naukach jak socjologia, antropologia czy psychologia by zobrazować procesy społeczne, zjawiska kulturowe czy zmiany socjalne;*
- *nierówna reprezentacja – metoda używana często w przypadku walki politycznej, kiedy to przeciwnikom „ucina" się wypowiedzi, streszcza się szerszy punkt widzenia w jednym zdaniu lub przerywa w pół słowa;*
- *równa reprezentacja – metoda stosowana zazwyczaj w ostatniej fazie kampanii dezinformacyjnej, gdy zdecydowana większość publiczności jest już przekonana do tez lansowanych przez dezinformatorów. Wtedy wystarczy tak naprawdę utrwalić powszechnie obowiązującą opinię i zamknąć temat. Wówczas dezinformator publikuje równą ilość argumentacji za i przeciw tezie. Przy czym argumenty służące osobie lub grupie, która ma zyskać na operacji dezinformacyjnej, są przedstawione w sposób o wiele bardziej przekonujący i sugestywny, poparte zdaniem ekspertów budzących zaufanie, natomiast argumenty przeciwników podane są nieciekawie i często wygłaszają je osoby mało wiarygodne.*[118]

118 V. Volkoff, *Dezinformacja: oręż wojny* (cyt. za) A. Januszko-Szakiel, *Dezinformacja jako narzędzie manipulacji świadomością* [w:] J. Aksman (red.), *Manipulacja: pedagogiczno-społeczne aspekty*, Kraków 2010, s. 212.

Wraz z powyższą analizą technik dezinformacji stosowanych w procesach manipulacji rodzi się pytanie o to, kto stoi za tworzeniem informacji nieprawdziwych, które mogą prowadzić nie tylko do chaosu, ale i zakłócenia bezpieczeństwa życia jednostek? Mianowicie, działania o charakterze dezinformacyjnym mogą być tworzone między innymi przez liderów opinii do których możemy zaliczyć osoby o ugruntowanej i opiniotwórczej pozycji, posiadające umiejętność wpływania na poglądy innych użytkowników sieci, poprzez tworzenie realnych na pierwszy rzut oka tez. Konta tworzone przez takie osoby stanowią skuteczny pas transmisyjny zarówno świadomej jak i nieświadomej dezinformacji. Innym przykładem osób tworzących dezinformacje mogą być media i dziennikarze, którzy stanowią specjalny zbiór funkcjonujący w ramach grupy liderów opinii. Do osób tworzących sfabrykowane informacje można zaliczyć także zwykłych użytkowników sieci, którzy po prostu często komentują lub udostępniają różne treści bez ich uprzedniej weryfikacji. Należy jednak pamiętać także o dużym znaczeniu sztucznej inteligencji w kontekście dezinformacji, gdzie mamy do czynienia z trollami – są to osoby, które często ze swoich fałszywych kont publikują kontrowersyjne, prowokacyjne lub obraźliwe treści w sieci w celu wywołania konfliktu wśród użytkowników poprzez publikowanie prowokujących komentarzy lub fałszywych treści. Innym przykładem twórców treści dezinformacyjnych są także boty – konta zautomatyzowane lub półzautomatyzowane, które charakteryzują się powtarzającymi się zachowaniami dotyczącymi interakcji z publikowanymi przez inne konta treściami[119], co ukazuje nam, że nie zawsze za informację sfabrykowaną odpowiedzialny jest człowiek.

Jak walczyć z dezinformacją?

W społeczeństwie cyfrowym, w którym obecnie żyjemy, walka z dezinformacją stanowi kluczowy element życia społecznego. Z tego względu wiele krajów na całym świecie zaczęło podejmować działania pozwalające na przeciwdziałanie problemowi jaki stanowi dezinformacja w Internecie. Istotne wydaje się zwalczanie problemu dezinformacji z poziomu państwa. W ramach podejmowanych działań znalazły się między innymi: lokalizowanie i usuwanie fałszywych kont, dostosowanie algorytmów

119 E. Domańska, *Dezinformacja czym jest i jak ją zweryfikować*, Cyber Profilaktyka NASK, https://cyberprofilaktyka.pl/blog/dezinformacja---czym-jest-i-jak-ja-zweryfikowac_i23.html, [dostęp dn. 31.10.2024 r.].

wyszukiwarek w celu promowania wartościowych treści, zmniejszenie opłacalności publikowania nieprawdziwych informacji, a także wzmocnienie współpracy z organizacjami[120] *w kontekście dostarczania sprawdzonych wiadomości, które mogłyby choć w małym stopniu zminimalizować problem fake newsów w sieci.*

Działania w zakresie walki z dezinformacją rozpoczęła Komisja Europejska, która w styczniu 2018 roku powołała **grupę doradców tzw. „wysokiego szczebla"** *(high-level group of experts – HLEG) w skład której wchodziło 39 ekspertów – reprezentantów społeczeństwa, mediów społecznościowych, środowisk dziennikarskich, akademickich i organizacji trzeciego sektora – którzy wspólnie przeprowadzili analizę zjawiska dezinformacji*[121]*. W celu zapobiegania rozprzestrzenianiu się dezinformacji w Internecie wypracowano szereg rekomendacji, które obejmują wdrożenie działań w czterech obszarach:*

- *Transparentność – odgrywa kluczową rolę w walce z dezinformacją. Dzięki niej użytkownicy mogą rozróżniać wiarygodne treści od fałszywych, co pozwala na weryfikację źródeł skąd pochodzi dana informacja i ocenę ich rzetelności. Wprowadzenie standardów transparentności może pomóc w odbudowaniu zaufania do mediów, a także zwiększenia świadomości użytkowników |internetu na temat źródeł z których czerpią informację;*
- *Edukacja z zakresu korzystania z mediów i informacji – w tym obszarze należy podjąć działania zwiększające świadomość posługiwania się informacją zarówno wśród dzieci jak i ludzi dorosłych w każdym wieku. Istotną rolę w tym aspekcie odgrywa rozwijanie umiejętności analitycznych i krytycznego myślenia, które pozwolą użytkownikom sieci na ocenę wiarygodności informacji. Z tego też względu wydaje się konieczne, aby systemy edukacji zostały jak najszybciej dostosowane do nowej rzeczywistości;*

120 European Commission, *A multi-dimensional approach to disinformation: Report of the independent High level Group on fake news and online disinformation*, 2018, https://op.europa.eu/en/publication-detail/-/publication/6ef4df8b-4cea-11e8-be1d-01aa75ed71a1/language-en, [dostęp dn. 02.11.2024 r.].

121 J. Balcewicz, *Fake News – Dezinformacja w świecie nowych mediów*, NASK Cyber Policy, https://cyberpolicy.nask.pl/fake-news-dezinformacja-w-swiecie-nowych-mediow/, [dostęp dn. 02.11.2024 r.].

- *Wzmocnienie pozycji użytkowników i dziennikarzy – uznawane jest za istotny krok w kierunku zapewnienia większej wiarygodności i rzetelności informacji rozpowszechnianych w Internecie. Z jednej strony kluczowe wydaje się uwrażliwienie pracowników mediów na temat krytycznego podejścia do źródeł informacji. Z drugiej strony sami użytkownicy Internetu powinni przykładać większą wagę do oceny jakości informacji, które otrzymują. W tym przypadku ważne jest filtrowanie informacji, dlatego użytkownicy sieci powinni mieć zapewniony dostęp do narzędzi, które pomogą im filtrować wyniki wyszukiwania na przykład na podstawie trafności informacji i jakości źródeł;*
- Różnorodność i trwałość europejskiego ekosystemu mediów informacyjnych – dezinformacja jest rozpowszechniana ze względu na swoją atrakcyjność, a tym samym potencjał zainteresowania jak najszerszego grona odbiorców. Możemy przeciwdziałać zjawisku poprzez dbanie o odpowiedni poziom informacji, edukację w zakresie działania mediów, wpieranie niezależnych mediów informacyjnych, promowanie dziennikarstwa wysokiej jakości, inwestowanie w innowację w zakresie poprawy usług serwisów medialnych online czy współpracę międzynarodową.[122]

Do walki z dezinformacją powinno zaliczyć się także tzw. aktywne przeciwstawianie dezinformacji, które miałoby polegać na doświadczeniach własnych oraz innych krajów na świecie, które również walczą z dużym natężeniem antagonistycznych i nieprzychylnych działań w sferze informacji[123]. Mogłoby to pozwolić na stałe monitorowanie, analizowanie i kształtowanie na przykład polskiej przestrzeń informacyjnej poprzez osiągnięcie gotowości zwalczania dezinformacji poprze zbudowanie zdolności, tworzenie procedur i podnoszenie umiejętności jednostek w sferze rozróżniania fake newsów od informacji rzetelnych i prawdziwych[124]. W walce z dezinformacją istotne znaczenie odgrywa także aktywna obrona cyberprzestrzeni, która niestety obecnie nie jest na tyle dobrze zabezpieczona w efekcie czego luki występujące

122 Por. J. Balcewicz, *Fake News – Dezinformacja w świecie nowych mediów*, NASK Cyber Policy, https://cyberpolicy.nask.pl/fake-news-dezinformacja-w-swiecie-nowych-mediow/, [dostęp dn. 02.11.2024 r.].

123 M. Wrzosek (red.), *Zjawisko dezinformacji w dobie rewolucji cyfrowej. Państwo. Społeczeństwo. Polityka. Biznes*, Warszawa 2019, s. 10.

124 *Ibidem*.

w systemach komputerowych, oprogramowaniach, sieci i cyfrowych zasobach[125], są często wykorzystywane do rozprzestrzeniania dezinformacji. Takie działania mające na celu rozprzestrzenienie sfabrykowanych informacji, które w znacznym stopniu ukierunkowane są na zakłócenie stabilności społecznej oraz ładu społecznego, a ponadto wpływa znacznie na spadek zaufania obywateli do instytucji państwowych demokratycznego porządku. *Obecnie za szczególnie szkodliwe działania dezinformacyjne uznaje się ataki hybrydowe, które wywołują nie tylko chaos, ale i niepewność poprzez łączenie ich z przemocą fizyczną, cyberatakami i dezinformacją. Z tego też względu warto podkreślić, że niezbędne staje się wdrażanie skutecznych strategii obrony. Struktury aktywnej obrony cyberprzestrzeni powinny koncentrować się przede wszystkim na monitorowaniu zagrożeń, co umożliwiłoby szybkie reagowanie na potencjalne incydenty zarówno w ramach obrony wewnętrznej kraju, jak i za jego granicami w ramach działań międzynarodowych przy współpracy placówek dyplomatycznych*[126]*, co pozwoliłoby na minimalizację skutków i zapewnienie poczucia większego komfortu bezpieczeństwa jednostkom. Ponadto, w kontekście zwalczania dezinformacji coraz częściej mówi się także o aktywnej współpracy organów państwowych, przemysłu prywatnego oraz organizacji pozarządowych działających w ramach trzeciego sektora, gdzie takiego typu współprace powinny cechować się nie tylko autonomią, ale i różną dynamiką przy jasno określonych priorytetach, a także skorelowanych celach*[127]*, gdzie głównym założeniem jest wzajemna kooperacja w celu szybkiego reagowania na informacje niezgodne z prawdą.*

Walka z dezinformacją to współprace różnych środowisk, a wraz z rozwojem technologii metody walki nieustannie ulegają ewolucji i udoskonaleniu. Podmioty realizujące działania w tej sferze stale dążą do tworzenia nowych rozwiązań walki z dezinformacją, aby uniknąć szablonowości i powtarzania wcześniej zastosowanych metod, co przede wszystkim pozwoli informacji pozostać informacją, a nie poprzez fake newsy i manipulację stać się tylko i wyłącznie szumem informacyjnym.

125 *Ibidem.*
126 *Ibidem.*
127 *Ibidem.*

Podsumowanie

Powyższa analiza teoretyczna pozwala potwierdzić postawioną we wstępie hipotezę, że dezinformacja w znaczący sposób jest wykorzystywana jako narzędzie manipulacji w sieci w oparciu o różnorodność technik jakie można zastosować do rozprzestrzeniania informacji fałszywych i niezgodnych z prawda. Wraz z rozwojem technologii problem dezinformacji rozrasta się i w coraz intensywniejszy sposób wpływa na różne obszary życia społecznego budząc tym samym coraz większe obawy, zwłaszcza ze względu na łatwość dostępu do takich źródeł i brak świadomości istnienia fałszywych informacji wśród odbiorców.

Udało się także odpowiedzieć na sformułowany w artykule problem badawczy, czy dezinformacja stanowi narzędzie manipulacji użytkownikami w sieci? Można zauważyć, że tak naprawdę każdy użytkownik Internetu jest dość mocno narażony na manipulację w sieci poprzez dezinformację. Fałszywa informacja może w znaczny sposób wpłynąć na podejmowane przez użytkowników Internetu decyzje. Istnieje także ryzyko, że fałszywa treść, która dotrze do użytkowników sieci następnie może być przez nich powielana poprzez jej udostępnianie na przykład kolejnemu gronu znajomych, którzy tej treści nie widzieli wcześniej, co z pewnością będzie tworzyć szum informacyjny i narażać na nieprawdziwe informacje coraz więcej osób.

Ze względu na fakt, że wrogie działania informacyjne stanowią coraz większe zagrożenie to wymagają one szczególnej uwagi i nadzoru ze strony podmiotów odpowiedzialnych za bezpieczeństwo narodowe[128], ale także dużej rozwagi użytkowników Internetu. Bowiem, w dzisiejszym świecie, w którym informacje rozprzestrzeniają się w szybkim tempie trzeba być czujnym na potencjalne działania dezinformacyjne pojawiające się w sieci. Konieczna wydaje się refleksja nad skutecznymi metodami przeciwdziałania atakom informacyjnym poprzez tworzenie kampanii zwalczania dezinformacji w celu edukacji obywateli o tym jak radzić sobie w rzeczywistości internetowej zdominowanej przez nieprawdziwe informacje. Czynnikiem niezwykle istotnym jest także rozpowszechnienie w szerokich kręgach społecznych wiedzy na ten

128 T. Grabowski, *Metody walki informacyjnej w mediach elektronicznych na przykładzie konfliktu rosyjsko-ukraińskiego (2014-2016)*, „Horyzonty Polityki", 2016, nr 7(20), s. 51.

temat[129] *w celu ukazania aktualności i ważności tematu jaki stanowi dezinformacja w sieci zwłaszcza, gdy powiążemy ją ze sztuczną inteligencją, która może dzięki złym algorytmom generować dużą ilość sfabrykowanych i nieprawdziwych informacji na różnorodne tematy.*

Bibliografia

Balcewicz J., Fake News – *Dezinformacja w świecie nowych mediów*, NASK Cyber Policy, https://cyberpolicy.nas*k.pl/fake-news-dezinformacja-w-swiecie-nowych-mediow/, [dostęp dn. 31.10.2024 r.]*.

Bielawski R., Grenda B., Majdan P., Wieloaspektowa ewaluacja wykorzystania mediów społecznościowych na potrzeby kierowania SBN RP (ewaluacji ryzyka cyberzagrożeń BN) (cyt. za) Wachowicz M. J., Ujęcie teoretyczne pojęcia dezinformacji, Wiedza Obronna, 2019, T. 266-267, nr 1-2, s. 226-253, DOI: https://doi.org/10.34752/x40y-nc78.

Bralczyk J., Manipulacja językowa [w:] Bauer Z., Chodziński E. (red.), Dziennikarstwo i świat mediów, Wydawnictwo UNIVERSITAS, Kraków 2000, s. 244-250.

Casey M., Europejska polityka informacyjna. Wyzwania i perspektywy dla administracji publicznej, Wydawnictwo Naukowe Uniwersytetu Mikołaja Kopernika, Toruń 2001.

Chmielecka P., Zjawisko dezinformacji w komunikacji politycznej na przykładzie imigrantów z Ukrainy – zarys problemu [w:] Boćkowski D., Dąbrowska-Prokopowska E., Goryń P., Gorynia K. (red.), Dezinformacja – Inspiracja – Społeczeństwo. Cybersecurity, Wydawnictwo Uniwersytetu w Białymstoku, Białystok 2022, s. 63-78.

Domańska E., *Dezinformacja czym jest i jak ją zweryfikować*, Cyber Profilaktyka NASK, https://cyberprofilaktyka.*pl/blog/dezinformacja---czym-jest-i-jak-ja-zweryfikowac_i23.html, [dostęp dn. 31.10.2024 r.]*.

Dubisz S. (red.), Uniwersalny słownik języka polskiego, T. 1, Wydawnictwo Naukowe PWN, Warszawa 2003, s. 601

Encyklopedia psychologii, Wyd. 1, Wydawnictwo Fundacja Innowacja, Warszawa 1998.

European Commission, A multi-dimensional approach to disinformation: Report of the independent High level Group on fake news and online disinformation, 2018, https://op.europa.eu/en/publication-detail/-/publication/6ef4df8*b-4cea-11e8-be1d-01aa75ed71a1/language-en, [dostęp dn. 02.11.2024 r.]*.

Grabowski T., Metody walki informacyjnej w mediach elektronicznych na przykładzie konfliktu rosyjsko-ukraińskiego (2014-2016), „Horyzonty Polityki", 2016, nr 7(20), s. 27-53, DOI: https://doi.org/10.17399/HP.2016.072002.

Hamer H., Psychologia społeczna, Wydawnictwo Difin, Warszawa 2005.

Hetmański M., Społeczny charakter informacji [w:] Chyrowicz B. (red.), Społeczeństwo informatyczne. Szansa czy zagrożenie?, Wydawnictwo Towarzystwo Naukowe KUL, Lublin 2003, s. 9-36.

Januszko-Szakiel A., Dezinformacja jako narzędzie manipulacji świadomością [w:] Aksman J. (red.), Manipulacja: pedagogiczno-społeczne aspekty, Oficyna Wydawnictwa AFM, Kraków 2010, s. 209-216.

Juszczyk S., Internet – współczesne medium komunikacji społecznej, „Edukacja i Dialog", 2011, nr 5/6, s. 42-46.

129 T. Grabowski, *Metody walki informacyjnej w mediach elektronicznych na przykładzie konfliktu rosyjsko-ukraińskiego (2014-2016),* „Horyzonty Polityki", 2016, nr 7(20), s. 51.

Kacała T., Dezinformacja i propaganda w kontekście zagrożeń dla bezpieczeństwa państwa, „Przegląd Prawa Konstytucyjnego", 2015, nr 2 (24), s. 49-65.

Kamińska A. M., Internetowe narzędzia komunikacji, czyli jak zapanować nad chaosem informacyjnym, „Nowa Biblioteka. Usługi, Technologie Informacyjne i Media", 2017, nr 4 (27), s. 19-35.

Kubicek H., Möglichkeiten und Gefahren der „Informationsgesellschaft" (cyt. za) Goliński M., Społeczeństwo informacyjne: problemy definicyjne i problemy pomiaru, Dydaktyka Informatyki, 2004, s. 43-55.

Lepa A., Świat manipulacji (cyt. za) Nagi J., Manipulacja jako narzędzie dezinformacji, „Resovia Sacra", 2019, nr 26, s. 297-310.

Markowski A., Wielki słownik poprawnej polszczyzny (cyt. za) Chałubińska-Jentkiewicz K., Dezinformacja jako akt agresji w cyberprzestrzeni, "Cybersecurity and Law", 2021, nr 5(1), s. 9-24, DOI: https://doi.org/10.35467/cal/142175.

McQuail D., Teoria komunikowania masowego (cyt. za) T. Goban-Klas (red.), Cywilizacja medialna: geneza, ewolucja, eksplozja, Wydawnictwo Szkolne i Pedagogiczne S.A., Warszawa 2007.

Szymańska N., Dezinformacja jako narzędzie manipulacji medialnej, „Roczniki Studenckie Akademii Wojsk Lądowych", 2023, nr 7, s. 39-49.

Tomaszewska A. W., Społeczeństwo informacyjne – pojęcie, pomiar i stopień rozwoju w Polsce, [w:] Urbanek P., Ekonomia i zarządzanie w teorii i praktyce. Tom 6. Determinanty konkurencyjności przedsiębiorstw, regionów, gospodarek, Wydawnictwo Uniwersytetu Łódzkiego, Łódź 2013, s. 300-316.V.

Volkoff V., Dezinformacja: oręż wojny (cyt. za) Januszko-Szakiel A., Dezinformacja jako narzędzie manipulacji świadomością [w:] Aksman J. (red.), Manipulacja: pedagogiczno-społeczne aspekty, Oficyna Wydawnictwa AFM, Kraków 2010, s. 209-216.

Wrzosek M., Dezinformacja jako komponent operacji informacyjnych, Akademia Obrony Narodowej, Warszawa 2005.

Wrzosek M., (red.), Zjawisko dezinformacji w dobie rewolucji cyfrowej. Państwo. Społeczeństwo. Polityka. Biznes, NASK Cyber Policy, Warszawa 2019, s. 10.

Żarna K., Wybrane przykłady dezinformacji podczas kampanii wyborczej do Rady Narodowej Republiki Słowackiej w 2023 roku, "Politeja", 2024, nr 1 (88/2), s. 155-168, DOI: https://doi.org/10.12797/Politeja.20.2024.88.2.10.

„dot.pl" - czasopismo Rejestru domeny .pl

Ukryte zasoby Internetu a terroryzm

Krzysztof Kaczmarek
Politechnika Koszalińska, Wydział Humanistyczny
ORCID: https://orcid.org/0000-0001-8519-1667
E-mail: puola@tlen.pl

Streszczenie

Powszechność korzystania z Internetu nie oznacza pełnej znajomości jego zawartości. Znaczna część zasobów sieci nie jest indeksowana i tym samym pozostaje niedostępna dla większości użytkowników. Artykuł analizuje wpływ tych nieindeksowanych zasobów na bezpieczeństwo cyfrowe. W szczególności badany jest ich związek z terroryzmem oraz przestępczością. Hipoteza badawcza zakłada, że ukryte zasoby Internetu znacząco wpływają na poziom bezpieczeństwa społeczeństw i państw. Do weryfikacji tej hipotezy zastosowano przegląd literatury, analizę jakościową treści dostępnych w dark webie oraz metodę desk research. Wyniki badań wskazują na istotne zagrożenia związane z działalnością terrorystyczną oraz nielegalnym handlem w ciemnej sieci, a także na wyzwania związane z monitorowaniem i zwalczaniem tych zagrożeń przy użyciu zaawansowanych technologii, w tym sztucznej inteligencji.

Słowa kluczowe: deep web, darknet, terroryzm, sztuczna inteligencja

Received: 25.04.2024
Accepted: 24.05.2024
Published: 27.05.2024

Cite this article as:
K. Kaczmarek
"Ukryte zasoby Internetu a terroryzm"

DOT.PL, no. 1/ 2024,
10.60097/DOTPL/189286

Corresponding author:
Krzysztof Kaczmarek
Politechnika Koszalińska,
Wydział Humanistyczny
E-mail: puola@tlen.pl

Hidden Internet Resources and Terrorism

Abstract

The widespread use of the Internet does not mean full knowledge of its content. A significant part of the network resources is not indexed and therefore remains inaccessible to most users. The article examines the impact of these nonindexed resources on digital security. In particular, their relationship with terrorism and crime is examined. The research hypothesis assumes that hidden Internet resources significantly influence the level of security of societies and countries. To verify this hypothesis, a literature review, qualitative analysis of content available on the Dark Web and the desk research method were used. Research results indicate significant threats related to terrorist activities and illegal trade on the Dark Web, as well as the challenges associated with monitoring and combating these threats using advanced technologies, including artificial intelligence.

Keywords: deep web, darknet, terrorism, artificial intelligence

Wstęp

Trywializmem jest stwierdzenie, że funkcjonowanie współczesnych społeczeństw i państw opiera się na dostępie do Internetu[130]. Cyfrowy świat wydaje się być naturalnym środowiskiem współczesnego człowieka. Należy jednak zauważyć, że nie wszystkie zasoby Internetu są powszechnie dostępne. Znaczna część treści jest nieindeksowana i ukryta przed standardowymi wyszukiwarkami, a dostęp do nich wymaga specjalnych uprawnień[131]. Najczęściej używane wyszukiwarki nie docierają do większości danych w Internecie, a sieć szybko pogłębia się zyskując dodatkowy wymiar. Uważa się, że większość informacji jest ukryta w głębokiej sieci (ang. *deep web*)[132]. Można przyjąć, że poszukiwanie informacji w Internecie to przeszukiwanie sieci powierzchownej lub przeszukiwanie ukrytej sieci. Pierwsza jest publicznie i bezpośrednio dostępna oraz

[130] K. Huczek, *Cyfrowi tubylcy i cyfrowi imigranci. O społecznych wyzwaniach i zagrożeniach w cyberprzestrzeni*, „Cybersecurity and Law", 2023, nr 10(2), pp. 415.
[131] K. Kaczmarek, *Darknet jako przedmiot badań nauk społecznych*, „Cybersecurity and Law", 2020, nr 4(2), pp.106.
[132] L. Ismailova, V. Wolfengagen, S. Kosikov, *A Semantic Model for Indexing in the Hidden Web*, „Procedia Computer Science", 2021, nr 190, pp. 324-325.

posiada adres statyczny. Natomiast druga jest ukryta i jest dostępna jedynie poprzez rejestrację, a interfejs wyszukiwania i dostęp są często płatne[133]. Zatem, najogólniej ujmując, ukryte zasoby Internetu to te, które nie są dostępne dla konwencjonalnych wyszukiwarek.

W związku z tym można przyjąć, że znaczna część cyfrowej przestrzeni stanowi, dla części osób korzystających w jakiejkolwiek formie z Internetu, obszar nieznany. Skutkuje to tym, że poruszanie się po ukrytych zasobach sieci może stanowić wyzwanie dla bezpieczeństwa informacji i danych. Należy jednocześnie zauważyć, że cyberprzestrzeń generuje pewne problemy i ryzyka, których liczba zwiększa się wraz z postępującym w dziedzinie ICT postępem[134], a kompetencje cyfrowe są jednym z ważniejszych wyznaczników jakości życia[135]. Zagrożenia te wynikają przede wszystkim z postępującego uzależniania funkcjonowania społeczeństw od bezawaryjnego dostępu do sieci. Dotyczy to również bezpieczeństwa. Taki stan rzeczy jest wykorzystywany przez zewnętrzne podmioty do wywierania wpływu na zachowania społeczne czy przeprowadzania cyberataków[136].

W tym miejscu należy podkreślić, że również sieci elektroenergetyczne są elementem cyberbezpieczeństwa[137]. W kontekście napiętej sytuacji międzynarodowej, zmian klimatycznych i możliwości wystąpienia ekstremalnych zjawisk pogodowych czy kryzysu energetycznego należy brać pod uwagę również możliwość fizycznego uszkodzenia infrastruktury teleinformatycznej lub elektroenergetycznej. W takich przypadkach, oparte na dostępie do informacji, funkcjonowanie społeczeństw może zostać zakłócone[138].

W przeciwdziałaniu cyfrowym zagrożeniom jednym z najważniejszych elementów jest świadomość ich istnienia. Tymczasem jednym z największych problemów związanych z

---

[133] S. Kaur, A. Singh, G. Geetha, X. Cheng, *IHWC: intelligent hidden web crawler for harvesting data in urban domains*, "Complex & Intelligent Systems", 2023, nr 9(4), pp. 3636.

[134] A. Bencsik, M. Karpiuk, M. Kelemen, E. Włodyka, *Cybersecurity in the Visegrad Group Countries*, "Lex Localis Press", Maribor 2023, pp. 89.

[135] A. Bencsik, M. Karpiuk, N. Strizzolo, *Information Society Services and Their Cybersecurity*, „Cybersecurity and Law", 2024, nr 11(1), pp. 259.

[136] M. Karpiuk, *Crisis management vs. cyber threat*, „Sicurezza, terrorismo e società", 2022, nr 16, pp. 121.

[137] E. M. Włodyka, K. Kaczmarek, *Cyber Security of Electrical Grids – A Contribution to Research*, „Cybersecurity and Law", 2024, nr 2(12), pp. 268.

[138] M. Karpiuk, W. Pizło, K. Kaczmarek, *Cybersecurity Management – Current State And Directions Of Change*, "International Journal of Legal Studies", 2023, nr 2, pp. 660.

zapewnieniem bezpieczeństwa (w tym cyberbezpieczeństwa) jest skuteczność postrzegania sygnałów ostrzegawczych[139]. Dotyczy to zarówno zagrożeń związanych ze złośliwym oprogramowaniem jak i z wywieraniem wpływu na użytkowników Internetu. Może to odnosić się zarówno do szeroko rozumianej ingerencji w procesy wyborcze w państwach demokratycznych[140], czy rozpowszechniania mogących wywoływać niepokoje społeczne fałszywych informacji. Tymczasem w większości europejskich państw problem fake newsów jest traktowany jako część systemów medialnych[141].

W tym kontekście istotna jest analiza wpływu ukrytych zasobów Internetu na cyberbezpieczeństwo. Przede wszystkim deep web oraz dark web oferują środowisko, w którym mogą powstawać i rozwijać się różnorodne zagrożenia, takie jak handel nielegalnymi towarami i usługami, wymiana złośliwego oprogramowania, czy planowanie oraz organizowanie cyberataków i zamachów terrorystycznych.

Celem niniejszego artykułu jest analiza wpływu nieindeksowanych zasobów Internetu na bezpieczeństwo. Natomiast hipoteza badawcza zakłada, że zasoby i środowisko ukrytej sieci (deep web i dark web) znacząco wpływają na poziom cyfrowego bezpieczeństwa społeczeństw i państw.

W celu jej weryfikacji zastosowano następujące metody badawcze: przegląd literatury i dostępnych źródeł internetowych. Przeprowadzona została również analiza jakościowa treści dostępnych w dark webie. Natomiast metoda desk research pozwoliła na uporządkowanie informacji dotyczących skuteczności cyfrowych narzędzi pozwalających na monitorowanie ukrytych zasobów Internetu.

Typologia zasobów Internetu i wyzwania bezpieczeństwa dla jego warstw

Ze względu na dostępność zasobów Internet można podzielić na trzy warstwy:

[139] B. Ćwik, *Postrzeganie zagrożeń w systemach bezpieczeństwa organizacji*, „Modern Management Review", 2017, nr 3, pp. 28.
[140] E. M. Włodyka, *Polaryzacja, kohabitacja czy integracja? Wyzwania cyberbezpieczeństwa procesów wyborczych w Polsce*, [in:] *Cyberbezpieczeństwo. Aspekty krajowe i międzynarodowe*, M. Karpiuk [ed.], Wydawnictwo Akademii Sztuki Wojennej, Warszawa 2024, pp. 116.
[141] K. Wasilewski, *Fake News and the Europeanization of Cyberspace*, "Polish Political Science Yearbook", 2021, nr 50(4).

- Internet powierzchniowy (ang. *Surface Web*) – publicznie dostępny, indeksowany przez standardowe wyszukiwarki takie jak Google czy Bing. Zawiera strony internetowe, blogi, portale społecznościowe i informacyjne, itp.
- Głęboka sieć (ang. *Deep Web*) – zawiera zasoby nieindeksowane przez standardowe wyszukiwarki, które są dostępne za pomocą specjalnych uprawnień lub rejestracji. Mogą to być bazy danych lub płatne serwisy.
- Ciemna sieć (ang. *Dark Web, Dark Net*) – część głębokiej sieci dostępna jedynie za pomocą specjalnego oprogramowania (np. TOR), celowo ukryta. Chociaż nie gwarantuje, pozwala na zachowanie anonimowości. Zawiera anonimowe fora, nielegalne rynki, strony z nielegalnym oprogramowaniem.

Przed każdą z tych warstw stoją inne, chociaż wiążące się ze sobą, wyzwania bezpieczeństwa. Dla Internetu powierzchniowego są one najczęściej związane z phishingiem, malware, atakami XSS (ang. *Cross-Site Scripting*), utratą prywatności przez cookies[142]. W przypadku głębokiej sieci wyzwania te dotyczą naruszenia danych, nieautoryzowanego dostępu i działalności przestępczej[143]. Natomiast wyzwania bezpieczeństwa związane z dark web dotyczą anonimowości ułatwiającej przestępczą działalność, kradzieży tożsamości (handel skradzionymi dokumentami i danymi osobowymi) i cyberbezpieczeństwa (handel cyfrowymi narzędziami umożliwiającymi przeprowadzanie cyfrowych ataków)[144]. Każda z warstw Internetu wymaga unikalnego podejścia do zarządzania bezpieczeństwem, które uwzględnia jej specyficzne zagrożenia i ryzyka.

Darknet

Darknet, jako najbardziej ukryta część deep web, jest miejscem, w którym kluczowa jest anonimowość. Jej rozmiar, nieindeksowana, fragmentaryczna i wielowarstwowa zawartość sprawiają, że wykrywanie w niej przestępstw jest skrajnie trudne, a w wielu przypadkach niemożliwe. Dodatkowo ekosystem ciemnej sieci jest wysoce

[142] G. A. Khan, *The Web Layers: Security Challenges and Solutions in Surface, Deep and Dark Web*, SSRN 2024, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4722851, dostęp: 19.05.2024.
[143] ibidem.
[144] ibidem.

nieprzewidywalny – każdego dnia stare strony znikają i pojawiają się nowe[145]. Należy również podkreślić, że aby znaleźć określoną zawartość w dark web należy korzystać z katalogów lub dedykowanych wyszukiwarek. W katalogach najłatwiej można spotkać adresy stron z nielegalnymi towarami i usługami. Jednocześnie transakcje odbywają się przy wykorzystaniu kryptowalut, które pozwalają użytkownikom na zachowanie anonimowości. Najczęściej są to oferty sprzedaży kradzionych lub fałszywych dokumentów, kart płatniczych, nielegalnych leków i narkotyków czy hakerów do wynajęcia[146]. Jednak można tam znaleźć również, zapewniające anonimowość, strony do kontaktu ze służbami wywiadowczymi państw, np. z amerykańską Centralną Agencją Wywiadowczą[147].

Dostęp do dark web sam w sobie nie jest nielegalny, choć ta część sieci jest często kojarzona z nielegalną działalnością ze względu na jej anonimowy charakter. Jednak technologia i sieci tworzące dark web nie są niezgodne z prawem. Natomiast legalność działań podejmowanych w darknecie zależy od charakteru tych działań i jurysdykcji, której podlegają. Natomiast ciemna sieć to złożona i różnorodna część Internetu, która pozostaje owiana tajemnicą i często źle rozumiana przez ogół społeczeństwa. Jej technologie prywatności i anonimowości oferują kluczowe korzyści w zakresie ochrony wolności słowa, prywatności i umożliwienia bezpiecznej komunikacji, zwłaszcza w środowiskach, w których jest ona zagrożona. Jednakże zdolność dark web do anonimizowania użytkowników i działań stwarza również poważne wyzwania, ponieważ może ułatwiać nielegalne i szkodliwe działania. Jest oczywiste, że ciemna sieć będzie nadal ewoluować, podobnie jak narzędzia i metody dostępu do niej, charakter prowadzonych w niej działań oraz ramy prawne i etyczne regulujące jej wykorzystanie.

W zwalczaniu przestępstw w darknecie coraz większe zastosowanie znajdują technologie sztucznej inteligencji (AI), które stają się coraz skuteczniejsze w analizie danych zarówno z powierzchniowego jak i ciemnego Internetu. Algorytmy uczenia maszynowego są

[145] S. Nazah et. al., *Evolution of Dark Web Threat Analysis and Detection: A systematic Approach*, "Ieee Access", 2020, nr 8, pp. 171815.
[146] *OnionLinks*, http://s4k4ceiapwwgcm3mkb6e4diqecpo7kvdnfr5gg7sph7jjppqkvwwqtyd.onion/ (adres w Dark Web), dostęp: 19.05.2024.
[147] Central Intelligence Agency, http://ciadotgov4sjwlzihbbgxnqg3xiyrg7so2r2o3lt5wz5ypk4sxyjstad.onion/ (adres w Dark Web), dostęp: 19.05.2024.

wykorzystywane do automatycznego łączenia profili użytkowników na różnych forach, analizując podobieństwa w nazwach użytkowników, treściach i sieciach kontaktów. AI pomaga w identyfikacji i powiązaniu tożsamości osób działających w ciemnej sieci z ich tożsamościami w powierzchniowym Internecie[148].

Jednak istotne jest to, że dark web pozwala na zachowanie anonimowości, ale jej nie gwarantuje. Pozwalają na to cyfrowe narzędzia są jedynie narzędziami, których sposób i efektywność wykorzystania zależą jedynie od użytkowników. Jednocześnie wydaje się, że istnieją lub wkrótce powstaną narzędzia pozwalające na monitorowanie tej części sieci. Nie będą natomiast powszechnie dostępne.

Terrorystyczna aktywność w Darknecie

Terroryści są aktywni na różnych platformach internetowych od końca lat 90. XX wieku. Jednak surface web okazała się zbyt ryzykowna dla poszukujących anonimowości terrorystów: można ją było monitorować, śledzić, a użytkowników lokalizować. W związku z tym po atakach w Paryżu z listopada 2015 r. organizacje terrorystyczne przeniosły znaczną część swojej aktywności do darknetu. Jednym z przykładów wykorzystywania ciemnej sieci przez terrorystów jest działalność tzw. państwa islamskiego (ang. Islamic State of Iraq and Syria, ISIS), które wykorzystywało dark web do rekrutacji bojowników, planowania ataków oraz rozpowszechniania propagandy. Dzięki ciemnej sieci, organizacja ta mogła skutecznie prowadzić globalną kampanię terroru[149].

Jednak aktywność tego typu organizacji w Darknecie polega nie tylko na przygotowywaniu ataków, ale również na zdobywaniu środków finansowych na swoją działalność. W związku z tym podjętych zostało wiele działań mających na celu monitorowanie tej części Internetu.

---

[148] K. Foy, *Artificial intelligence is helping investigators fight crime on the dark web*, Lincoln Laboratory, Massachusetts Institute of Technology, 2019, https://www.ll.mit.edu/news/artificial-intelligence-helping-investigators-fight-crime-dark-web, dostęp: 19.05.2024.

[149] G. Weimann, *Going Darker? The Challenge of Dark Net Terrorism*, Woodrow Wilson International Center for Scholars, Washington, 2021, https://www.wilsoncenter.org/sites/default/files/media/documents/publication/going_darker_challenge_of_dark_net_terrorism.pdf, dostęp: 22.05.2024.

Jedną z inicjatyw mających na celu analizę i zwalczanie nielegalnej działalności prowadzonej w Darknecie był, współfinansowany przez unijny program Horyzont 2020, projekt DANTE (Darknet Advanced Network Technology and Exploitation). Był to europejski projekt badawczo-rozwojowy, który miał na celu opracowanie narzędzi i technologii pozwalających na monitorowanie, analizę i wykrywanie nielegalnych działań w ciemnej sieci.

Główne cele projektu DANTE obejmowały:

- zbieranie i analizowanie danych: opracowanie technologii do zbierania danych z różnych źródeł w ciemnej sieci, w tym z ukrytych usług i forów dyskusyjnych;
- wykrywanie i śledzenie: rozwijanie algorytmów do identyfikacji podejrzanych działań i śledzenia nielegalnych transakcji oraz komunikacji;
- analiza danych: stosowanie zaawansowanych technik analizy danych, w tym analizy big data i sztucznej inteligencji, w celu odkrywania wzorców i powiązań między różnymi podmiotami w ciemnej sieci;
- współpraca międzynarodowa: promowanie współpracy między agencjami rządowymi, organami ścigania i instytucjami badawczymi na całym świecie w celu skuteczniejszej walki z przestępczością w ciemnej sieci[150].

System powstały w ramach projektu DANTE jest obecnie wykorzystywany między innymi do:

- wykrywania i monitorowania źródeł istotnych danych związanych z terroryzmem w powierzchniowej, głębokiej sieci i ciemnej sieci;
- dokładnego i szybkiego wykrywania, analizy i kategoryzacji wielojęzycznych treści podejrzanych o terroryzm;
- zakrojonych na szeroką skalę analiz czasowych trendów terrorystycznych;
- podsumowywania w czasie rzeczywistym wielojęzycznych i multimedialnych treści związanych z terroryzmem;
- wykrywania dezinformacji w internetowych treściach;

[150] D. Cohen et al., *DANTE: A framework for mining and monitoring darknet traffic,* "Computer Security–ESORICS 2020: 25th European Symposium on Research in Computer Security", 2020, Proceedings, Part I 25, Springer International Publishing, https://doi.org/10.48550/arXiv.2003.02575

- wykrywania i monitorowania osób oraz łączenie pseudonimów z osobami fizycznymi;
- dokładnej i szybkiej identyfikacji internetowych społeczności i grup terrorystycznych;
- przechwytywania, przechowywania i zabezpieczania odpowiednich danych do dalszej analizy kryminalistycznej[151].

Rozwój sztucznej inteligencji sprawia, że powstaje coraz więcej, opartych na jej algorytmach, cyfrowych narzędzi, które są w stanie samodzielnie monitorować i analizować ruch w Darknecie[152]. Można zatem przyjąć, że istnieją skuteczne narzędzia zwalczania terroryzmu i innych przestępstw w ciemnej sieci. Należy jednak przeanalizować zarówno ich możliwości jak i efektywność wykorzystywania.

Podsumowanie

Istniejące cyfrowe narzędzia pozwalają na monitorowanie darknetu, jednak ich efektywność jest ograniczona, o czym świadczy liczba i dostępność znajdujących się w tej części sieci sklepów z nielegalnymi towarami. Narzędzia te, mimo że są technologicznie zaawansowane, nie są w stanie skutecznie przeciwdziałać nielegalnym i niebezpiecznym aktywnościom.

Jednym z głównych problemów jest skala i złożoność darknetu, który charakteryzuje się dużą anonimowością użytkowników oraz dynamicznie zmieniającą się strukturą. Sklepy z nielegalnymi towarami często zmieniają swoje adresy, co utrudnia ich namierzanie i stałe monitorowanie. Dodatkowo wiele transakcji odbywa się za pomocą kryptowalut, co dodatkowo utrudnia śledzenie przepływu środków finansowych.

Narzędzia do monitorowania darknetu, takie jak zaawansowane systemy analizy danych oraz algorytmy sztucznej inteligencji, pozwalają na identyfikowanie wzorców i trendów, jednak ich efektywność jest ograniczona przez konieczność ciągłej aktualizacji i adaptacji do nowych metod stosowanych przez przestępców i organizacje terrorystyczne. Istotnym

[151] DANTE, *DANTE- Detecting and analysing terrorist-related online contents and financing activities*, https://www.h2020-dante.eu/, dostęp: 22.05.2024.
[152] Q. Abu Al-Haija et al., *Machine-Learning-Based Darknet Traffic Detection System for IoT Applications*, "Electronics", 2022, nr 11(4), 556, pp. 7.

wyzwaniem jest również współpraca międzynarodowa. Darknet jest zjawiskiem globalnym, co wymaga skoordynowanych działań różnych państw i organizacji międzynarodowych. Jednak brak jednolitych standardów prawnych i różnice w podejściu do ochrony prywatności i wolności obywatelskich stanowią dodatkowe wyzwanie.

Narzędzia monitorujące są często stosowane reaktywnie, a nie proaktywnie. Oznacza to, że działania podejmowane są dopiero po wykryciu nielegalnych działań, co daje przestępcom przewagę czasową na zatarcie śladów. Ponadto, ograniczone zasoby finansowe i kadrowe organów ścigania sprawiają, że monitorowanie darknetu nie jest priorytetem w porównaniu do innych działań operacyjnych.

W celu poprawy efektywności monitorowania darknetu konieczne jest inwestowanie w rozwój technologii oraz szkolenie specjalistów z zakresu cyberbezpieczeństwa. Współpraca publiczno-prywatna oraz wymiana informacji między sektorem technologicznym a organami ścigania mogą znacząco przyczynić się do zwiększenia skuteczności działań. Ważne jest również prowadzenie badań naukowych nad nowymi metodami analizy danych i algorytmami sztucznej inteligencji, które mogą pomóc w identyfikacji i śledzeniu aktywności kryminalnej i terrorystycznej.

Należy również podkreślić, że jednym z działań, których celem jest zapobieganie atakom terrorystycznym jest monitoring i analiza całego Internetu w czasie rzeczywistym. W kontekście napiętej sytuacji międzynarodowej badania nad opracowaniem takich narzędzi powinny być jednym z priorytetów państw demokratycznych. Należy bowiem brać pod uwagę to, że reżimy totalitarne działają w zupełnie odmiennej od zachodniej, kulturze politycznej i prawnej.

Tocząca się w cyberprzestrzeni wojna i mający tam miejsce wyścig zbrojeń powodują, że zagrożenia związane ze wszystkimi warstwami Internetu będą miały coraz większy wpływ na funkcjonowanie nie tylko społeczeństw i państw, ale i jednostek. Narzędzia pozwalające na monitorowanie głębokiej sieci mogą być wykorzystywane również przez ugrupowania terrorystyczne w celu zdobycia informacji lub pozyskania środków finansowych. Pozwalają one również na naruszenie integralności danych, w tym tych, które są kluczowe dla bezpieczeństwa państwa. Natomiast narzędzia pozwalające na

monitorowanie darknetu, wykorzystane przez reżimy totalitarne, mogą spowodować utratę osobowych źródeł informacji. W związku z tym sposoby analizy całej, łącznie z ciemną, sieci, nie powinny być powszechnie znane, a wykorzystywane narzędzia dostępne. Powinny one być traktowane tak jak technologie wojskowe, którymi w znacznym stopniu są. Podejście takie pozwala na postawienie hipotezy, że tego rodzaju narzędzia już istnieją. Natomiast brak widoczności efektów zwalczania rynku nielegalnych towarów i usług w ciemnej sieci może wynikać z konieczności ukrywania istnienia takich narzędzi. Jednak mogą one zostać (lub są) wykorzystywane w celu przeciwdziałaniu wielkoskalowym zagrożeniom takim jak hybrydowe operacje państw totalitarnych.

Bibliografia

Abu Al-Haija, Q., Krichen, M., Abu Elhaija, W., *Machine-Learning-Based Darknet Traffic Detection System for IoT Applications*, "Electronics", 2022, nr11(4), 556, pp. 1-19.

Bencsik, A., Karpiuk, M., Kelemen, M., Włodyka, E., *Cybersecurity in the Visegrad Group Countries*, Lex Localis Press, Maribor 2023.

Bencsik, A., Karpiuk, M., Strizzolo, N., *Information Society Services and Their Cybersecurity*, „Cybersecurity and Law", 2024, nr 11(1), pp. 258-270.

Central Intelligence Agency, http://ciadotgov4sjwlzihbbgxnqg3xiyrg7so2r2o3lt5wz5ypk4sxyjstad.onion/ (adres w Dark Web) , dostęp: 19.05.2024.

Cohen, D., et al., *DANTE: A framework for mining and monitoring darknet traffic. Computer Security–ESORICS 2020: 25th European Symposium on Research in Computer Security, ESORICS 2020, Guildford, UK, September 14–18, 2020, Proceedings, Part I 25*, Springer International Publishing, 2020, https://doi.org/10.48550/arXiv.2003.02575.

Ćwik, B., *Postrzeganie zagrożeń w systemach bezpieczeństwa organizacji*, „Modern Management Review", 2017, nr 3, pp. 27-37.

DANTE, *DANTE- Detecting and analysing terrorist-related online contents and financing activities*, https://www.h2020-dante.eu/, dostęp: 22.05.2024.

Foy, K., *Artificial intelligence is helping investigators fight crime on the dark web*, Lincoln Laboratory. Massachusetts Institute of Technology 2019, https://www.ll.mit.edu/news/artificial-intelligence-helping-investigators-fight-crime-dark-web, dostęp: 19.05.2024.

Huczek, K., *Cyfrowi tubylcy i cyfrowi imigranci. O społecznych wyzwaniach i zagrożeniach w cyberprzestrzeni*, „Cybersecurity and Law", 2023, nr 10(2), pp. 414-429.

Ismailova, L., Wolfengagen, V., Kosikov, S., *A Semantic Model for Indexing in the Hidden Web*, „Procedia Computer Science", 2021, nr 190, pp. 324-331.

Kaczmarek, K., *Darknet jako przedmiot badań nauk społecznych*, „Cybersecurity and Law", 2020, nr 4(2), pp. 105-113.

Karpiuk M., *Crisis management vs. cyber threat*, „Sicurezza, terrorismo e società", 2022, nr 16(2), pp. 113-123.

Karpiuk M., Pizło W., Kaczmarek K., *Cybersecurity Management – Current State And Directions Of Change*, „International Journal of Legal Studies", 2023, nr 2, pp. 645-663.

Kaur, S., Singh, A., Geetha, G., Cheng, X., *IHWC: intelligent hidden web crawler for harvesting data in urban domains*, "Complex & Intelligent Systems", 2023, nr 9(4), pp. 3635-3653.

Khan, G. A., *The Web Layers: Security Challenges and Solutions in Surface, Deep and Dark Web*, SSRN 2024, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4722851, dostęp: 19.05.2024.

Nazah, S., et. al., *Evolution of Dark Web Threat Analysis and Detection: A systematic Approach* "Ieee Access", 2020, nr 8, pp. 171796-171819.

OnionLinks, http://s4k4ceiapwwgcm3mkb6e4diqecpo7kvdnfr5gg7sph7jjppqkvwwqtyd.onion/ (adres w Dark Web), dostęp: 19.05.2024.

Wasilewski, K., *Fake News and the Europeanization of Cyberspace*, „Polish Political Science Yearbook", 2021, nr 50(4).

Weimann, G., *Going Darker? The Challenge of Dark Net Terrorism*, Woodrow Wilson International Center for Scholars, Washington 2021, https://www.wilsoncenter.org/sites/default/files/media/documents/publication/going_darker_challenge_of_dark_net_terrorism.pdf, dostęp: 22.05.2024.

Włodyka E. M., *Polaryzacja, kohabitacja czy integracja? Wyzwania cyberbezpieczeństwa procesów wyborczych w Polsce* [in:] *Cyberbezpieczeństwo. Aspekty krajowe i międzynarodowe*, M. Karpiuk (red.), Wydawnictwo Akademii Sztuki Wojennej, Warszawa 2024.

Włodyka, E. M., Kaczmarek, K., *Cyber Security of Electrical Grids – A Contribution to Research*, „Cybersecurity and Law", 2024, nr 2(12), 22. 260-272.

„dot.pl" - czasopismo Rejestru domeny .pl

New challenges of local and regional public service provision: platforms and their cybersecurity issues

István Hoffman
Eötvös Loránd University (Budapest), Faculty of Law, Hungary
ORCID: https://orcid.org/0000-0002-6394-1516
E-mail: hoffman.istvan@ajk.elte.hu

Received: 25.04.2024
Accepted: 24.05.2024
Published: 27.05.2024

Cite this article as:
Is.Hoffman, "New challenges of local and regional public service provision: platforms and their cybersecurity issues"

DOT.PL, no. 1/ 2024,
10.60097/DOTPL/189319

Corresponding author:
E-mail:
hoffman.istvan@ajk.elte.hu

Abstract

Public service provision and administration have been transformed by the digitalization and application of information and communication technologies (ICT). My paper will focus mainly on the impact of these changes on the service provision and on the cybersecurity issues. The new, general systems offer a more efficient service provision but it has several, non-primarily perceived impacts. First of all, the 'platformisation' of the local services could be interpreted as a new form of centralization. These platforms are either managed by the central government or the data for the local and regional managed platforms are provided by the central government. The approach of the data management and the data provision has a standardisation, and thus a centralisation effect. The centrally managed platforms and the interface between local and central system has

even cybersecurity issues: these interfaces, and especially the local systems could be vulnerable to cyberattacks.

Keywords: centralization, decentralization, digitalization, public service provision, cybersecurity

Introduction

In the developed democratic states, the administration and management of local public affairs is inconceivable without local self-governance. Local and regional governments and the services provided by them have a significant impact on the structure of the public administration of a given country. It should be emphasised that the development of information and communication technologies (ICT) resulted a significant change in administrative activities, which transformation impacted the centralization of administrative tasks.[153] This change is significant, because the main elements of the alteration of the system are quite latent, but these modifications can be interpreted as a 'silent revolution' of the local and regional public service provision.

As it has been mentioned later, the platforms as tools of e-governance can be observed in most of the countries, even the administrative systems of the developing countries use the platforms as a tool for performing and managing public administration.[154] However, the evolvement of e-governance and the even extensive application of platforms could be considered as a global phenomenon,[155] but there are differences between the countries and between their approaches. In my paper, I would like to focus on the general elements of this platformisation, but my analysis will partially focus on the approach and system of the Visegrád countries, especially Hungary. These countries have an interesting situation. First of all, they are Member States of the European Union, and therefore they should follow the EU regulation on the protection of critical infrastructure. Secondly, they are

[153] I. Hoffman et al., *New Ways of Providing Public Services: Platforms of Service Provision and the Role of Artificial Intelligence: in the Light of the Development of the Hungarian Public Administration.* In: S. Benković et al. (Eds.), *Digital Transformation of Financial Industry. Approaches and Applications*, Springer, Cham, 2023, pp. 187.
[154] Y. Shen et al., *From recovery resilience to transformative resilience: How digital platforms reshape public service provision during and post COVID-19,* „Public Management Review" 25 (4), 2023, pp. 712-714.
[155] S. Kim et al., *Platform Government in the Era of Smart Technology,* Public Administration Review 82 (2), 2022, pp. 363-365.

developing their e-governance systems, and they try to use the e-governance as a tool for economic development, as well. Last, but not least, especially Hungary has been introduced obligatory application of e-services and administrative platforms for several legal subjects in the last two decades, therefore, the evolvement of these systems is strongly supported by the legislation and by central government policies.[156]

Methods

My paper is based on a jurisprudential analysis. First of all, I would like to analyse the models and paradigms of the municipal systems, because the municipal e-administration is part of the municipal policies. These policies are strongly influenced by the given municipal systems. The examination will focus on the public service provision. The platforms as centralised and standardised systems are more effective than the fragmented e-systems, but based on this concentration, several vulnerability threats could be observed. Therefore, the cybersecurity issues of the local platforms will be analysed.

However, the major method of the analysis will be jurisprudential. Similarly, the policies on e-local government will be reviewed shortly.

Platforms and public administration

It is emphasised by the literature that that platforms can be approached from several angles: firstly, as a specific product development outcome, secondly, as a specific technological strategy, and thirdly, as an industrial economic phenomenon.[157] Platforms can also be analysed as a specific network, typically connected to the Internet, and as a specific ecosystem. Platforms are interpreted by the market theory as both a network interface connecting two groups and a system that creates value through a common architecture. The interpretation of technology management approach is based on the network nature of the platforms. It is emphasised by this approach that they are standardised ecosystems which are highly interconnected and systemised. Strategic

---

[156] A. Bencsik, M. Karpiuk & N. Strizzolo: *Information Society Services and Their Cybersecurity,* „Cybersecurity and Law" 11 (1): 258-270 (2024), pp. 262-266.

[157] Y. B. Carliss & C. J. Woodard: *The architecture of platforms: a unified view*. In A. Gawer (ed.): *Platforms, Markets and Innovation*. Edward Elgar, Cheltenham (UK) – Northampton (MA, USA), 2009. p. 19-20.

management looks at the corporate operation of the platform as a network and the system of processes that create value. On the one hand, the best-known platforms are systems linked to the provision of services, such as various data analytics platforms. However, the role of platforms is much broader than that: in fact, modern corporate governance relies extensively on these solutions, which are standardised and easily adaptable to the company's own processes and to other companies' systems. In this context, I would like to highlight the different enterprise performance management systems, for example the SAP system as an example of a widely used solution. It should be emphasised that the above-mentioned platform definitions are also applicable to the analysis of public administration activities.[158]

Because of the widespread application of platforms, they have also become strongly embedded in the regulatory issues of public administration. Public attention has focused primarily on the regulation of the above-mentioned platforms which are based on the sharing economy. However, the infocommunications revolution has also had a significant impact on the activities of public administrations, and the emergence of e-government has been influenced by platforms.[159]

It is undeniable that the digital revolution has now reached public administrations. E-government brings many benefits. For example, customers are not bound by office hours, they do not have to meet officials, they have easier access to information and a range of tools to help them make decisions. E-government is an umbrella term: in the literature it is used to describe government innovation and government information and services. The goal of e-government is often defined as paperless offices, meaning that electronic administration transforms paper-based processes into electronic processes. E-government creates many ways for governments and citizens to communicate with each other. As a result, customers have become actors in the administrative system.[160] Therefore, eGovernment is a tool for economic development. Simplified procedures and

[158] A. Hein et al., *Digital platform ecosystems,* "Electronic Markets" 30. (2020), 87-98. p. 87-89.
[159] E. Vasilieva, *Digital Public Service Platforms: Challenges and Opportunities.* In: E. Zaramenskikh et al. (eds): *Digital Transformation and New Challenges. Lecture Notes in Information Systems and Organisation, vol 40,*) Springer, Cham, 2020. pp. 13-16.
[160] Kim et al., *op. cit.* pp. 362-364.

automation of decision-making can speed up procedures, which in turn can lead to a reduction in administrative costs. Therefore, the literature considers investment in e-government as an investment in economic development. Taking into account the impact and results of platforms in economic life, some public administrations have also started to adopt platform-like solutions relatively early, at the turn of the millennium. In the Hungarian public administration, systems have also emerged that ultimately fit different descriptions of platforms: thus, the general government electronic administration system, the Customer Gateway, and, closely related to it, the Central Identification Agent can be clearly described as such a specific network and ecosystem.[161]

If we look at the development of the European systems, we can point out that platform-like solutions were the first and most widespread in the field of financial administration, mainly in the area of public revenue management and payment.[162] Later, several such administrative sector solutions were developed, including those related to public revenues, for example in the field of social security and construction administration. Various platforms have also been developed in other areas of traditional public administration. Platform-like solutions have also appeared in the area of property registration, such as the electronic land registry system and the vehicle locator. The range of these platforms for registration has been continuously expanding in recent years. These platforms were essentially related to administrative-public authority functions, i.e. traditional public authority administrative activities, including public authority enforcement and, to some extent, public authority supervisory activities.[163]

Public administrations also provide a wide range of public services. Given that economic platforms have been particularly successful in the field of services, it is logical that these solutions have also been introduced in the field of public services in the various public administrations. These platforms for service information and administration have also appeared in the public services organised by the Hungarian public administration. Thus,

---

[161] Hoffman et al., *op. cit.* pp. 184-188.
[162] A. Drigas et al., *Government Online: An E-Government Platform to Improve Public Administration Operations and Services Delivery to the Citizen*. In: M. D. Lytras *et al.* (eds.) *Visioning and Engineering the Knowledge Society. A Web Science Perspective,* Springer, Berlin & Heidelberg, 2009. p. 523-532.
[163] Vasilieva, *op. cit.* pp. 14-18.

in the field of social security services and, in particular, health services, such solutions have already been developed at the turn of the millennium. These systems have been adapted several times and the services they provide and the data they handle have been continuously extended. The role of these health service platforms has been increased during the COVID-19 pandemic, because it could offer the possibility of telemedicine and thus to decrease the personal interactions and the risk of infections.[164] Similarly, the COVID-19 pandemic has brought to the fore platforms in the field of education. The first platforms in higher education have been developed during the Millennia. The higher education has been internationalised even in the field of platforms, major systems (for example Coospace, Canvas, Moodle and kahoot!) have been developed and they are widely used by the different higher education systems. The individual university systems were based on these engines. During the 2010s, based on the classroom and on-line conference management systems, the universities have built systems which are integrated with these conference and classroom engines (for example Zoom, Webex and the MS Teams). These systems have been widely used by universities during the different emergency situations of the polycrisis of the 2020s.[165]

Platforms as a tool of 'stealth centralisation'?

The latent, 'stealth' centralisation has also taken on 21st century forms. With the informatics 'revolution', the widespread application of ICT and the emergence of the information society, information and data related to public services are becoming increasingly important. In the majority of the developed countries, these data systems and platforms are generally organised by the central government. Since without this data, the new types of public service organisation solutions for local authorities, which are extensively based on digital solutions and which in many cases are linked to the smart city concept, cannot be implemented or can only be implemented to a limited extent, the ownership of and access to data has also led to a kind of centralisation in these countries, which is only indirectly perceived at first sight. This centralisation is similar to the above-

[164] D. M Mann et al., *COVID-19 transforms health care through telemedicine: Evidence from the field, "Journal of the American Medical Informatics Association"*, 27 (7), 2020, pp.1132-1135.
[165] V. Shevchenko at al., *Distance Learning in Ukraine in COVID-19 emergency,* "Open Learning: The Journal of Open, Distance and e-Learning", 39 (1), 2024, pp. 5-7.

mentioned transformation of the business sector: the introduction of corporate digital ecosystems – for example, one of the most known is the System Applications and Products in Data Processing (hereinafter: SAP), which is the leading software in Enterprise Resource Planning market[166]– resulted the centralisation of the company management and the standardisation of the different corporate procedures and activities[167]. The corporate ecosystem of the multinational companies has been more centralised after the introduction of these platforms because the former differences in procedures and management have been disappeared.[168] The impact of the ICT on public service is similar to the digital transformation of the business sector. However, these alterations are quite visible, the digital transformation is the 'stealthy' one, but the evolvement of the public service provision platforms could be interpreted as a very real and significant centralisation. This latent centralisation is also evident in Australia.[169]

Cybersecurity and platforms

Cybersecurity became an important issue of the municipal administration after the Millennials, especially after 2010, when the eGovernment and the municipal e-services begun to evolve rapidly.[170]

After the challenges of the new era, especially to ensure a better defence of the administrative cyberspace, a new regulatory approach has been evolved after 2010. These regulatory issues were accelerated by significant cyberattacks and the experiences of these attacks and the defense against them. Mainly centrally supervised systems have been regulated.

---

[166] T. Leimbach, *The SAP Story: Evolution of SAP within the German Software Industry,* "IEEE Annals of the History of Computing" 30 (4), 2008, pp. 62-64.

[167] A. Hein et al., *Digital platform ecosystems,* Electronic Markets: 30, 2020, pp. 88-90;
J. Kostrubiec, *Preventing the Abuse of the FinTech Sector for Money Laundering and Fiscal Fraud in Terms of Polish Law: Legal Measures and Postulates of Normative Changes,* [in:] S. Benković et al. (eds.), *Digital Transformation of Financial Industry. Approaches and Applications*, Springer, Cham 2023. p. 192.

[168] F. Ludacka et al., *Digital Transformation of Global Accounting at Deutsche Bahn Group: The Case of the TIM BPM Suite*, In: J. von Brocke et al. (Eds.), *Business Process Management Vol 2. Digital Transformation- Strategy, Processes and Execution*, Springer, Cham, 2021, pp. 58-61.

[169] R. Tomlinson, *The failure to learn from others: vertical fiscal imbalance, centralisation and Australia's metropolitan knowledge deficit,* Austrialian Journal of Public Administration, vol.78 (2), 2019, pp. 218-221.

[170] M. Czuryk et al., *The legal status of local self-government in the field of public security*, "Studia nad Autorytaryzmem i Totalytaryzmem", 41 (1), 2019, pp. 34-36.

It should be emphasised that the major challenges of the municipal cybersecurity are linked to nationally defined requirements. Especially in those countries which have fragmented municipal systems, and the number of the local offices are quite high, the local offices are quite small. These offices have often lack of resources and lack of human capacities, especially in the field of cybersecurity.

The majority of the civil servants of the municipal offices have limited training in the field of cybersecurity, even in larger, urban municipalities.[171] It should be emphasised, that not only the lack of resources for a more developed cybersecurity defence hardware and software is a major element of the vulnerability of the municipal systems.[172] Another threat of these system is the human factor.[173] Those municipal officers who have not been trained on avoiding cyberattacks based on the inexperience of the platform users could be a significant threat on these centralised platforms, as well. It is emphasised by the literature, that one of the most significant vulnerability factors of these systems are the human users, because their inexperience could result in large scale cyberattacks, as well. Similarly, the increasing number of the users and interfaces result an increasing threat on these systems. Therefore, those general systems which are linked to the municipal systems and have a large number of users have a more significant risk of vulnerability. [174] Because of the existence of delegated state tasks, these municipalities have links to the central systems, especially to the registrations of the population and their addresses. Therefore, these small offices can be an Achilles heel of the fragmented systems, because they are more vulnerable than the national(ised) systems.[175] Similarly, the university systems could be considered such a vulnerability because of the great range of interfaces and users.[176] Thus, the central governments have significant tasks in

[171] B. Preis et al., *Municipal Cybersecurity: More Work Needs to Be Done,* „Urban Affairs Review" 58 (2), 2022, pp. 620-624.
[172] *Idem,* pp. 621-623.
[173] V. Dutt, Y-S. Ahn et al., *Cyber Situation Awareness: Modeling Detection of Cyber Attacks With Instance-Based Learning Theory,* „Human Factors", 55 (3), 2013, pp. 607-609.
[174] M. Ovelgönne et al., *Understanding the Relationship between Human Behavior and Susceptibility to Cyber Attacks: A Data-Driven Approach,* "ACM Transactions on Intelligent Systems and Technology", 8 (4), 2017, pp. 17-20.
[175] I. Hoffman et al., *The local self-government's place in the cybersecurity domain. Examples of Poland and Hungary,* "Cybersecurity and Law", 7 (1), 2022, pp. 184-186.
[176] C. Melchior et al., *Security of Personal Data in Cyberspace in the Opinion of Students of the University of Udine,* "Cybersecurity and Law", 11 (1), 2024, pp. 232-235.

strengthening the municipal cybersecurity. And as it can be seen, it is not enough to issue legislative and regulatory acts, but even the local trainings should be supported by the central government. Because of these centralised platforms, the municipal cybersecurity is not only a local issue; it has significant impact on the national systems, as well.[177]

Conclusions

The digitalisation and the e-administration are important issues of the public administration reforms of the last decades. The challenges of the new, digital ages resulted the transformation of the traditional administration. As we reviewed, the regulation on e-Government and on the digitalisation of the public administration transformed significantly. The regulation was focused on the development a horizontally integrated e-administration. The municipal e-administration systems have been built by the municipalities (especially by the larger municipalities), but their operation could be developed. The regulation and the supervision activities of e-Government are detailed regulated and have evolved quickly during the last years, and its focus have been partly transformed. Not only the individual decisions, but even the provision of public services have become digitalised. The new, centrally operated platforms can be even interpreted as a ne, 'soft' tool of the centralisation.

Literature

Bencsik A, Karpiuk M. & Strizzolo N., *Information Society Services and Their Cybersecurity,* „Cybersecurity and Law" 11 (1): 258-270 (2024), https://doi.org/10.35467/cal/188446

Carliss Y. B., Woodard C. J., *The architecture of platforms: a unified view,* [in:] A. Gawer (ed.), *Platforms, Markets and Innovation,* Edward Elgar, Cheltenham (UK) – Northampton (MA, USA), 2009. pp. 19-44, https://doi.org/10.4337/9781849803311

Czuryk M., Kostrubiec J., *The legal status of local self-government in the field of public security,* "Studia nad Autorytaryzmem i Totalytaryzmem" 41 (1)33-47, 2019, http://dx.doi.org/10.19195/2300-7249.41.1.3

Drigas A., Koukianakis L., *Government Online: An E-Government Platform to Improve Public Administration Operations and Services Delivery to the Citizen,* [in:] M. D. Lytras et al. (eds.) *Visioning and Engineering the Knowledge Society. A Web Science Perspective. WSKS 2009.* Springer, Berlin & Heidelberg, 2009, pp. 523-532, http://dx.doi.org/10.1007/978-3-642-04754-1_53

[177] I. Hoffman et al., *E-Administration in Polish and Hungarian Municipalities – a Comparative Analysis of the Regulatory Issues* "Lex localis – Journal of Local Self-government", 20 (3): 2022, pp. 633-637.

Dutt V, Ahn Y-S. & Gonzalez C., *Cyber Situation Awareness: Modeling Detection of Cyber Attacks With Instance-Based Learning Theory,* „Human Factors" 55 (3): 605-618 (2013), https://doi.org/10.1177/0018720812464045

Hein A. et al., *Digital platform ecosystems,* "Electronic Markets" 30: 87-98 (2020), https://doi.org/10.1007/s12525-019-00377-4

Hein A., Schreieck M., Risanow T., Setzke D. S., Wiesche M., Böhm M, Krcmar H., *Digital platform ecosystems,* "Electronic Markets" 30: 87-98. (2020) http://dx.doi.org/10.1007/s12525-019-00377-4

Hoffman I., Bencsik A., *New Ways of Providing Public Services: Platforms of Service Provision and the Role of Artificial Intelligence: in the Light of the Development of the Hungarian Public Administration*, [in:] S. Benković, A. Labus, & M. Milosavljević (Eds.), *Digital Transformation of Financial Industry. Approaches and Applications* (pp. 171-190), Springer, Cham, 2023. https://doi.org/10.1007/978-3-031-23269-5_10

Hoffman I., Karpiuk M., *The local self-government's place in the cybersecurity domain. Examples of Poland and Hungary,* "Cybersecurity and Law" 7 (1): 171-190. (2022), http://dx.doi.org/10.35467/cal/151826

Hoffman I., Karpiuk M., *E-Administration in Polish and Hungarian Municipalities – a Comparative Analysis of the Regulatory Issues* "Lex localis – Journal of Local Self-government" 20 (3): 617-640 (2022), https://doi.org/10.4335/20.3.617-640(2022)

Kim S., Andersen K. N. & Lee J., *Platform Government in the Era of Smart Technology,* Public Administration Review 82 (2): 362-368 (2022), https://doi.org/10.1111/puar.13422

Kostrubiec J., *Preventing the Abuse of the FinTech Sector for Money Laundering and Fiscal Fraud in Terms of Polish Law: Legal Measures and Postulates of Normative Changes*, [in:] S. Benković, A. Labus & M. Milosavljević (Eds.), *Digital Transformation of Financial Industry. Approaches and Applications* (pp. 191-201), Springer, Cham, 2023. http://dx.doi.org/10.1007/978-3-031-23269-5_11

Leimbach T., *The SAP Story: Evolution of SAP within the German Software Industry,* "IEEE Annals of the History of Computing" 30 (4): 60-76 (2008), http://dx.doi.org/10.1109/MAHC.2008.75

Ludacka F., Duell J., Waibell P., *Digital Transformation of Global Accounting at Deutsche Bahn Group: The Case of the TIM BPM Suite,* [in:] J. von Brocke, J. Mendling & M. Rosemann (Eds.), *Business Process Management Vol 2. Digital Transformation- Strategy, Processes and Execution* (pp. 57-68), Springer, Cham, 2021, http://dx.doi.org/10.1007/978-3-662-63047-1_5

Mann D. M, Chen J., Chunara R., Testa P. A, Nov O., *COVID-19 transforms health care through telemedicine: Evidence from the field*, "*Journal of the American Medical Informatics Association",* 27 (7): 1132-1135 (2020), https://doi.org/10.1093/jamia/ocaa072

Melchior C., Soler U., *Security of Personal Data in Cyberspace in the Opinion of Students of the University of Udine,* "Cybersecurity and Law" 11 (1): 227-247 (2024), https://doi.org/10.35467/cal/188451

Ovelgönne M., Dumitraş T, Prakash B. A.,Subrahmanian V. S. & Wang B., *Understanding the Relationship between Human Behavior and Susceptibility to Cyber Attacks: A Data-Driven Approach,* "ACM Transactions on Intelligent Systems and Technology" 8 (4): 1-25 (2017), https://doi.org/10.1145/2890509

Preis B., Susskind L., *Municipal Cybersecurity: More Work Needs to Be Done,* „Urban Affairs Review" 58 (2): 614-629 (2022), https://doi.org/10.1177/1078087420973760

Shen Y, Cheng Y. & Yu J., *From recovery resilience to transformative resilience: How digital platforms reshape public service provision during and post COVID-19,* „Public Management Review" 25 (4): 710-733 (2023), https://doi.org/10.1080/14719037.2022.2033052

Shevchenko V., Malysh N., Tkachuk-Miroshnychenko O., *Distance Learning in Ukraine in COVID-19 emergency*, "Open Learning: The Journal of Open, Distance and e-Learning" 39 (1): 4-19. (2024), https://doi.org/10.1080/02680513.2021.1967115

Tomlinson R., *The failure to learn from others: vertical fiscal imbalance, centralisation and Australia's metropolitan knowledge deficit,* "Australian Journal of Public Administration" 78 (2): 213-226 (2019), https://doi.org/10.1111/1467-8500.12387

Vasilieva E., *Digital Public Service Platforms: Challenges and Opportunities*. In: Zaramenskikh E. & Fedorova A. (eds): *Digital Transformation and New Challenges. Lecture Notes in Information Systems and Organisation, vol 40*. (pp. 11-23.) Springer, Cham, 2020. https://doi.org/10.1007/978-3-030-43993-4_2

„dot.pl" - czasopismo Rejestru domeny .pl

Freedom of Expression on the Internet and National Security in Europe: Liberty and Basic Goods

Luka Martin Tomažič
Institutum Studiorum Humanitatis, Alma Mater Europaea University, Slovenska ulica 17, 2000, Maribor, Slovenia
ORCID: 0000-0002-2296-0489
E-mail: luka.tomazic@almamater.si

Received: 29.07.2024
Accepted: 27.08.2024
Published: 28.08.2024

Cite this article as:
Luka M. Tomažič, "*Freedom of Expression on the Internet and National Security in Europe: Liberty and Basic Goods*"

DOT.PL, no. 1/ 2024,
10.60097/DOTPL/192648

Corresponding author:
Luka Martin Tomažič
Institutum Studiorum Humanitatis, Alma Mater Europaea University, Slovenia
E-mail:
luka.tomazic@almamater.si

Abstract

XThe tension between freedom of expression and the protection of national security is a timeless research problem. Based on the specific historical moment and international political and security situation for Europe in general and the Three Seas region specifically, the aim of this article will be a normative assessment of the appropriate approach to potential limitations on online freedom of expression considering national security. The starting point will be an overview of the state of the art of the European Court of Human Rights practice. Then, the analytical framework of Berlin's two concepts of liberty will be utilised to differentiate between laissez-faire approaches connected to the first paragraph of Article 10 and the limitations, which are necessary in a democratic society per the second paragraph of Article 10 of the European Convention on the Human Rights and

Fundamental Freedoms. In a novel approach to the problem at hand, the main research hypotheses that are subject to analysis are that there is a need for a more nuanced approach to balancing online freedom of expression and national security and that Berlin's two concepts of liberty, when connected to Finnis's basic goods, can be a useful normative framework in this regard. The need to differentiate between values and facts while recognising the incommensurability of values will be considered.

Keywords: Freedom of Expression, National Security, ECHR, Internet, Liberty,

1. Introduction

We are situated in the historical moment when Europe and European Union more broadly and the Three Seas region[178] specifically are facing a myriad of novel threats, from Russian aggression on Ukraine and thinly-veiled threats with nuclear annihilation,[179] to hybrid warfare utilising migration,[180] disinformation campaigns[181] and (primarily) Islamist terrorism.[182] Such circumstances, in combination with the rise of utilisation of artificial intelligence in novel forms, especially regarding large language models and generative artificial intelligence,[183] pose new societal questions regarding freedom of expression on the internet. One of them is the potential need for (re)conceptualisation of the existing relationship between freedom of expression and national security, especially in terms of balancing liberty with the protection of basic goods.

---

[178] G. Grgić, *The changing dynamics of regionalism in Central and Eastern Europe: The case of the Three Seas Initiative, "*Geopolitics", vol. 28, no. 1, 2023, pp. 216-238.
[179] M.J. Williams, *Who's Afraid of the Bomb?: The Euromissiles Crisis and Nuclear Weapons in Europe, Past and Present, "*International Studies Review", vol. 26, no. 1, 2024, viae008.
[180] J. Straczuk, *Hybrid war, military humanitarianism, and epistemic friction. Framing illegalised migration on the Polish-Belarusian border*, "Journal of Ethnic and Migration Studies", 2023, pp. 1-19.
[181] A. Jacuch, *Czech-Russian Relations. Russian Disinformation Campaign*, "Polish Political Science Yearbook", vol. 1, no. 53, 2024, pp. 145-166.
[182] P.R. Neumann, *Europe's jihadist dilemma,* "Survival, Routledge", 2023, pp. 71-84.
[183] E. Ferrara, *GenAI against humanity: Nefarious applications of generative artificial intelligence and large language models*, "Journal of Computational Social Science", 2024, pp. 1-21.

While the tension of the need for as free societal expression of opinions as possible and national security considerations is not entirely novel, the contemporary tools and new-found determination of different hostile and potentially adversary actors to spread disinformation and influence democratic processes in individual states and Europe more broadly, are putting the scientific and societal discussions in a new light. The aim of this article is to conceptualise the idea of freedom of expression on the internet and its balancing with national security consideration in line with the two concepts of liberty,[184] while proposing the basic goods that might make the limitations on freedom of expression justified. The attempt is not as ambitious to claim to solve all the normative dilemmas, but it does aim to contribute to the ongoing debates in a productive and doctrinally novel manner, especially regarding the connection of freedom of expression with the basic values.

Due to the number of potentially relevant national jurisdictions, the scope of this article will be limited to the European Convention of Human Rights and Fundamental Freedoms legal framework, especially considering its transnational and supranational relevance and the close connection between constitutional discussions on freedom of expression in the Three Seas region and the practice of the European Court of Human Rights.[185] A further research limitation will be the article's focus on the freedom of expression on the internet. While there might be a large degree of overlap between legal treatment of online and offline expression, unless specifically stated otherwise, online freedom of expression in connection with the internet will be the subject of this article.

In analysing the liberty-related aspects of limiting online freedom of expression on national security grounds, Berlin's two concepts of liberty will be used as the default theoretical framework.[186] In ascertaining the relevance of the relevant values, Finnis's neo-Thomist basic goods will be the starting point of exploration and incommensurability of values will be taken into account.[187]

---

[184] I. Berlin, *Two Concepts of Liberty*, "Reading Political Philosophy, Routledge", 2014, pp. 231-237.
[185] L. Nalyvaiko et al., *Application of the principle of the rule of law international and national courts*, "Щорічник", 2023, p. 143.
[186] I. Berlin, *Two Concepts of Liberty*, Reading Political Philosophy, Routledge, 2014, pp. 231-237.
[187] J. Finnis, *Natural law and natural rights*, "Oxford University Press", 2011.

Methodology will be primarily rooted in the fields of law and philosophy. Logical, dialectical and dogmatic methods will be used to assure the rigorousness of reasoning, the arrival at relevant conclusion through an internal process of considering different scientific, legal and philosophical standpoints and through treating law itself as a normative phenomenon which influences the societal conduct of legal subjects, respectively. Philosophical theories will be utilised primarily in the manner of applied ethics and political philosophy, to shed light on the analysed normative legal issues.

After the introduction, the second heading will focus on researching freedom of expression in the European Court of Human Rights framework and national security. Third heading will be dedicated to the need for positive liberty and fourth will deal with the basic values in limiting freedom of expression for national security reasons. Finally, yet importantly, conclusions will follow and potential avenues for future research will be sketched.

2. Freedom of Expression in the ECHR Framework and National Security

Considerations of national security as a part of the requirement of any interference with the freedom of expression being necessary in a democratic society[188] have featured less prominently than some other potentially legitimate reasons for restricting speech and other modes of expression. While the Council of Europe's analytic guide on the freedom of expression in the European Court of Human Rights practice does offer a good basic overview of court practice,[189] it is lacking in terms of the depth of analysis and additionally needs further contextualisation considering the problematic at hand. Deeper research in the wording of a select number of individual decisions is necessary.

At the outset, it needs to be stated that in certain circumstances, the European Court of Human Rights obviously finds national security to be a legitimate reason for interference

---

[188] H. Fenwick*, Freedom of expression and human rights: Interrogating the focus at Strasbourg on political expression under Article 10 ECHR*, "The Routledge Companion to Freedom of Expression and Censorship*,* Routledge", 2024, pp. 324-333, p. 325.

[189] European Court of Human Rights, *Guide on Article 10 of the European Convention on Human Rights: Freedom of expression,* 2022.

with the general requirement to protect the freedom of expression.[190] This was reflected already in the case of Castells v. Spain, where although in 1992 decision the court found that a violation of defendant's freedom of expression occurred, it at the same time stated that protection of order and national security could be a legitimate reason for interference with freedom of expression, as is clear from the wording of Article 10 of the European Convention on Human Rights and Fundamental Freedoms.[191]

As to specifically regarding the use of internet as a medium and to online expression in general, the European Court of Human Rights considers the internet a platform of utmost importance, especially regarding facilitating news and accessing information.[192] Wholesale blocking of internet access in principle conflicts with the Article 10 of the convention, per court practice.[193] In principle, internet-related expression is to be treated in an analogous manner to offline expression,[194] although there might be a need to adjust the legal concepts to the specific aspects of technology,[195] which would seem to include not only the internet but the application of generative artificial intelligence and large language models as well.

The court practice thus far, regarding balancing freedom of expression with national security, has in principle followed a restrictive approach. In the case of Stoll v. Switzerland, the court's grand chamber argued that national security needs to be applied with restraint, interpreted restrictively, and be brought into play only as a matter of necessity, when used as grounds to interfere with freedom of expression.[196] A similar approach was taken by the court in the Görmüş and Others v. Turkey case, where it stated

---

[190] Y. Bilousov, Yevhen et al., *The case law of the European Court of Human Rights on the protection of Human Rights and freedoms in terms of national security protection,* 2022, p. 80.

[191] European Court of Human Rights, *Castells v. Spain*, 23 April 1992, Series A no. 236.
[192] European Court of Human Rights, *Delfi AS v. Estonia* [GC], no. 64569/09, ECHR 2015; A. Wiśniewski, *The European Court of Human Rights and Internet-Related Cases*, "Białostockie Studia Prawnicze", vol. 3, no. 26, 2021, pp. 109-133.
[193] European Court of Human Rights, *Ahmet Yıldırım v. Turkey*, no. 3111/10, ECHR 2012, § 67; M.Fazaeli et al., *A Reflection on the Protection of Freedom of Expression in the Case Law of European Court of Human Rights as to Blocking the Access to Internet,* ModernTechnologies Law, vol. 2, no. 4, 2021, pp. 155-182.
[194] European Court of Human Rights, *Ashby Donald and Others v. France*, no. 36769/08, 10 January 2013, § 34.
[195] European Court of Human Rights, *Editorial Board of Pravoye Delo and Shtekel v. Ukraine*, no. 33014/05, ECHR 2011, § 63.
[196] European Court of Human Rights, *Stoll v. Switzerland* [GC], no. 69698/01, ECHR 2007-V, § 54.

that while the concept of national security may be utilised by military authorities, it should be applied with restraint, interpreted restrictively, and resorted to only as a matter of necessity.[197]

More leeway is given by the court to national authorities in specific connection with the cases related to combating and preventing terrorism.[198] In the Leroy v. France case, the court emphasized the need for case-by-case evaluation of compliance with the necessity in a democratic society standard and noted the difficulty of punishing the apology terrorism without interfering with freedom of expression at least to a certain degree.[199] While in Karatas v. Turkey, the court merely took note of the problems linked to the prevention of terrorism,[200] in Mahi v. Belgium, the interference with freedom of expression of a person in position of authority, stating criticism of a journalistic institution that was a victim of terrorism, was deemed to be legitimate.[201]

As far as political speech is concerned, the European Court of Human Rights has not been particularly receptive to national security grounds for limiting the freedom of expression. It namely views this particular liberty as being of special importance for the democratic process and the political health of individual societies.[202] Thus, in a number of Turkey-related cases, it has shown that any interference with freedom of expression that concerns politicians or political speech, is assessed in a specifically stringent manner.[203]

A particular problem is posed by the new forms of disinformation, including in terms of utilisation in hybrid warfare by nefarious actors. While the case law is still very much under development and not all of it relates to the Article 10 of the European Convention

---

[197] European Court of Human Rights, *Görmüş and Others v. Turkey*, no. 49085/07, 19 January 2016, §§ 37-38.
[198] J. Sikuta, *Threats of Terrorism and the European Court of Human Rights*, "European Journal of Migration and Law", vol. 10, no. 1, 2008, pp. 1-10.
[199] European Court of Human Rights, *Leroy v. France*, no. 36109/03, 2 October 2008, §§ 37-38.

[200] European Court of Human Rights, *Karataş v. Turkey*, no. 23168/94, ECHR 1999-IV, § 51.

[201] European Court of Human Rights, *Incal v. Turkey*, 9 June 1998, Reports of Judgments and Decisions 1998-IV.
[202] T. Tsomidis, Theo, *Freedom of expression in turbulent times–comparative approaches to dangerous speech: the ECtHR and the US Supreme Court*, "The International Journal of Human Rights, vol. 26, no. 3, 2022, pp. 379-399, p. 381.
[203] European Court of Human Rights, *Yalçıner v. Tu"rkey*, no. 64116/00, 21 February 2008; European Court of Human Rights, *Incal v. Turkey*, 9 June 1998, Reports of Judgments and Decisions 1998-IV; European Court of Human Rights, *Faruk Temel v. Turkey*, no. 16853/05, 1 February 2011.

on Human Rights and Fundamental Freedoms, some general lines of argumentation are emerging and can be inferred from the existing court practice and court's reasoning.

In Mouvement Raëlien Suisse v. Switzerland case, the court noted that states have a certain margin of appreciation when dealing with imparting ideas in public space and that the right of individuals to use the public space in this regard is not unconditional or unlimited, especially in relation to advertising or information campaigns.[204] In the Delfi AS v. Estonia judgment, the court emphasized special importance of the press and internet itself as it emphasized the need for a thorough substantiation of any grounds for limiting freedom of expression in the interest of preventing disinformation. [205]

Similarly, special protection of journalists was argued by the court in other cases, including Jersild v. Denmark.[206] While pursuing a noble aim of protecting the journalistic endeavour, at the same time it might be practically problematic in certain situations in the context of foreign agents posing as journalists[207] and the proliferation of freelance journalism on the internet.[208] The blocking of internet access is in any case especially limited per court practice, an action of last resort and must be extremely well substantiated and reasoned.[209]

3. The Need For Positive Liberty

In moving from a descriptive to normative understanding of the interrelation between freedom of expression on the internet and national security, first a conceptualisation is needed. Since the value of freedom, sometimes interchangeably known as liberty, is at

[204] European Court of Human Rights, *Mouvement raëlien suisse v. Switzerland* [GC], no. 16354/06, ECHR 2012, § 58 and 76.
[205] European Court of Human Rights, *Delfi AS v. Estonia* [GC], no. 64569/09, ECHR 2015.
[206] European Court of Human Rights, *Jersild v. Denmark*, 23 September 1994, Series A no. 298
[207] P. Lashmar, *Putting lives in danger? Tinker, tailor, journalist, spy: the use of journalistic cover*, "Journalism", vol. 21, no. 10, 2020, pp. 1539-1555.
[208] B. Josephi et al., *The blurring line between freelance journalists and self-employed media workers*, "Journalism", vol. 24, no. 1, 2023, pp. 139-156.
[209] G. Gosztonyi, *The European Court of Human Rights: Internet Access as a Means of Receiving and Imparting Information and Ideas*, »International Comparative Jurisprudence«, vol. 6, no. 2, 2020, pp. 134-140.

the core of the notion of freedom of expression itself, it is a lens through which the forthcoming analysis will be performed.

An appropriate way to conceptualise the tension between laissez-faire approaches and approaches aiming at the common good through imposing certain limitations on freedom of expression is through Berlin's two concepts of liberty. In this sense, negative liberty is a specific value, a separate ideal from positive liberty and is in concrete characterised by permitting the full scope of exercising the freedom of expression.[210] This has obvious societal benefits of enabling debate and ideational battling of different sets of values and assertions of facts in the intellectual or at least public domain.

At the same time, leaving freedom of expression completely unhindered might in certain less peaceful times enable adversaries and nefarious actors to run rampant, especially considering the novel forms of applications of artificial intelligence in the sense of large language models and deep fakes, ensuing a descent into a state of anarchy, or at least destabilisation of established social and public order institutions through election interference and other means. Balancing with positive liberty is thus necessary.

Positive liberty as a separate value has at its core the paternalist intervening of the state.[211] In relation to the freedom of expression, the authorities desire to prevent externalities and protect individuals from other individuals and states.[212] This, in Berlinian terms, includes legislating and deciding with public policy, what it truly means for an individual to be free, which freedom is true freedom. In relation to freedom of expression, it is included in the paragraph two of the Article 10 of the European Convention on Human Rights and Fundamental Freedoms in the context of limitations, necessary in a democratic society.[213]

While as per described practice of the European Court of Human Rights, de lege lata, the default is clearly the value of negative liberty, it can be discussed and proposed when the

---

[210] I. Berlin, *Two Concepts of Liberty*, "Reading Political Philosophy, Routledge", 2014, pp. 231-237, p. 233.
[211] I. Berlin, *Two Concepts of Liberty*, "Reading Political Philosophy, Routledge", 2014, pp. 231-237, p. 235.
[212] J. Stajnko, *Tackling hate speech in Western Balkans*, "Central European political science review", vol. 24, no. 94, 2023, pp. 65-77, p. 65.
[213] G. Gunatilleke, *Justifying Limitations on the Freedom of Expression*, "Human Rights Review", vol. 22, 2021, pp. 91-108, p. 91.

limitations in light of the value of positive liberty, in the name of national security, are appropriate in normative terms. Since the values of positive and negative liberty are two competing ideals,[214] a discussion on choosing one or the other and in which circumstances necessarily entails further reasoning and even valuation.

4. Basic Values in Limiting Freedom of Expression on the Internet for National Security Reasons

When approaching the question of legitimate grounds for limiting online freedom of expression in normative terms, valuation is necessarily at the core of such an endeavour. Since values seem to be incommensurable at least in the abstract sense, they must primarily be chosen.[215] Such a choice is not arbitrary, but reasoned and while there is no common measure for different values, the consequences of the chosen values do play out in human affairs and can themselves be measured and subjected to further valuation.[216]

Within the confines of this article, considering its limitations, we will briefly consider the basic values as proposed by Finnis, then choose and analyse arguably the most important ones. Finnis terms the values at the centre of the focal meaning of the law, in line with the common good, the basic goods and lists seven of them. These are life, knowledge, play, aesthetic experience, friendship, practical reasonableness and religion.[217]

While there might be something to say especially for the values of play, practical reasonableness and religion, I want to zero in especially onto the values of life and knowledge. There are several grounds for such a decision. Firstly, the protection of the value of life seems inherently connected to the notion of national security, or at least its

[214] I. Berlin, *Two Concepts of Liberty*, Reading Political Philosophy, Routledge, 2014, pp. 231-237, pp. 232-233.
[215] J. Finnis, *Natural law and natural rights*, Oxford University Press, 2011; V. Strahovnik, *Robert Audi, The Good in the Right: A Theory of Intuition and Intrinsic Value*, "Croatian Journal of Philosophy", vol. 15, 2005, pp. 583-589; L. Walasek, Lukasz et al., *Incomparability and incommensurability in choice: no common currency of value?* "Perspectives on Psychological Science", 2023, 17456916231192828.
[216] J. Finnis, *Natural law and natural rights*, "Oxford University Press", 2011.
[217] J. Finnis, *Natural law and natural rights*, "Oxford University Press", 2011.

bare minimum. Respectively, the value of knowledge seems to be at the centre of the free exchange of ideas ensured by the upholding of the right to freedom of expression. Furthermore, both values seem to be prone to at least indirect argumentation of their merit even in the abstract sense. Lastly, an overinclusive approach would not be in order, given the extremely restrictive de lege lata approach of the European Court of Human Rights.

Life is an obvious candidate for a basic good at the centre of protection through national security.[218] The importance of the value of life can barely be overstated. Since it is difficult to state that life is not a good and be philosophically consistent while consciously remaining alive, it can be deemed a value of at least some importance even in the abstract. While the national security does as a bare minimum aim at protecting the lives of citizens of an individual country or an alliance of countries, a further step is necessary.

The mere protection of life is not enough, national security is in principle, as it should be, concerned with ensuring enough security for a good life of its citizens, a life worth living.[219] The two undesirable options are sketched by example in Raz's abstracted account. He gives the examples of a man in a pit, who gets food thrown to him but can barely do anything productive with his life.[220] The second account is of a woman who is chased by wild beasts and can always barely escape, living her life in a constant state of psychological terror and physical exhaustion.[221] Especially the second exemplary account underscores the core concern of the programmes of national security.

In protecting online freedom of expression, while life might feature indirectly, protection of the basic good of knowledge is at its core. For a society, free expression serves as an appropriate tool for ascertaining the truth of different sets of facts and at the same time, to reason about the chosen values and their consequences to facilitate human

---

[218] R. Radwański et al., *Premises for Protecting the Polish Population in the Context of the National Security Strategy,* "Journal of Security and Sustainability Issues", vol. 13, no. 1, 2023.
[219] D. Machek, *The Life Worth Living in Ancient Greek and Roman Philosophy*, "Cambridge University Press", 2023.
[220] J. Raz, *The Morality of Freedom*, "Oxford, Oxford University Press", 1986, p. 373.
[221] Ibidem.

flourishing. In abstract, the value of knowledge can be asserted indirectly, since the claim that knowledge is not a value is internally inconsistent.

At the same time, it needs to be understood, that knowledge for knowledge's sake is not enough. It is obvious that pursuit of knowledge is possible in blatant disregard of human life.[222] Thus, even in pursuit of knowledge, moral limitations do and necessarily must apply.

In ascertaining when to give priority to negative liberty, primarily through the choice of the pursuit of the underlying main value of knowledge and protecting freedom of expression and when to give priority to positive liberty and protection of life and human flourishing through national security related measures, a potential approach could be in differentiating between facts and values.[223]

Differentiation between values and facts may not always be straightforward, especially in connection with political speech, but it is nevertheless an analytically useful description.[224] Facts are a matter of observation, and values are a matter of a reasoned judgement of what is good and what is not.[225]

There are two abstract types of facts that could be reason for limitations of freedom of expression, the first being deliberate disinformation and the second being sensitive, confidential information. Disinformation, when it can be ascertained, should be a reason for limiting expression but only when it can be discerned with a high degree of probability. The requirement for confidentiality might also be necessary and should be established considering the ECHR standards on a case-by-case basis.

Regarding values, less leeway is appropriate for limiting expression on national security grounds, to prevent descent into a totalitarian society. Ideologies which clearly oppose

---

[222] H. Gold, Hal, *Unit 731: Testimony*, "Tuttle Publishing", 2011.
[223] N. Mchedlidze, *Modern Challenges to Freedom of Expression: Need for Recalibration of the ECtHR Approach to Facts and Value Judgments*, "Georgian Journal of Comparative Law", vol. 28, 2023.

[224] I.M. Lami, Isabella et al., *A multi-methodological combination of the strategic choice approach and the Analytic Network Process: From facts to values and vice versa,* "European Journal of Operational Research", vol. 307, no. 2, 2023, pp. 802-812.
[225] M. Schroeder, *Value Theory*, The Stanford Encyclopedia of Philosophy (Fall 2021 Edition), E.N. Zalta (red.), URL = https://plato.stanford.edu/archives/fall2021/entries/value-theory/.

both liberty and life might be an exception. European Court of Human Rights already sets sufficient and appropriate standards in this regard.[226] Severity of threat should continue to be taken into account in terms of the necessity of limitation.

In general, differentiating between de lege lata practice of the European Court of Human Rights and de lege ferenda necessities of a shifting societal, multinational and technological landscape, calls for allowing certain slightly broader limitations on the freedom of expression in service of national security than current practice reflects. It requires a clear differentiation between facts, where more limitations should be allowed and values, where a strict primacy of a laissez-faire approach remains appropriate.

The two core values at the centre of the debates should be life and knowledge, both assessed through the competing ideals of negative and positive liberty, where a certain degree of tension and value conflict is inherent. When the basic good of life in the narrower sense, interpreted restrictively, is threatened, national security should be given priority over knowledge. Such an approach will allow for a clearer understanding of the changes in court practice and a better ascertainment of when limitations on freedom of expression in consideration of national security are appropriate.

5. Conclusions

The shifting societal, technological and international circumstances call for a nuanced understanding of freedom of expression on the internet as it relates to national security. When dealing with such complex matters in normative terms, we are like people in a dark room, trying to make sense of a large unknown object. This article contributes to the discussion on appropriate limitations on online freedom of expression grounded in arguments of national security through the competing values of positive and negative liberty.

---

[226] P. Lobba, *Holocaust Denial before the European Court of Human Rights: Evolution of an Exceptional Regime*, "European Journal of International Law", vol. 26, no. 1, 2015, pp. 237-253.

While these are indeed two separate ideals, at the same time, in a novel approach, the article connected the two concepts of liberty to two of Finnis's incommensurable basic goods, reflected in their application as it relates to the freedom of expression. While the idea of negative liberty and the ensuing laissez faire approach are more closely connected to the basic good of knowledge and the prioritisation of unrestrained freedom of expression, the positive liberty in protecting the basic good of life calls for limitations based on the national security considerations. Both sets of values exist in a certain degree of tension, which only case-by-case ascertainment of reasons can resolve.

Applying these values could prove useful to interpret and progressively develop the case law of the European Court of Human Rights. In the normative sense, online disinformation utilising novel technological approaches, such as large language models and generative artificial intelligence cannot remain entirely unchecked. While erring on the side of restrictiveness of limiting freedom of expression on the internet is in order, erroneous facts spread by hostile actors for disinformation purposes are a clear candidate for a stricter approach by the European Court of Human Rights, as it protects not only the basic good of life of citizens, but also contributes to more productive knowledge exchange.

There is a vast potential for future research. In terms of applied ethics, further values could be subjected to reasoning and evaluation. Regarding analysis of the European Court of Human Rights, a more specific focus on disinformation might be relevant and other relevant limitations, not relying on the argument of national security, could be explored. The conceptual framework of analysing the Finnisian basic values behind different concepts, and the consequences of them being chosen considering their incommensurability, could be utilised to provide clarifications regarding other legal problems. Finally, yet importantly, content analysis could be performed on the European Court of Human Rights decisions and relevant scientific debates, to ascertain which values map together with both freedom of expression and national security as textual notions.

The eternal tension of safeguarding free discourse in a democratic society, while protecting members of the same society from nefarious actors abusing their rights will remain relevant. This article strived to provide a slight but meaningful contribution to the

ongoing debates. Hopefully the implementation and further research in value-based approaches to online freedom of expression and a clear differentiation between facts and values could serve to better navigate the tensions between safeguarding individual liberties on the internet while protecting the collective security and promoting common good.

Literature

Berlin, Isaiah, *Two Concepts of Liberty*, Reading Political Philosophy, Routledge, 2014, pp. 231-237.

Bilousov, Yevhen, et al., *The case law of the European Court of Human Rights on the protection of Human Rights and freedoms in terms of national security protection,* 2022.

European Court of Human Rights, *Ahmet Yıldırım v. Turkey*, no. 3111/10, ECHR 2012.

European Court of Human Rights, *Ashby Donald and Others v. France*, no. 36769/08, 10 January 2013.

European Court of Human Rights, *Castells v. Spain*, 23 April 1992, Series A no. 236.

European Court of Human Rights, *Delfi AS v. Estonia* [GC], no. 64569/09, ECHR 2015.

European Court of Human Rights, *Editorial Board of Pravoye Delo and Shtekel v. Ukraine*, no. 33014/05, ECHR 2011.

European Court of Human Rights, *Faruk Temel v. Turkey*, no. 16853/05, 1 February 2011.

European Court of Human Rights, *Görmüş and Others v. Turkey*, no. 49085/07, 19 January 2016.

European Court of Human Rights, *Guide on Article 10 of the European Convention on Human Rights: Freedom of expression*, 2022.

European Court of Human Rights, *Incal v. Turkey*, 9 June 1998, Reports of Judgments and Decisions 1998-IV.

European Court of Human Rights, *Jersild v. Denmark*, 23 September 1994, Series A no. 298.

European Court of Human Rights, *Karataş v. Turkey*, no. 23168/94, ECHR 1999-IV.

European Court of Human Rights, *Leroy v. France*, no. 36109/03, 2 October 2008.

European Court of Human Rights, *Mouvement raëlien suisse v. Switzerland* [GC], no. 16354/06, ECHR 2012.

European Court of Human Rights, *Stoll v. Switzerland* [GC], no. 69698/01, ECHR 2007-V.

European Court of Human Rights, *Yalçıner v. Turkey*, no. 64116/00, 21 February 2008.

Fazaeli, Mostafa, and Mousa Karami, *A Reflection on the Protection of Freedom of Expression in the Case Law of European Court of Human Rights as to Blocking the Access to Internet*, ModernTechnologies Law, vol. 2, no. 4, 2021, pp. 155-182.

Fenwick, Helen*, Freedom of expression and human rights: Interrogating the focus at Strasbourg on political expression under Article 10 ECHR*, The Routledge Companion to Freedom of Expression and Censorship*,* Routledge, 2024, pp. 324-333.

Ferrara, Emilio, *GenAI against humanity: Nefarious applications of generative artificial intelligence and large language models*, Journal of Computational Social Science, 2024, pp. 1-21.

Finnis, John, *Natural law and natural rights*, Oxford University Press, 2011.

Gosztonyi, Gergely, *The European Court of Human Rights: Internet Access as a Means of Receiving and Imparting Information and Ideas*, International Comparative Jurisprudence, vol. 6, no. 2, 2020, pp. 134-140.

Gold, Hal, *Unit 731: Testimony*, Tuttle Publishing, 2011.

Grgić, Gorana, *The changing dynamics of regionalism in Central and Eastern Europe: The case of the Three Seas Initiative,* Geopolitics vol. 28, no. 1, 2023, pp. 216-238.

Gunatilleke, G., *Justifying Limitations on the Freedom of Expression*, Human Rights Review, vol. 22, 2021, pp. 91-108.

Jacuch, Andrzej, *Czech-Russian Relations. Russian Disinformation Campaign*, Polish Political Science Yearbook, vol. 1, no. 53, 2024, pp. 145-166.

Josephi, Beate, and Penny O'Donnell, *The blurring line between freelance journalists and self-employed media workers*, Journalism, vol. 24, no. 1, 2023, pp. 139-156.

Lami, Isabella M., and Elena Todella*, A multi-methodological combination of the strategic choice approach and the Analytic Network Process: From facts to values and vice versa,* European Journal of Operational Research vol. 307, no. 2, 2023, pp. 802-812.

Lashmar, Paul, *Putting lives in danger? Tinker, tailor, journalist, spy: the use of journalistic cover*, Journalism vol. 21, no. 10, 2020, pp. 1539-1555.

Machek, David, *The Life Worth Living in Ancient Greek and Roman Philosophy*, Cambridge University Press, 2023.

Mchedlidze, Nana, *Modern Challenges to Freedom of Expression: Need for Recalibration of the ECtHR Approach to Facts and Value Judgments,* Georgian Journal of Comparative Law, vol. 28, 2023.

Nalyvaiko, Larysa, and Olha Chepik-Trehubenko, *Application of the principle of the rule of law international and national courts*, Щорічник, 2023, p. 143.

Neumann, Peter R., *Europe's jihadist dilemma,* Survival, Routledge, 2023, pp. 71-84.

Paolo Lobba, *Holocaust Denial before the European Court of Human Rights: Evolution of an Exceptional Regime*, European Journal of International Law, vol. 26, no. 1, 2015, pp. 237-253.

Radwański, Ryszard, Justyna Stochaj, and Krzysztof Rejman, *Premises for Protecting the Polish Population in the Context of the National Security Strategy,* Journal of Security and Sustainability Issues, vol. 13, no. 1, 2023.

Raz, Joseph, *The Morality of Freedom*, Oxford, Oxford University Press, 1986.

Schroeder, Mark, *Value Theory*, The Stanford Encyclopedia of Philosophy (Fall 2021 Edition), Edward N. Zalta (ed.), URL = https://plato.stanford.edu/archives/fall2021/entries/value-theory/.

Sikuta, Jan, *Threats of Terrorism and the European Court of Human Rights*, European Journal of Migration and Law, vol. 10, no. 1, 2008, pp. 1-10.

Straczuk, Justyna, *'Hybrid war', military humanitarianism, and epistemic friction. Framing illegalised migration on the Polish-Belarusian border*, Journal of Ethnic and Migration Studies, 2023, pp. 1-19.

Stajnko, Jan, *Tackling hate speech in Western Balkans*, Central European political science review, vol. 24, no. 94, 2023, pp. 65-77.

Strahovnik, Vojko, *Robert Audi, The Good in the Right: A Theory of Intuition and Intrinsic Value*, Croatian Journal of Philosophy, vol. 15, 2005, pp. 583-589.

Tsomidis, Theo, *Freedom of expression in turbulent times–comparative approaches to dangerous speech: the ECtHR and the US Supreme Court*, The International Journal of Human Rights, vol. 26, no. 3, 2022, pp. 379-399.

Walasek, Lukasz, and Gordon DA Brown, *Incomparability and incommensurability in choice: no common currency of value?* Perspectives on Psychological Science, 2023, 17456916231192828.

Williams, Michael John, *Who's Afraid of the Bomb?: The Euromissiles Crisis and Nuclear Weapons in Europe, Past and Present,* International Studies Review vol. 26, no. 1, 2024, viae008.

Wiśniewski, Adam, *The European Court of Human Rights and Internet-Related Cases*, Białostockie Studia Prawnicze, vol. 3, no. 26, 2021, pp. 109-133.

Source of financing

The work was created within the framework of the research program Research of Cultural Formations (P6-0278 (A), 2019–2024), funded by Slovenian Research and Innovation Agency ARIS.

„dot.pl" - czasopismo Rejestru domeny .pl

The Iranian Cyberattacks in Albania: Actors, Tactics, Targets

"The attack on Albania is a reminder that while the most aggressive Iranian cyber activity is generally focused in the Middle East region, it is by no means limited to it. Iran will carry out disruptive and destructive cyberattacks as well as complex information operations globally"[227].

John Hultquist, Mandiant Vice President

Tal Pavel
Communication Science, Alma Mater Europaea – European Center, Maribor, Slovenia
ORCID: https://orcid.org/0000-0002-4046-0867
E-mail: Tal@cybureau.org

Received: 01.12.2024
Accepted: 03.12.2024
Published: 03.12.2024

Cite this article as:
T. Pavel, "The Iranian Cyberattacks in Albania: Actors, Tactics, Targets"

DOT.PL, no. 1/ 2024, 10.60097/DOTPL/196772

Corresponding author:
Tal Pavel
Communication Science, Alma Mater Europaea – European Center, Maribor, Slovenia
E-mail: Tal@cybureau.org

Abstract

The paper aims to analyze the Iranian cyber-attacks in Albania, a small yet strategically vital nation in the Balkans. It examines the cyber incidents attributed to Iranian actors, focusing on the objective behind these operations, the tactics employed, and the sectors targeted. Given the escalating geopolitical tensions between Iran and Albania, particularly due to Albania's support for an Iranian dissident group, Tehran has increasingly used cyber warfare as a means of influence and retaliation. By assessing the effectiveness of these cyber campaigns and their implications for Albania's

[227] L. Semini, *Albania Cuts Diplomatic Ties with Iran over July Cyberattack*, AP News, 7 September 2022. https://apnews.com/article/nato-technology-iran-middle-east-6be153b291f42bd549d5ecce5941c32a accessed 10 October 2024.

national security, the study provides insights into how state-sponsored cyber activities function as tools of foreign policy.

The goal of this study is to illuminate the complex dynamics of state-sponsored cyber aggression and its implications for national and regional security. Specifically, it examines how cyber-attacks serve as instruments for achieving political objectives, as demonstrated by Iran's use of cyber warfare against Albania. Additionally, the study explores the potential for future Iranian cyber activities targeting other Balkan states as part of its broader strategy and that of its allies.

To achieve its objective and goal, this study employs a methodical approach to source selection, ensuring a comprehensive and balanced analysis. Sources were carefully chosen for their relevance, reliability, and diversity, drawing from academic articles, cyber research company analyses, journalistic reports, and official publications. This methodology provides a solid and credible foundation for understanding the nature and implications of Iranian cyber-attacks on Albania.

Keywords: Albania, Cyber Security, Strategy, Balkans, Iran

Introduction

Over the years, Iran launched multiple cyber-attacks against various states around the globe[228]. Some of them caused much damage and gained international resonance, including a massive power outage in Turkey (2015)[229], "the biggest hack in history" against Saudi Aramco, one of the world's largest oil companies (2015)[230], the British Parliament

[228] American Coalition Against Nuclear Iran, *History of Iranian Cyber Attacks and Incidents*, 2024. https://www.unitedagainstnucleariran.com/sites/default/files/UPDATE%20-%20The%20Iranian%20Cyber%20Threat.pdf; accessed 1 September 2024; Chuck Freilich, *Major Iranian Cyeberattacks Around the World*, "The Iranian Cyber Threat", Institute for National Security Studies, 2024 https://www.inss.org.il/wp-content/uploads/2024/02/Part-3.pdf; accessed 2 September 2024.

[229] M. Halpern, *Iran Flexes Its Power by Transporting Turkey to the Stone Age, "*Observer*"*, 22 April 2015. https://observer.com/2015/04/iran-flexes-its-power-by-transporting-turkey-to-the-stone-ages/ accessed 1 September 2024.

[230] J. Pagliery, *The inside Story of the Biggest Hack in History*, "CNN Business", 5 August 2015. https://money.cnn.com/2015/08/05/technology/aramco-hack/index.html accessed 1 September 2024.

(2017)[231], and many more various cyber-attacks against diverse sectors in the U.S.[232] and Israel[233] across the years, in addition to vast disinformation campaigns worldwide[234].

Vast literature analysed the widespread Iranian-affiliated cyber-attacks. Some refer to cybersecurity in Albania: Organised and cybercrime threat assessments (2015)[235] and regulations[236], cybersecurity awareness[237], cyber resilience[238], cyber regulations[239], and teaching cyber security in higher academic institutions in Albania[240].

Aleksander Biberaj and others (2022) examined cyber-attacks against Albania and its digital assets, including against the national database (e-Albania)[241]. Annita Larissa Sciacovelli (2023) covers the Iranian cyber-attacks in Albania relating to technical and legal attribution and the role of private security tech companies in the attribution[242].

---

[231] The Telegraph, *Iran Blamed for Cyberattack on Parliament That Hit Dozens of MPs, Including Theresa May*, 14 October 2017. https://web.archive.org/web/20171206135812/https://www.msn.com/en-gb/news/uknews/iran-blamed-for-cyberattack-on-parliament-that-hit-dozens-of-mps-including-theresa-may/ar-AAtpPag?li=AAmiR2Z&ocid=spartanntp accessed 2 September 2024.

[232] Cybersecurity & Infrastructure Security Agency (CISA), *Potential for Iranian Cyber Response to U.S. Military Strike in Baghdad*, 4 October 2020. https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-006a accessed 2 September 2024.

[233] Ch. Freilich, *The Iranian Cyber Threat to Israel*, "The Iranian Cyber Threat", Institute for National Security Studies, 2024. https://www.inss.org.il/wp-content/uploads/2024/02/Part-4.pdf accessed 2 September 2024.

[234] Paul de Souza, *Iran's Assault on Our Democracy and a Closer Look at Their Disinformation Tactics*, LinekdIn, 28 August 2024. https://www.linkedin.com/pulse/copy-irans-assault-our-democracy-closer-look-tactics-de-souza-96baf/?trackingId=Vb8cw2ZO%2FflLSLUMKGsTcg%3D%3D accessed 2 September 2024.

[235] F. Zhilla, B. Lamallari, *Organised Crime Threat Assesment in Albania*, 2015. https://globalinitiative.net/wp-content/uploads/2018/02/Threat_Assessment_of_Albanian_Organised.pdf accessed 1 September 2024.

[236] A. Shkembi, I. Shtupi, A. Qafa, *The Regulation of Cyber Crime in Albania in the Framework of Harmonization of Internal Legislation with the European Legislation*, "Academic Journal of Interdisciplinary Studies", 2016, vol. 5, No.1, https://pdfs.semanticscholar.org/cd34/8906b7b5170601c731763dde70a27ed159f4.pdf accessed 1 September 2024.

[237] E. Moci, *Cybersecurity Awareness in Albania*, European Journal of Social Science. Education and Research, 2021, vol. 8, No. 3. https://revistia.com/files/articles/ejser_v8_i3_21/Moci.pdf accessed 1 September 2024.

[238] R. Bahiti, J. Josifi, *Towards a More Resilient Cyberspace: The Case of Albania*, Information & Security: An International Journal, 2015, vol. 32. https://connections-qj.org/system/files/3310_albania.pdf accessed 1 September 2024.

[239] E. Tiri, E. Aliaj, *Cyber-Security Regulation in Albania*, Perspectives of Law and Public Administration, 2023, vol.12, No. 2. https://www.ceeol.com/search/article-detail?id=1221788 accessed 1 September 2024.

[240] E. Ceko, *Cyber Security Issues in Albanian Higher Education Institutions Curricula,* 2021, CRJ, vol. 1(1). https://albanica.al/CRJ/article/view/2728 accessed 1 September 2024.

[241] A. Biberaj et al., *Cyber Attack Against E-Albania and Its Social, Economic and Strategic Effects,* The Journal of Corporate Governance, Insurance, and Risk Management (JCGIRM), 2022, vol. 9 (2). https://www.ceeol.com/search/article-detail?id=1161455 accessed 1 September 2024.

[242] A. L. Sciacovelli, *Taking Cyberattacks Seriously: The (Likely) Albanian Cyber Aggression and the Iranian Responsibility*, WORKING PAPER OSSERVATORIO SULLE ATTIVITÀ DELLE ORGANIZZAZIONI INTERNAZIONALI E SOVRANAZIONALI, UNIVERSALI E REGIONALI, SUI TEMI DI INTERESSE DELLA POLITICA ESTERA ITALIANA, 2023, https://ricerca.uniba.it/handle/11586/438480 accessed 1 September 2024.

Jakub Vostoupal's research (2024) analyses the attribution of the Stuxnet, WannaCry, and the 2022 cyber-attacks against Albania[243]. Therefore, the current literature does not comprehensively analyse various aspects of the Iranian cyber-attacks in Albania.

To address the literature gap, the research will analyse the following research questions: (1) What strategies and tactics have Iranian cyber actors employed in their attacks in Albania? (2) What are the threats to the Balkans from Iranian cyber-attacks?

Methodology

This study focused on choosing as diverse and reliable sources as possible. The selection of sources was based on several principles:

Relevance – the selected sources are relevant to the research topic and questions.

Reliability – choosing the most reliable and trustworthy sources.

Diversity – The research includes diverse primary and secondary sources, including academic articles, analyses by cyber research companies, journalistic articles, and official publications.

Findings

Attacks – Albania was under several waves of cyber-attacks allegedly performed by Iranian state-sponsored actors: (1) **initial access** to the network of the Albanian government as early as May 2021[244], followed by email exfiltration from the compromised network between October 2021 and January 2022. (2) email **harvesting** between November 2021 and May 2022. (3) Destructive campaign in mid-July 2022[245] (4) and

[243] J. Vostoupal, *Stuxnet vs WannaCry and Albania: Cyber-Attribution on Trial,* Computer Law & Security Review, 2024, vol. 54. https://www.sciencedirect.com/science/article/abs/pii/S026736492400075X accessed 1 September 2024.
[244] Microsoft Threat Intelligence, *Microsoft Investigates Iranian Attacks against the Albanian Government*, Microsoft Security Blog, 8 September 2022. https://www.microsoft.com/en-us/security/blog/2022/09/08/microsoft-investigates-iranian-attacks-against-the-albanian-government/ accessed 7 September 2024.
[245] E. Elezi, N. Gholami, *Albania Blames Iran for Cyberattacks,* Deutsche Welle, 16 September 2022. https://www.dw.com/en/albania-once-again-the-target-of-cyberattacks-after-cutting-diplomatic-ties-with-iran-and-expelling-diplomats/a-63146285 accessed 13 October 2024.

September 2022[246] against the Albanian government computer system that **destroyed data** and disrupted government services. (5) Cyber-attack on the Albanian Parliament in December 2023, **disrupting** the Parliament services[247]. (6) **Destroyed and leaked data** of allegedly over 100 terabytes of Albania's geographic information system and population data at the end of January 2024[248].

Methods – The National Institute of Standards and Technology (NIST) defines Computer Network Operations (CNO) as "the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace"[249]. CNO includes three known types of attacks:

(1) Computer network Exploitation (CNE) – "Actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves"[250].

(2) Computer Network Attack (CNA) – "Actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves"[251].

[246] Cybersecurity & Infrastructure Security Agency (CISA), *Iranian State Actors Conduct Cyber Operations Against the Government of Albania,* 23 September 2022. https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-264a accessed 19 October 2024.
[247] D. Antoniuk, *Albanian Parliament, Telecom Company Hit by Cyberattacks,* Recorded Future News, 27 December 2023. https://therecord.media/albanian-parliament-telecom-company-hit-by-cyberattacks accessed 19 October 2024; Llazar Semini, *A Cyberattack Targets Albanian Parliament's Data System, Halting Its Work,* 27 December 2023. https://apnews.com/article/albania-cyberattack-parliament-iran-cc1a03b58bd753bbe935ad74f1abc0f7 accessed 19 October 2024.
[248] The National Authority for Cyber Security (AKSK), *Deklaratë Zyrtare, 1* February 2024 https://aksk.gov.al/deklarate-zyrtare-5/ accessed 19 October 2024. D. Antoniuk, *Iran-Linked Hackers Claim Attack on Albania's Institute of Statistics,* Recorded Future News, 2 February 2024. https://therecord.media/iran-linked-hackers-claim-attack-on-albania-census-org accessed 19 October 2024.
[249] National Institute of Standards and Technology (NIST), *Computer Network Operations* (CNO), https://csrc.nist.gov/glossary/term/computer_network_operations accessed 12 October 2024.
[250] National Institute of Standards and Technology (NIST), *Computer Network Attack* (CNA), https://csrc.nist.gov/glossary/term/computer_network_attack accessed 12 October 2024.
[251] ibidem

(3) Computer Network Influence (CNI) – "Actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves"[252].

The Iranian cyber-attacks in Albania consisted of the three known categories:

The Iranian cyber-attacks in Albania included **CNE** activities of ransomware attacks[253], deletion of national data[254], and **CNA** activities of leaks and publication of personal data of thousands of Albanians[255], including Albanian government data and details of emails from the Prime Minister and Ministry of Foreign Affairs[256].

Mandiant researchers defined the versatile activities of this Iranian cyber actor as "a formidable threat actor that likely supports various objectives ranging from espionage to network attack operation"[257] that maintains an arsenal of passive backdoors and sophisticated techniques to avoid standard monitoring methods, obtain footholds into victim networks, and set up long-term access without attracting attention.

CNI – A channel of Iranian soft power is propaganda to monitor and expand its public diplomacy, among others, by publishing Albanian-language news items on an Iranian state-sponsored media outlet. An analysis by the Balkan Investigative Reporting Network in Albania sampled 715 articles published by Iran's Pars Today News Agency in Albanian from 27 June to 26 September 2022 to reveal several thematic biases in the news narratives to "shape public perceptions in accordance with its geopolitical interests and

---

[252] ibidem

[253] L. Jenkins at al., *ROADSWEEP Ransomware Targets the Albanian Government,* Google Cloud Blog, 4 August 2022. https://cloud.google.com/blog/topics/threat-intelligence/likely-iranian-threat-actor-conducts-politically-motivated-disruptive-activity-against/ accessed 2 September 2024.

[254] ClearSky Security, *Wiper Attack on Albania by Iranian APT,* 2024. https://www.clearskysec.com/wp-content/uploads/2024/01/No-Justice-Wiper.pdf accessed 7 September 2024.

[255] Albanian Daily News, *Homeland Justice Published the Detailed Data of Albanians,* 23 June 2024. https://albaniandailynews.com/news/homeland-justice-published-the-detailed-data-of-albanians accessed 13 October 2024.

[256] GOV.UK, *UK Condemns Iran for Reckless Cyber Attack against Albania,* 7 September 2022. https://www.gov.uk/government/news/uk-condemns-iran-for-reckless-cyber-attack-against-albania accessed 14 October 2024.

[257] S. Shulman et al., *UNC1860 and the Temple of Oats: Iran's Hidden Hand in Middle Eastern Networks,* Google Cloud Blog, 20 September 2024. https://cloud.google.com/blog/topics/threat-intelligence/unc1860-iran-middle-eastern-networks accessed 12 October 2024.

ideology"[258]. In addition, the Iranian Sahar TV channel operates in several languages, including Albanian, and addresses the Balkans in a dedicated section of the website[259]. Moreover, researchers claim that besides propaganda, Iran is involved in the dissemination of fake news against the Iranian opposition group Mojahedin-e Khalq Organization (MEK) and its attempt to influence the debate about Iran in the Western Balkan, a region that was "among the most vulnerable to the spread of fake news" and therefore "an easier target for (Iranian) disinformation campaigns"[260].

Suspected actors – Various statements and reports indicate that more than one cyber actor has conducted cyber-attacks in Albania. One of them, "Homeland Justice"[261], took credit for the cyber-attacks in Albania conducted from July 2022.

In his message from 7 September 2022, Albania's Prime Minister mentioned "the engagement of four groups that enacted the aggression – one of them being a notorious international cyber-terrorist group, which has been a perpetrator or co-perpetrator of earlier cyber-attacks targeting Israel, Saudi Arabia, UAE, Jordan, Kuwait and Cyprus"[262]. Mandiant researchers stressed "with moderate confidence that one or multiple threat actors who have operated in support of Iranian goals are involved", mentioning "a cross-team collaboration or other scenarios that we lack insight into at this time"[263]. Microsoft researchers assessed "with high confidence that multiple Iranian actors participated in this attack—with different actors responsible for distinct phases"[264].

The Iranian cyber actors are known by different names given by various cybersecurity vendors and researchers and have been active since at least 2014, targeting regional

[258] B. Bino, B. Likmeta, *Iran's Propaganda in Albanian Language,* Balkan Investigative Reporting Network in Albania Tirana, 2023. https://birn.eu.com/wp-content/uploads/2023/07/Media-Analysis_Irans-Propaganda-in-Albanian-Language.pdf accessed 19 October 2024.
[259] Sahar, *SAHAR Balkans,* https://balkan.sahartv.ir/ accessed 27 October 2024.
[260] A. Rrustemi et al., *Geopolitical Influences of External Powers in the Western Balkans,* HCSS Security, Report, 2021. https://hcss.nl/wp-content/uploads/2021/01/Geopolitical-Influences-of-External-Powers-in-the-Western-Balkans_0.pdf accessed 27 October 2024.
[261] AJ. Vicens, *Albania Cuts Diplomatic Ties with Iran after July Cyberattack,* CyberScoop, 7 September 2022. https://cyberscoop.com/albanian-cyberattack-diplomatic-iran/ accessed 13 October 2024.
[262] Albanian Government, *Videomessage of Prime Minister Edi Rama,* 7 September 2022. https://www.kryeministria.al/en/newsroom/videomesazh-i-kryeministrit-edi-rama/ accessed 13 October 2024.
[263] Op. cit. (n. 27)
[264] Op. cit. (n. 19).

allies and enemies alike (Saudi Arabia, Israel, the United Arab Emirates, Iraq, Jordan, Lebanon, Kuwait, Qatar, Albania, the U.S. and Turkey) or affiliated organisations in the telecommunications, government, defence, oil, chemical manufacturing, and financial services, for espionage and intelligence gathering, and destruction, on behalf of the Iranian government based on infrastructure details that contain references to Iran and is linked to Iran's Ministry of Intelligence and Security (MOIS)[265].

However, Gentian Progni, an Albanian researcher, believes that "Iran was not acting alone", suggesting a collaboration between Russia and Iran in the cyber-attacks in Albania. He mentions that (1) the cyber actors operated from Russian territory. (2) The leaked information was disseminated from a Russian website, justicehomeland.ru (3), and through Telegram channels, which were also used to spread pro-Russian propaganda. (4) Montenegro, Bulgaria, Kosovo and North Macedonia were hit by cyber-attacks by Russian-speaking cyber groups, and during the same period, Albania was attacked. (5) The claim that "the range of the attacks were too big"[266]. (6) The ongoing cyber partnership between Russia and Iran, including a cyber-defence cooperation diplomacy agreement from June 2015 on the "exchange of intelligence, interaction against threats and joint defense"[267], and the January 2021 cyber agreement between the two countries[268], which stipulates broad cybersecurity cooperation, including "coordination of actions, exchange of technologies, training of specialists"[269]. Miad Nakhvali, an Iranian researcher, emphasises the importance of this agreement, which

---

[265] R. Lemos, *As Geopolitical Tensions Mount, Iran's Cyber Operations Grow,* DarkReading, 18 September 2024. https://www.darkreading.com/cyberattacks-data-breaches/geopolitical-tensions-mount-iran-cyber-operations-grow accessed 11 October 2024.

[266] A. Oghanna, *How Albania Became a Target for Cyberattacks,* FP Dispatch, 25 March 2023. https://foreignpolicy.com/2023/03/25/albania-target-cyberattacks-russia-iran/#selection-1123.0-1123.44 accessed 19 October 2024.

[267] Tasnim News Agency, *Iran, Russia Agree on Cyber-Defense Cooperation: Official,* 13 June 2015. https://www.tasnimnews.com/en/news/2015/06/13/768309/iran-russia-agree-on-cyber-defense-cooperation-official accessed 20 October 2024.

[268] TASS, *Russia, Iran Sign Agreement on Cyber Security Cooperation,* 26 January 2021. https://tass.com/politics/1248963 accessed 20 October 2024.

[269] Izvestia, *MFA Reveals Details of Iran-Russia Agreement on Information Security,* 26 January 2021. https://iz.ru/1116475/2021-01-26/mid-raskryl-detali-soglasheniia-irana-i-rossii-ob-informatcionnoi-bezopasnosti accessed 20 October 2024.

"signals a deeper level of cooperation between the two countries at all administrative levels in the areas of cybersecurity, technological transfer and joint training"[270].

Motivation – Iran's interest in the Western Balkans, the "Eastern world in the West", reflects the region's growing strategic significance to Iran and a potential "base for future proxy conflicts between Iran and the West"[271]. Iran wants to expand its influence, spread the Islamic Revolution, and develop economic and bilateral relations based on religious, ideological, and geopolitical factors. In this regard, Iran is engaged in various activities, low to medium, through overt political and economic interactions, mainly covert hybrid warfare techniques, including disinformation and cyber-attack campaigns.

The early stage of Iran's involvement in the region was during the Bosnia's war for independence from Yugoslavia in the 1990s, by sending arms and volunteer troops to support the Bosnian Muslim leader Alija Izetbegovic, who had established ties with Iran after the Islamic Revolution.

Future proxy conflicts may used for political purposes. They may translate into a long-term security impact by undermining current regimes and provoking anti-Western and subversive religious and ideologic sentiments. Indeed, Iran has demonstrated increased cultural and religious activities in the Western Balkans due to the similarities in culture, religion, and discourse. Persian was popular in some areas of the Balkans in ancient times, and over 1,700 Persian words are still used in the Bosnian language[272].

Despite the low level of Iranian political interactions and influence in the Western Balkans, due to what Iran perceives as a pro-U.S. Albania stand, mainly against Iranian interests, Iran "now has a direct interest in this region", and Albania is considered a "frontline country in Iran's fight against terrorism"[273]. In 2013, Albania agreed to the U.S. request to host some 3,000 members of the exiled MEK group, which Iran considers a

[270] Op. cit. (n. 40).
[271] Op. cit. (n. 32).
[272] IBNA News Agency, *Over 1,700 Persian Words Used in Bosnian Language: Expert,* 24 December 2016. https://web.archive.org/web/20201108112639/https://www.ibna.ir/en/naghli/243605/over-1-700-persian-words-used-in-bosnian-language-expert accessed 26 October 2024.
[273] Nejat Society, *Mojahedin Khalq Terrorist Training Camp in Albania Impacts Whole Balkan Region,* 10 January 2018. https://www.nejatngo.org/en/posts/7862 accessed 28 October 2024.

terrorist organisation compared to ISIS[274], allowing them to set up a camp ("Ashraf 3") outside Tirana[275].

The Iranian retaliation was allegedly in both dimensions: physical and cyber-attacks and propaganda.

In October 2019, the Albanian Police announced it foiled several planned attacks during 2018 against MEK members in Albania by "an active cell of the foreign operations unit of the Iranian QUDS forces"[276].

Among their activities, the MEK conducted, beginning in 2016, an annual "Free Iran" conference. The 2002 conference was planned for 23-24 July 2022[277] but was postponed by the organisers "upon recommendations by the Albanian government, for security reasons, and due to terrorist threats and conspiracies"[278]. Indeed, the U.S. Embassy in Albania issued a security alert to U.S. citizens in Albania, stating that "The U.S. government is aware of a potential threat targeting the Free Iran World Summit to be held near Durres, Albania on July 23-24, 2022"[279].

The Iranian motivation and role in the 15 July 2022 cyber-attacks on Albania may be found in an open letter from 23 July to the President of Albania, Ilir Meta, issued by the two of a Pro-Iran and anti-MEK organisation called the Association for the Support of Iranians

---

[274] Nejat Society, *Mojahedin Khalq Supports Daesh, Plans Terrorist Training Camp in Albania,* 25 June 2015. https://www.nejatngo.org/en/posts/6128 accessed 28 October 2024.
[275] P. Dockins, *US Praises Albania for MEK Resettlement,* Voice of America (VOA), 14 February 2016. https://www.voanews.com/a/us-albania/3190311.html accessed 13 October 2024.
[276] op. cit. (n. 18).
[277] Iran Freedom, *We Can and We Must Free Iran, Take Action: Free Iran World Summit 2022,* 22 July 2022. https://iranfreedom.org/en/news/2022/07/we-can-and-we-must-free-iran-take-action-free-iran-world-summit-2022/35290/ accessed 13 October 2024. National Council of Resistance of Iran (NCRI), Free Iran World Summit 2022. https://www.ncr-iran.org/en/news/free-iran-world-summit/free-iran-2022-world-summit/ accessed 13 October 2024.
[278] Iran Freedom, *Iran NCRI: Postponement of the Free Iran World Summit at Ashraf 3,* 23 July 2022. https://iranfreedom.org/en/free-iran-2022/2022/07/iran-ncri-postponement-of-the-free-iran-world-summit-at-ashraf-3/35303/ accessed 13 October 2024. National Council of Resistance of Iran (NCRI), Postponement of the Free Iran World Summit at Ashraf 3, 22 July 2022. https://www.ncr-iran.org/en/ncri-statements/postponement-of-the-free-iran-world-summit-at-ashraf-3/ accessed 13 October 2024.
[279] U.S. Embassy in Albania, *Security Alert – Threat Targeting the Free Iran World Summit (July 21, 2022)*, 23 January 2023. https://al.usembassy.gov/security-alert-threat-targeting-the-free-iran-world-summit-july-21-2022/ accessed 13 October 2024.

Living in Albania (ASILA), wondering whether "Albania has entered into a cyber and military conflict with the Islamic Republic of Iran"[280].

After the assassination of Iranian General Qassem Soleimani by a U.S. drone on 3 January 2020, Albania welcomed the assassination. It immediately expelled two Iranian diplomats for "engaging in activities deemed unacceptable for diplomats". Iran's supreme leader, Ali Khamenei, referred to that affair by saying, "There is a small but evil European country in which Americans and traitors against Iran got together to conspire against the Islamic Republic"[281].

Albania, a NATO member since 2009, stands on the side of the U.S. as a close ally. In early July 2022, the U.S. Special Operations Command said on social media that it "made the decision to locate a forward-based Special Operations Forces (SOF) headquarters, on a rotational basis, in Albania!" which Albania's prime minister defined as "fantastic news" adding that "It is an expression of a very high credibility and a very close cooperation[282].

Microsoft research indicates that the selected targets and the messaging of the cyber attacker indicate Iran used the cyber-attacks in Albania as retaliation for previous[283] cyber operations of an Iranian hacktivist group, "Uprising till Overthrow", that hacked several Iranian government websites in July 2022 and leaked sensitive official documents[284]. The September 2022 cyber-attacks came several days after Albania cut diplomatic relations with Iran over July 2022 cyber-attacks[285].

Therefore, Iran's motivation to launch the cyber-attacks against Albania lay on strategic, political and ideological motives.

---

[280] O. Jazexhi, G. Thanasi, *Letter to Albania Gov. Concerning the Cyber Attacks against Albania and Iran*, Niejat Society, Albania Media and blogs, 23 July 2022 https://archive.vn/N8yZN#selection-597.0-606.0 accessed 28 October 2024.

[281] A. Ruci, L. Arapi, *Iran Lashes out against Albania after Soleimani Killing,* Deutsche Welle, 21 January 2020. https://www.dw.com/en/iran-lashes-out-against-albania-after-soleimani-killing/a-52102170 accessed 19 October 2024.

[282] Deutsche Welle, *US Opens Special Forces Base in Albania,* 1 July 2022. https://www.dw.com/en/us-constructs-new-special-forces-regional-base-in-albania/a-60361419 accessed 13 October 2024.

[283] Op. cit. (n. 20)

[284] Iran International, *Hacktivist Group Targets Iran's Government Organization,* 3 July 2022. https://www.iranintl.com/en/202207032504 accessed 20 October 2024.

[285] AJ. Vicens, *Albania Says Iranian Hackers Hit the Country with Another Cyberattack,* Cyberscoop,12 September 2022. https://cyberscoop.com/iranian-cyberattack-albania-homeland-justice/ accessed 13 October 2024.

Targets – The Iranian cyber-attacks targeted various Albanian organisations and governmental institutions aiming to paralyse essential infrastructure in Albania, including telecom (One.al, EagleMobile.al), transportation (Albanian airlines), law enforcement (Albanian police force's Total Information Management System (TIMS)[286], a system that the U.S. government helped Albania to deploy in 2007) and governmental sectors (the Albanian government portal, Albanian Institute of Statistics (INSTAT), National Electronic Documentation, Cyber Security Institution (AKCESK))[287]. Implications – The Iran cyber-attacks were catastrophic for Albanian public services, hampering the government's ability to govern and affecting every citizen. (1) The vast majority of government services had been digitised and brought online to circumvent the slow and corrupt bureaucratic public process. (2) The hackers managed to gather, delete and leak private and even classified information of the general public and civil servants, including customer financial records, the data of everyone who entered and exited Albania for more than 17 years, and the identities of hundreds of undercover Albanian intelligence officers[288].

Indeed, Prime Minister Edi Rama emphasised, "Based on the investigation, the scale of the attack was such that the aim behind it was to completely destroy our infrastructure back to the full paper age, and at the same time, wipe out all our data"[289].

Discussion

This study aims to portray Iran's cyber-attacks on Albania during 2021-2024, including the different waves of the cyber-attacks, the methods of operations, suspected actors, motivations, and targets. In addition, the study analyses the implications of those cyber-attacks and their mitigation, including at the local, bilateral, and international levels.

---

[286] K. Kote, *TIMS Functional Quite Soon, Interior Ministry Vows,* Albanian Daily News, 10 September 2022. https://albaniandailynews.com/news/tims-functional-quite-soon-interior-ministry-vows accessed 13 October 2024.

[287] T. Ozturk, *Albania Blames Iranian-Backed Group for Cyberattack on Its Statistical Institute,* Anadolu Ajansı, 16 February 2024. https://www.aa.com.tr/en/europe/albania-blames-iranian-backed-group-for-cyberattack-on-its-statistical-institute/3137301 accessed 13 October 2024.

[288] Op. cit. (n. 40)

[289] T. Starks, *How Albania Reckoned with Alleged Iranian Hackers,* The Washington Post, 26 September 2022. https://www.washingtonpost.com/politics/2022/09/26/how-albania-reckoned-with-alleged-iranian-hackers/ accessed 20 October 2024.

The findings enable answering the different research questions:

(1) During the waves of cyber-attacks attributed by various sources to Iran, three types of cyber-attack tactics were conducted:
    a. Computer network Exploitation (CNE) – **Intelligence Gathering** – the first stage of the cyber-attacks aimed to gain initial access to the Albanian government's network for 14 months, as well as email harvesting and exfiltration.
    b. Computer Network Attack (CNA) – **Destruction** – was the next stage of cyber-attacks, which aimed to destroy data and disrupt Albania's government services.
    c. Computer Network Influence (CNI) – **Influence** – The cyber-attacker, "Homeland Justice", not only took credit for the attacks but also published pro-Iran and anti-MEK messages that echoed over the Internet, alongside ongoing propaganda in various Iranian media outlets and in the Albanian language as well.

Those attacks were catastrophic for Albanian public services, hampering the government's ability to govern and affecting every citizen by gathering, deleting and leaking private and even classified information of the general public and civil servants.

Alongside the various research attributes of the cyber-attacks with Iran, the different stages, duration, complexity, and needed resources of the attacks suggest the involvement of a nation-state, cyber-actor, known as Advanced Persistent Threat (APT), with strategic motivations that may serve a state rather than cyber criminals or hacktivists[290].

(2) Iran's aim in the Western Balkans is to spread the Islamic Revolution and develop economic and bilateral relations based on religious, ideological, and geopolitical factors. Despite a modest economic and political Iranian influence in

[290] Kaspersky, *What Is an Advanced Persistent Threat (APT)?*, Kaspersky Lab, 2024 https://www.kaspersky.com/resource-center/definitions/advanced-persistent-threats accessed 30 October 2024.

the Western Balkans, the cultural and religious one is more prevalent, based on similarities in culture, religion, and discourse.

Iran considers Albania as an anti-Iran state due to what Iran perceives as a pro-U.S. stand and the host Albania provided to the MEK organisation, which Iran considers a terrorist organisation. Those cyber-attacks demonstrated that Iran is an active player in the Western Balkans and may conduct various cyber operations for strategic purposes against distant rivals. Therefore, such cyber-attacks may be addressed in other Western Balkan countries, even throughout the Balkans, as another tool for Iran to influence and retaliate against its rivals.

The literature covers various aspects of Iran's cyber capabilities, attacks, motivations, targets, and actors but does not address Albania's cyber-attacks. The research of Aleksander Biberaj and others (2022) indicated the need for "improving essentially the cyber infrastructure to avoid in the future such attacks with high social, economic and strategical cost". Their research showed the failures and, therefore, measures of improvements to avoid such cyber-attacks, "In the institution there was not a team for Cyber Security Monitoring the system, so called SOC (Security Operation Center), who controls in the real time all the logins. It was missing as well as the so-called "Identifying Behavior" as well. There was not e separation of active directory, in physic machines and virtual machines, they were altogether. As the administrator had Full Right Privilege, the hacker doesn't need to create a Privilege Escalation Vertical, so he easily took all the right of Admin"[291].

Conclusions

The research stresses the threat posed by external cyber actors to Albania and the potential proliferation in the Balkans:

Strategic Cyber Operations – The Iranian cyberattacks on Albania demonstrate the increasing use of cyber operations for state-sponsored retaliation, geopolitics, and ideological influence. These attacks were not limited to disruption but also included

[291] Op.cit. (n. 15)

espionage and the dissemination of propaganda, showcasing the multifaceted objectives of Iranian cyber actors.

Vulnerability of Small States – The attacks and their consequences highlight smaller states' vulnerabilities to advanced persistent threats (APTs) and underscore the importance of robust cybersecurity frameworks to mitigate such risks.

Proliferation – The attacks reveal Iran's broader strategic interests in the Western Balkans, including influencing regional politics and countering perceived adversaries. This suggests that similar states in the region could become future targets. Ongoing wars and regional conflicts may expand cyber threats to more regions and by various actors. Indeed, experts believe that the Iranian-Israeli confrontation may enter a full-scale war with spillover that could potentially reach the Balkans due to some Iranian influence in Bosnia and Herzegovina and Serbia and the status of Bulgaria as a top destination for tourists and "digital nomads" from Israel. This threat already materialises in the 2012 explosion in Burgas linked by the Bulgarian authorities to the Lebanese Hezbollah[292]. The conclusion of Mandiant researchers should be a red alert for cyber threats posed by Iran to the Balkan, the E.U. and NATO member states: "This activity is a geographic expansion of Iranian disruptive cyber operations, conducted against a NATO member state. It may indicate an increased tolerance of risk when employing disruptive tools against countries perceived to be working against Iranian interests"[293]. Therefore, cyber actors may pose threats outside the geographical region against those not necessarily considered typical targets.

Future Research

The following research will analyse the implications of the Iranian cyber-attacks on Albania and the various local, bilateral, and international mitigation measures taken, including recommendations to minimise the implications of future cyber-attacks in Albania and the Balkans.

[292] G. Cafiero, *Will the Iran-Israel Confrontation Reach the Balkans?*, Amwaj.media, 8 July 2024. https://amwaj.media/article/will-the-iran-israel-confrontation-reach-the-balkans accessed 9 October 2024.
[293] Op. cit. (n. 27)

References

Albanian Daily News, ‘Homeland Justice Published the Detailed Data of Albanians’ (23 June 2024) <https://albaniandailynews.com/news/homeland-justice-published-the-detailed-data-of-albanians> accessed 13 October 2024

Albanian Government, ‘Videomessage of Prime Minister Edi Rama’ (7 September 2022) <https://www.kryeministria.al/en/newsroom/videomesazh-i-kryeministrit-edi-rama/> accessed 13 October 2024

American Coalition Against Nuclear Iran, ‘History of Iranian Cyber Attacks and Incidents’ (2024) <https://www.unitedagainstnucleariran.com/sites/default/files/UPDATE%20-%20The%20Iranian%20Cyber%20Threat.pdf> accessed 1 September 2024

Antoniuk D, ‘Albanian Parliament, Telecom Company Hit by Cyberattacks’ (*Recorded Future News*, 27 December 2023) <https://therecord.media/albanian-parliament-telecom-company-hit-by-cyberattacks> accessed 19 October 2024

‘Iran-Linked Hackers Claim Attack on Albania’s Institute of Statistics’ (*Recorded Future News*, 2 February 2024) <https://therecord.media/iran-linked-hackers-claim-attack-on-albania-census-org> accessed 19 October 2024

Bahiti R and Josifi J, ‘Towards a More Resilient Cyberspace: The Case of Albania’ (2015) 32 Information & Security: An International Journal 1 <https://connections-qj.org/system/files/3310_albania.pdf> accessed 1 September 2024

Biberaj A and others, ‘Cyber Attack Against E-Albania and Its Social, Economic and Strategic Effects’ (2022) 9 The Journal of Corporate Governance, Insurance, and Risk Management (JCGIRM) 341 <https://www.ceeol.com/search/article-detail?id=1161455> accessed 1 September 2024

Bino B and Likmeta B, ‘Iran’s Propaganda in Albanian Language’ (2023) <https://birn.eu.com/wp-content/uploads/2023/07/Media-Analysis_Irans-Propaganda-in-Albanian-Language.pdf> accessed 19 October 2024

Cafiero G, ‘Will the Iran-Israel Confrontation Reach the Balkans?’ (*Amwaj*, 8 July 2024) <https://amwaj.media/article/will-the-iran-israel-confrontation-reach-the-balkans> accessed 9 October 2024

Ceko E, ‘Cyber Security Issues in Albanian Higher Education Institutions Curricula’ [2021] CRJ 56 <https://albanica.al/CRJ/article/view/2728> accessed 1 September 2024

ClearSky Security, ‘Wiper Attack on Albania by Iranian APT’ (2024) <https://www.clearskysec.com/wp-content/uploads/2024/01/No-Justice-Wiper.pdf> accessed 7 September 2024

Cybersecurity & Infrastructure Security Agency (CISA), ‘Potential for Iranian Cyber Response to U.S. Military Strike in Baghdad’ (4 October 2020) <https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-006a> accessed 2 September 2024

‘Iranian State Actors Conduct Cyber Operations Against the Government of Albania’ (23 September 2022) <https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-264a> accessed 19 October 2024

de Souza P, ‘Iran’s Assault on Our Democracy and a Closer Look at Their Disinformation Tactics’ (*LinekdIn*, 28 August 2024) <https://www.linkedin.com/pulse/copy-irans-assault-our-democracy-closer-look-tactics-de-souza-96baf/?trackingId=Vb8cw2ZO%2FflLSLUMKGsTcg%3D%3D> accessed 2 September 2024

Deutsche Welle, ‘US Opens Special Forces Base in Albania’ (1 July 2022) <https://www.dw.com/en/us-constructs-new-special-forces-regional-base-in-albania/a-60361419> accessed 13 October 2024

Dockins P, ‘US Praises Albania for MEK Resettlement’ (*Voice of America (VOA)*, 14 February 2016) <https://www.voanews.com/a/us-albania/3190311.html> accessed 13 October 2024

Elezi E and Gholami N, 'Albania Blames Iran for Cyberattacks' (*Deutsche Welle*, 16 September 2022) <https://www.dw.com/en/albania-once-again-the-target-of-cyberattacks-after-cutting-diplomatic-ties-with-iran-and-expelling-diplomats/a-63146285> accessed 13 October 2024

Freilich C, 'Major Iranian Cyeberattacks Around the World', *The Iranian Cyber Threat* (Institute for National Security Studies (INSS) 2024) <https://www.inss.org.il/wp-content/uploads/2024/02/Part-3.pdf> accessed 2 September 2024

'The Iranian Cyber Threat to Israel', *The Iranian Cyber Threat* (Institute for National Security Studies (INSS) 2024) <https://www.inss.org.il/wp-content/uploads/2024/02/Part-4.pdf> accessed 2 September 2024

GOV.UK, 'UK Condemns Iran for Reckless Cyber Attack against Albania' (7 September 2022) <https://www.gov.uk/government/news/uk-condemns-iran-for-reckless-cyber-attack-against-albania> accessed 14 October 2024

Halpern M, 'Iran Flexes Its Power by Transporting Turkey to the Stone Age' (*Observer*, 22 April 2015) <https://observer.com/2015/04/iran-flexes-its-power-by-transporting-turkey-to-the-stone-ages/> accessed 1 September 2024

IBNA News Agency, 'Over 1,700 Persian Words Used in Bosnian Language: Expert' (24 December 2016) <https://web.archive.org/web/20201108112639/https://www.ibna.ir/en/naghli/243605/over-1-700-persian-words-used-in-bosnian-language-expert> accessed 26 October 2024

Iran Freedom, 'We Can and We Must Free Iran, Take Action: Free Iran World Summit 2022' (22 July 2022) <https://iranfreedom.org/en/news/2022/07/we-can-and-we-must-free-iran-take-action-free-iran-world-summit-2022/35290/> accessed 13 October 2024

'Iran NCRI: Postponement of the Free Iran World Summit at Ashraf 3' (23 July 2022) <https://iranfreedom.org/en/free-iran-2022/2022/07/iran-ncri-postponement-of-the-free-iran-world-summit-at-ashraf-3/35303/> accessed 13 October 2024

Iran International, 'Hacktivist Group Targets Iran's Government Organization' (3 July 2022) <https://www.iranintl.com/en/202207032504> accessed 20 October 2024

Izvestia, 'MFA Reveals Details of Iran-Russia Agreement on Information Security' (26 January 2021) <https://iz.ru/1116475/2021-01-26/mid-raskryl-detali-soglasheniia-irana-i-rossii-ob-informatcionnoi-bezopasnosti> accessed 20 October 2024

Jazexhi O and Thanasi G, 'Letter to Albania Gov. Concerning the Cyber Attacks against Albania and Iran' (23 July 2022) <https://archive.vn/N8yZN#selection-597.0-606.0> accessed 28 October 2024

Jenkins L and others, 'ROADSWEEP Ransomware Targets the Albanian Government' (*Google Cloud Blog*, 4 August 2022) <https://cloud.google.com/blog/topics/threat-intelligence/likely-iranian-threat-actor-conducts-politically-motivated-disruptive-activity-against/> accessed 2 September 2024

Kaspersky, 'What Is an Advanced Persistent Threat (APT)?' <https://www.kaspersky.com/resource-center/definitions/advanced-persistent-threats> accessed 30 October 2024

Kote K, 'TIMS Functional Quite Soon, Interior Ministry Vows' (*Albanian Daily News*, 10 September 2022) <https://albaniandailynews.com/news/tims-functional-quite-soon-interior-ministry-vows> accessed 13 October 2024

Lemos R, 'As Geopolitical Tensions Mount, Iran's Cyber Operations Grow' (*DarkReading*, 18 September 2024) <https://www.darkreading.com/cyberattacks-data-breaches/geopolitical-tensions-mount-iran-cyber-operations-grow> accessed 11 October 2024

Microsoft Threat Intelligence, 'Microsoft Investigates Iranian Attacks against the Albanian Government' (*Microsoft Security Blog*, 8 September 2022) <https://www.microsoft.com/en-us/security/blog/2022/09/08/microsoft-investigates-iranian-attacks-against-the-albanian-government/> accessed 7 September 2024

Moci E, ‘Cybersecurity Awareness in Albania ’ (2021) 8 European Journal of Social Science Education and Research 1 <https://revistia.com/files/articles/ejser_v8_i3_21/Moci.pdf> accessed 1 September 2024

National Council of Resistance of Iran (NCRI), ‘Free Iran World Summit 2022’ (2022) <https://www.ncr-iran.org/en/news/free-iran-world-summit/free-iran-2022-world-summit/> accessed 13 October 2024

‘Postponement of the Free Iran World Summit at Ashraf 3’ (22 July 2022) <https://www.ncr-iran.org/en/ncri-statements/postponement-of-the-free-iran-world-summit-at-ashraf-3/> accessed 13 October 2024

National Institute of Standards and Technology (NIST), ‘Computer Network Attack (CNA)’ <https://csrc.nist.gov/glossary/term/computer_network_attack> accessed 12 October 2024

‘Computer Network Operations (CNO)’ <https://csrc.nist.gov/glossary/term/computer_network_operations> accessed 12 October 2024

Nejat Society, ‘Mojahedin Khalq Supports Daesh, Plans Terrorist Training Camp in Albania’ (25 June 2015) <https://www.nejatngo.org/en/posts/6128> accessed 28 October 2024

‘Mojahedin Khalq Terrorist Training Camp in Albania Impacts Whole Balkan Region’ (10 January 2018) <https://www.nejatngo.org/en/posts/7862> accessed 28 October 2024

Oghanna A, ‘How Albania Became a Target for Cyberattacks’ (25 March 2023) <https://foreignpolicy.com/2023/03/25/albania-target-cyberattacks-russia-iran/#selection-1123.0-1123.44> accessed 19 October 2024

Ozturk T, ‘Albania Blames Iranian-Backed Group for Cyberattack on Its Statistical Institute’ (*Anadolu Ajansı*, 16 February 2024) <https://www.aa.com.tr/en/europe/albania-blames-iranian-backed-group-for-cyberattack-on-its-statistical-institute/3137301> accessed 13 October 2024

Pagliery J, ‘The inside Story of the Biggest Hack in History’ (*CNN Business*, 5 August 2015) <https://money.cnn.com/2015/08/05/technology/aramco-hack/index.html> accessed 1 September 2024

Rrustemi A and others, ‘Geopolitical Influences of External Powers in the Western Balkans ’ (2021) <https://hcss.nl/wp-content/uploads/2021/01/Geopolitical-Influences-of-External-Powers-in-the-Western-Balkans_0.pdf> accessed 27 October 2024

Ruci A and Arapi L, ‘Iran Lashes out against Albania after Soleimani Killing’ (21 January 2020) <https://www.dw.com/en/iran-lashes-out-against-albania-after-soleimani-killing/a-52102170> accessed 19 October 2024

Sahar, ‘SAHAR Balkans’ <https://balkan.sahartv.ir/> accessed 27 October 2024

Sciacovelli AL, ‘Taking Cyberattacks Seriously: The (Likely) Albanian Cyber Aggression and the Iranian Responsibility.’ (2023) 1 WORKING PAPER OSSERVATORIO SULLE ATTIVITÀ DELLE ORGANIZZAZIONI INTERNAZIONALI E SOVRANAZIONALI, UNIVERSALI E REGIONALI, SUI TEMI DI INTERESSE DELLA POLITICA ESTERA ITALIANA <https://ricerca.uniba.it/handle/11586/438480> accessed 1 September 2024

Semini L, ‘Albania Cuts Diplomatic Ties with Iran over July Cyberattack’ (*AP News*, 7 September 2022) <https://apnews.com/article/nato-technology-iran-middle-east-6be153b291f42bd549d5ecce5941c32a> accessed 10 October 2024

‘A Cyberattack Targets Albanian Parliament’s Data System, Halting Its Work’ (27 December 2023) <https://apnews.com/article/albania-cyberattack-parliament-iran-cc1a03b58bd753bbe935ad74f1abc0f7> accessed 19 October 2024

Shkembi A, Shtupi I and Qafa A, ‘The Regulation of Cyber Crime in Albania in the Framework of Harmonization of Internal Legislation with the European Legislation’ (2016) 5 Academic Journal of Interdisciplinary Studies 1 <https://pdfs.semanticscholar.org/cd34/8906b7b5170601c731763dde70a27ed159f4.pdf> accessed 1 September 2024

Shulman S and others, ‘UNC1860 and the Temple of Oats: Iran’s Hidden Hand in Middle Eastern Networks’ (20 September 2024) <https://cloud.google.com/blog/topics/threat-intelligence/unc1860-iran-middle-eastern-networks> accessed 12 October 2024

Starks T, ‘How Albania Reckoned with Alleged Iranian Hackers’ (*The Washington Post*, 26 September 2022) <https://www.washingtonpost.com/politics/2022/09/26/how-albania-reckoned-with-alleged-iranian-hackers/> accessed 20 October 2024

Tasnim News Agency, ‘Iran, Russia Agree on Cyber-Defense Cooperation: Official’ (13 June 2015) <https://www.tasnimnews.com/en/news/2015/06/13/768309/iran-russia-agree-on-cyber-defense-cooperation-official> accessed 20 October 2024

TASS, ‘Russia, Iran Sign Agreement on Cyber Security Cooperation - Russian Politics & Diplomacy’ (26 January 2021) <https://tass.com/politics/1248963> accessed 20 October 2024

The National Authority for Cyber Security (AKSK), ‘Deklaratë Zyrtare’ (1 February 2024) <https://aksk.gov.al/deklarate-zyrtare-5/> accessed 19 October 2024

The Telegraph, ‘Iran Blamed for Cyberattack on Parliament That Hit Dozens of MPs, Including Theresa May’ (14 October 2017) <https://web.archive.org/web/20171206135812/https://www.msn.com/en-gb/news/uknews/iran-blamed-for-cyberattack-on-parliament-that-hit-dozens-of-mps-including-theresa-may/ar-AAtpPag?li=AAmiR2Z&ocid=spartanntp> accessed 2 September 2024

Tiri E and Aliaj E, ‘Cyber-Security Regulation in Albania’ (2023) 12 Perspectives of Law and Public Administration 275 <https://www.ceeol.com/search/article-detail?id=1221788> accessed 1 September 2024

U.S. Embassy in Albania, ‘Security Alert – Threat Targeting the Free Iran World Summit (July 21, 2022)’ (23 January 2023) <https://al.usembassy.gov/security-alert-threat-targeting-the-free-iran-world-summit-july-21-2022/> accessed 13 October 2024

Vicens A, ‘Albania Cuts Diplomatic Ties with Iran after July Cyberattack’ (*CyberScoop*, 7 September 2022) <https://cyberscoop.com/albanian-cyberattack-diplomatic-iran/> accessed 13 October 2024

‘Albania Says Iranian Hackers Hit the Country with Another Cyberattack’ (12 September 2022) <https://cyberscoop.com/iranian-cyberattack-albania-homeland-justice/> accessed 13 October 2024

Vostoupal J, ‘Stuxnet vs WannaCry and Albania: Cyber-Attribution on Trial’ (2024) 54 Computer Law & Security Review 106008 <https://www.sciencedirect.com/science/article/abs/pii/S026736492400075X> accessed 1 September 2024

Zhilla F and Lamallari B, ‘Organised Crime Threat Assesment in Albania’ (2015) <https://globalinitiative.net/wp-content/uploads/2018/02/Threat_Assessment_of_Albanian_Organised.pdf> accessed 1 September 2024

„dot.pl" - czasopismo Rejestru domeny .pl

Affordability of quality: case of Slovenian online shopping

Ekaterina Kuznetsova
Institut ZIS Pomurje, Lendavska uliva 28, Rakičan, 9000 Murska Sobota, Slovenia
ORCID: 0009-0005-7918-8038
E-mail: ekaterina.kuznetsova2205@gmail.com

Received: 28.08.2024
Accepted: 09.10.2024
Published: 10.10.2024

Cite this article as:
E. Kuznetsova, "*Affordability of quality: case of Slovenian online shopping*"

DOT.PL, no. 1/ 2024,
10.60097/DOTPL/194388

Corresponding author:
Ekaterina Kuznetsova
Institut ZIS Pomurje, Lendavska uliva 28, Rakičan, 9000 Murska Sobota, Slovenia

E-mail:
ekaterina.kuznetsova2205@gmail.com

Abstract

This article examines the question buying preferences of Slovenians. General observation that we will try to test is that Slovenians are systematically not buying high end products (if price is considered indicator of quality). Especially since on-line shopping increased availability of products, it is harder to deny that in internet era there is no access to diverse products. Based on available data, the article tries to establish connection between average financial structure of Slovenian households and expenditures that are characteristics for most households. We can assume that brand, cost and amount of money spent of advertising are not necessarily an indicator of quality, however there is certain correlational (if no other, psychological one). We try to combine information on economic status of Slovenian households/individuals with the information regarding best-selling products in selected categories within the

online shop. The basic finding can be seen described as correlation between economic capabilities of people to the price level of goods purchased in the selected online store. Since products have also popular reviews, we can determine the perceived level of quality. Based on general positive reviews of the most purchased products, which are systematically on the lower side of average of price of all products in each chosen category, we can assume that a cheaper product does not necessarily have to be of poor quality. This would indicate that Slovenians are not only buying with their financial capabilities but also rationally in the perspective of equilibrium optimisation between price and quality also when it comes to online shopping.

Keywords: economic capacity; on-line stores; quality of goods; on-line shopping; quality of products ,

Introduction

According to some popular views in Slovenia, buying expensive goods is not necessary, because medium or low-price products can serve equally good. On contrary, in many cases it is understood that the more expensive, the better. Accordingly, it would be logical to draw the conclusion that people buy only expensive goods if they want to get high-quality product. Sellers often confuse the buyers by giving either an incomplete or a huge volume of information, which is very difficult for the average person to process. It is sometimes unclear whether the high price of a product is due to quality, brand, price of the components and production or due to the seller's desire for the economic gain[294]. In this work we will try to elaborate, if and why Slovenians do not buy expensive goods, supported by case of common technical goods sold on one of main online stores in Slovenia. Buying habits will be set in the context of economic situation of Slovenian households. In other words, we try to establish the connection between people's standard of living in relation to their (online) purchasing habits. The European Union in general and Slovenia in particular promote the belief that inhabitants have a good quality

[294]N.M., Rozanova, *Modern consumer caught in the web of global economy,* "Bulletin of the Institute of Economics of the Russian Academy of Sciences", 2024(3), pp. 26-46.

of life, stability, freedom, and enormous number of opportunities, that additionally increased by utilisation of information and communication technologies. There are lots of advertisement pictures and videos picturing main question, set up in this article is, if idealistic picture of life exists systematically when it comes to creating living standard, In other words whether it is possible for them to choose expensive goods without compromising their lives.

Additionally, the definition of high quality is quite broad. The criteria by which a particular product can be considered high quality refers to qualities of the product and we learn about to us such type of feeling. For such life people need a lot of different type of products. The them in the process of using the product. Before making the purchase, buyer is dealing with economic decision, based on his own beliefs and (partial) information. Despite people tend to buy the most preferred brand, they will still change their decision if somebody close to them recommends different product, product only partially satisfies their needs or if price is significantly out of their range[295]. By understanding the basis of the buyers' logic and economical capacity, it is possible to predict what and what quality/price range they will purchase in the near future.

As indicated before, we want to contribute to following two questions. First question is: what is actually economic capacity of people in Slovenia; how much they can spend on goods. This answer is in numbers somewhere between amount of money which people get and how much money they need for daily life. Second question is what are considered to be high-quality products? Is quality determined by set of characteristics of certain product or it is all only about the branding. Based on these two questions and analysing the case of online buying pattern we can assess the high end purchase ability in case of Slovenia.

Measuring quality

Quality is in many cases product of different regulations, like certification or permissions, which is especially relevant in online environment, where there is limited ability to examine products before purchase. However, we are more interested in consumers'

[295]M.-K., Minthiu, *The buying decision process and types of buying behaviour. Economic sciences, "*Sibiu Alma Mater University Journals. Series A. Economic Sciences*",* 2009, vol.2(4), pp. 27-33.

personal perception of the quality. We assume that, if product is in the market, it means that it has necessary permissions and certifications. This way we are coming to the point when in the market we have lots of goods, which fulfil minimal quality standards in accordance to number of permissions and certificates which regulatory organs are considering necessary for specific type of product. However, when it comes to online shopping, there is increased danger of business malpractices and non-adequate products. Trying to understand common characteristics of quality between all products, there is possibility to analyse what combinations of factors must occur in order for the product to be purchased. Moreover, for every product there is own list of specific indicators of quality. For example, a computer and a kettle perform completely different functions, therefore their requirements and quality criteria will be completely different. In addition, our expectations from using a computer and a kettle will be very different, and different amounts of time will be spent choosing one or the other product. There are some signs by which you can determine the possible good quality of a products:

- The product belongs to a brand which people trust
- Advertisement of products
- Comments and reviews for specific product
- Price of goods

Brands and quality

A brand is a name, term, design, symbol or any other feature that distinguishes one seller's good or service from those of other sellers[296]. According to the opinion of some scientist branding already existed around 2700 BCE[297]. Farmers used it to identify their animals. Slaves were also identified this way. These reasons were not connected to quality; they were used to find run-away slave or animal. But farmers, potters and traders started to use seals on their products as a mark of pride. Forms of branding were different

[296]American Marketing Association Dictionary Archived 2012-06-11 at the Wayback Machine. Retrieved 2011-06-29. The Marketing Accountability Standards Board (MASB) endorses this definition as part of its ongoing Common Language in Marketing Project Archived 2019-04-05 at the Wayback Machine

[297]E. Karev, *Mark them with my Mark': Human Branding in Egypt*, "The Journal of Egyptian Archaeology", 2022, vol.108(1-2), pp. 191-203

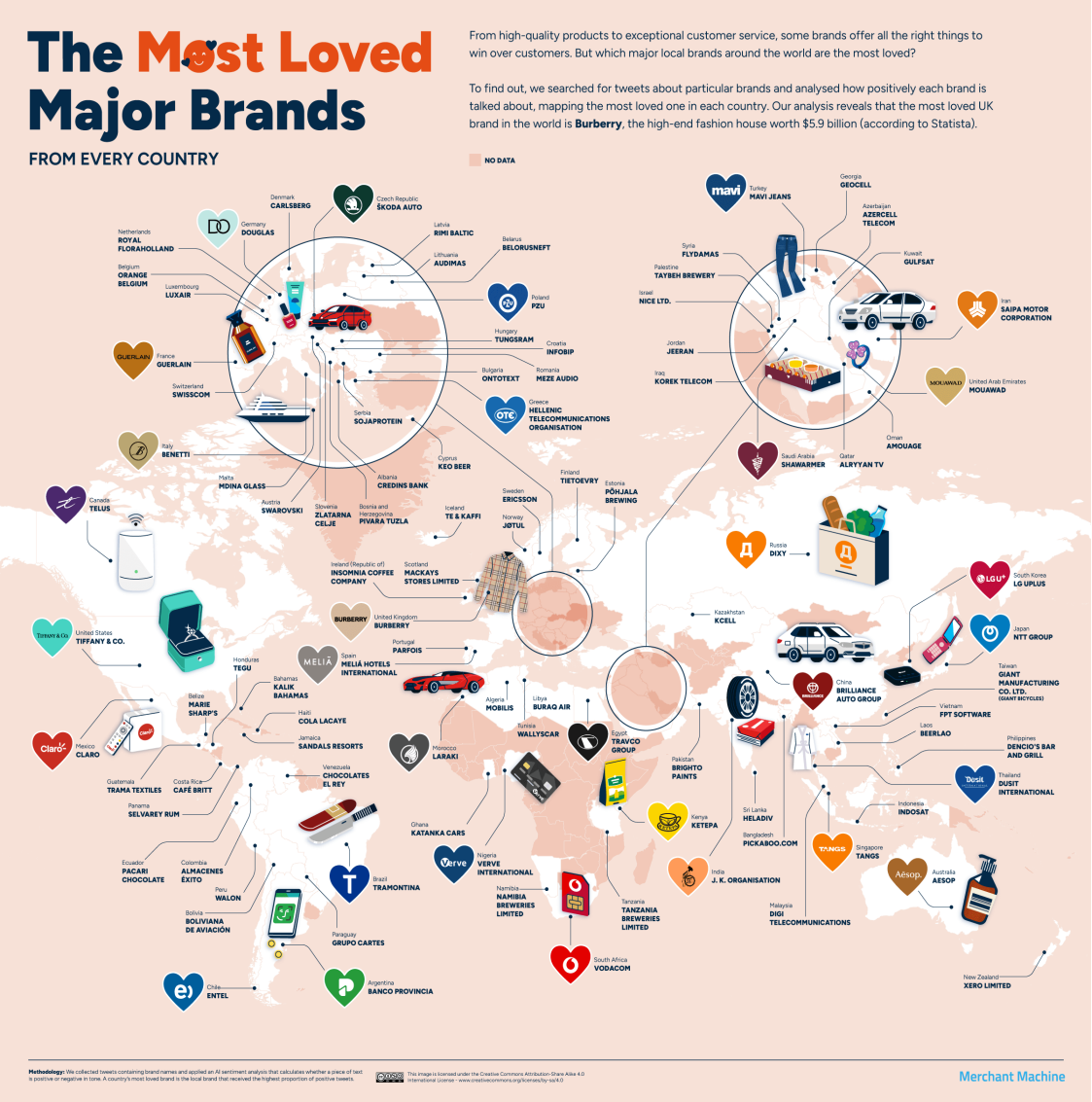
and some scientists are saying that it is not connected with nowadays brand[298]. However, people were recognizing products and its characteristics; at this moment, brand became stamp of quality. Living in information era, we have much better access to products' characteristics, which are hidden behind the name of the brand to make more informed decisions. Historically, brand was working like guarantee of quality, but with time and intensive globalisation this changed. Products from "unknown" producers are not necessarily of worse quality then goods from well-known brand. The process of creating a brand is complex and requires lots of resources. However, a correctly formed brand can bring significant profits to a company[299][300]. The price of branded goods is very often higher due to the brand reputation for certain quality/characteristics, but it is also based on the cost of investment and brand promotion[301].

Connection of price and quality of goods

According to Rizkova[302], the problem of pricing of goods is that buyer does not always understand how much it is reasonable to increase the price for a brand. A buyer does not have data on the long-term costs paid by the company for developing the brand. The buyer only decides whether he/she is ready or willing to pay this difference for the brand (in relation to the price of non-branded substitute). Since the brand develops the buyer's trust in it, brand can be used dishonestly in the future. Such example can be disproportionately increased prices for regular customers of amazon.com[303][304]. Merchantmachine.co.uk published information about the most loved and the most hated brands in the world. We can observe that in each country's most loved brand is usually local brand (measured by the highest proportion of positive tweets).

---

[298]K. Moore, S. Reid, *The birth of brand: 4000 years of branding,* "Business History"*,* 2008, vol. *50(4),* pp. 419-432.
[299]D.A., Aaker, *Managing brand equity: Capitalizing on the value of a brand name*, The Free Press, New York London Toronto Sydney, 2009.
[300]D.A., Aaker, E. Joachimsthaler, *Brand Leadership*, The free press, New York, 2012.
[301] I. Prosvirina, *Price of brand: view of financial specialist*. "Journal Business Key", 2008, vol. 5.
[302]M. Rizkova, *Connection of price and quality for goods*. "News of Tomsk Politechnic University. Georesources Engineering"*,* 2013, vol. 323(6), pp. 74-80.
[303]O. Amir, O. Label, D. Ariely, *Making Consumption Decisions by following Personal Rules*. In E. S. Ratneshwar, M. D. Glen (eds.): *Inside Consumption*. London: Routledge. London, 2005, pp. 86-101.
[304]E. S. Ratneshwar, M. D. Glen *Inside consumption: Consumer Motives, Goals and Desires*; In E. S. Ratneshwar, M. D. Glen (eds.): *Inside Consumption*. London: Routledge. London, 2005.

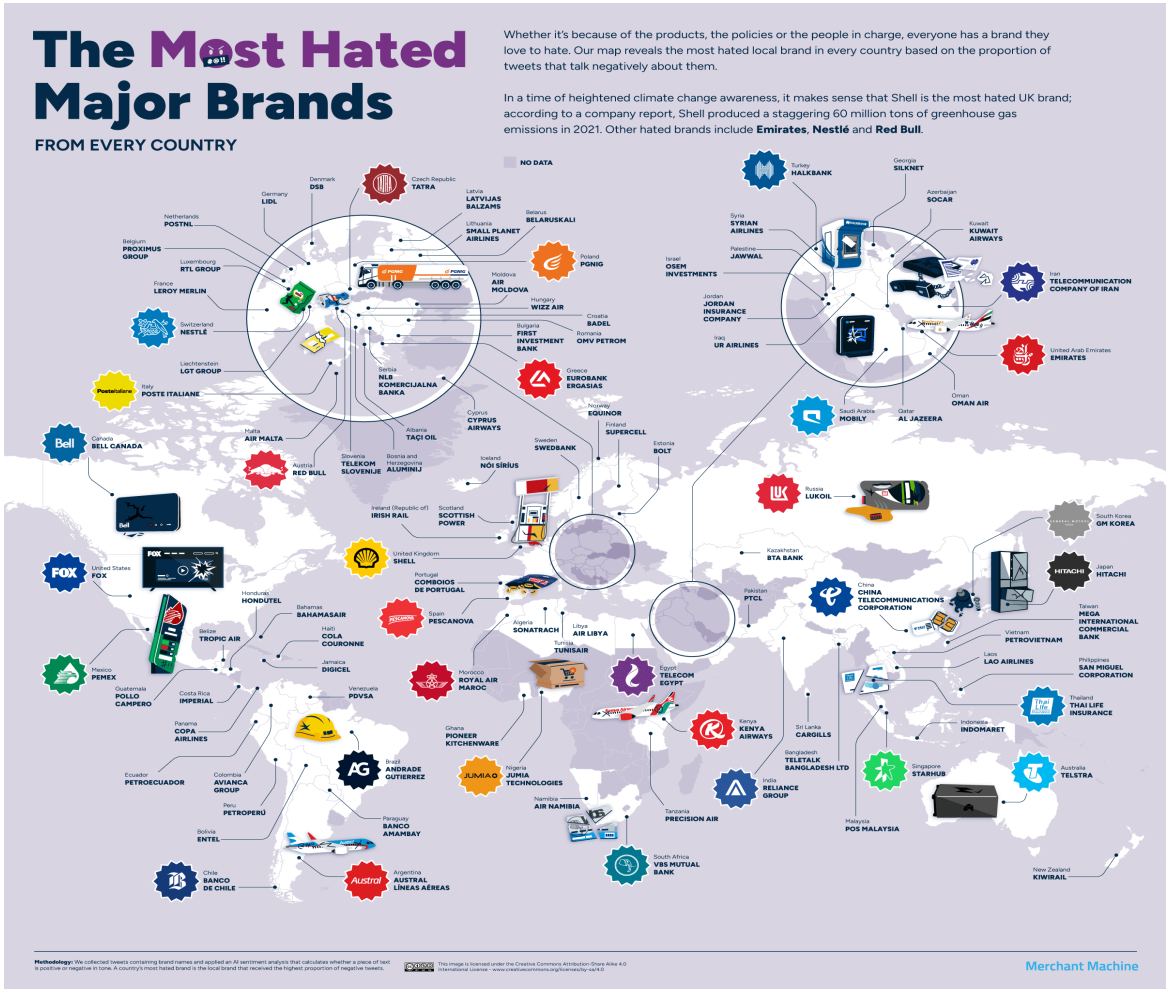


Picture1: *The Most Loved Major brands*, *Source: Wright, 2023.*

The most loved brand in Slovenia according to this research is Zlatarna Celje. We see lots of cosmetics, cars, phones, clothes, jewellery on this map. Living in information society with social media and using "tweets" or other online "shout-outs" as base of results, it is important to talk about the role of influencers in these results. Influencer marketing has emerged as an effective approach for brands to connect with customers by using the trust and psychological bond that influencers have established with their followers on social media[305]. Influencers forge deeper psychological bonds with their followers by

[305]C.C. Chillders, L.L. Lemon, M.G. Hoy, *Agency perspective on influencer marketing campaigns.* "Journal of Current Issues & Research in Advertising", 2019, vol. 40 (3), pp. 258-274.

sharing highly personal content that revolves around their lifestyle and interests[306]. Social media users see influencers like similar to them and according to users' perspective they are attractive and interesting[307]. With such connection between followers and influencers, one can easily understand connection between influencers' content and increased desirability of the shown content among followers. Influencers are a factor in choosing a favourite brand, alongside with one's mentality, weather conditions, economy of the country, etc. For followers, influencer is some kind of guarantee of quality.



Picture 2: *The Most Hated Major Brands. Source: Wright, 2023*

[306]T. Wondwesen, B.P. Wood, *Followers' engagement with instagram influencers: The role of influencers' content and engagement strategy.* "Journal of retailing and consumer services", 2021(58), p.102303.
[307]A. Sokolova, K. Hajer, *Instagram and YouTube bloggers promote it, why should I buy? How credibility and parasocial interaction influence purchase intentions. "Journal of retailing and consumer services",* 2020(53), p.101742.

Picture 2 represents the information about the most hated major brands. There is lots of research about brand hate, types and circumstances[308]. Hated brands are brands which people cannot avoid in their lives and have no better substitutes. These are usually airlines, insurance, banks, oil companies, telecommunications companies, etc. People will still use them because of life situations, but they will be much more eager to express their discontent, since named companies have low possibility of replacement with better option. In this case any kind of talk about quality looks useless. As long as people will need to fly, they will fly and even if quality of fling is poor, people will still use it because of their needs and lack of substitution options.

On the conceptual level Nelson[309] determined two types of quality of goods. Search quality of goods can be understood by consumer before he buys it. Characteristics of such goods are similar and prices too. Buyer can choose goods from any company and will get approximately the same result. For example, electricity, gas, salt, flavour are exchangeable goods (despite not always exactly the same, the differences between products of different providers are rather small). But with second type of quality – experience quality- logic is more complex, because most of the time prices of the same goods from different producers are not comparable (typically designer's products), number of producers and companies who are selling these goods is limited and characteristic is hard to observe at once[310].

Reputation as a sign of quality: Evidence from an online marketplace

"For buyers it is very hard choice when at the same time buyer wants to buy the cheapest item and save as much money as possible and simultaneously is afraid to lose quality of product with lowering the price."[311]. One of the ways to understand quality is to see signs

[308]C. Zhang, M. Laroche, *Brand hate: a multidimensional construct*, "Journal of Product & Brand Management", 2020, vol. 30(3), pp. 392-414.
[309]P. Nelson, *Advertising as information,* "Journal of political economy", 1974, vol. 82(4), pp. 729-754.
[310]L. Li, S. Tadelis, X, Zhou, *Buying reputation as a signal of quality: Evidence from an online marketplace.* "The RAND journal of economics", 2020, vol. 51(4), pp. 965-988.
[311]M. Rizkova, *Connection of price and quality for goods.* "News of Tomsk Politechnic University. Georesources Engineering", 2013, vol. 323(6), pp. 74-80.

of quality[312]. Only sellers of high-quality goods will spend money on ads to promote their experience goods because only they can be confident that they will receive positive returns from their expenditures. Advertising has to be costly enough to deter sellers of low-quality items from being willing to spend the money and sell one once to each customer because they will not attract repeat purchase. According to this opinion, ads are a sign of high-quality goods. If products are not good enough, company will not spend their economic resources towards ads, because spent resources will not return profits immediately. "Buyer is depending on ads, fashion trends, and other people who are important to him."[313]. Leibenstein defines few psychological effects of consumerism; bandwagon effect, snob effect and Veblens effect[314]. Bandwagon effect means that person is buying certain product in order not to differ from the majority. The Snob effect, on the contrary, is characterized by the acquisition of goods, with which the buyer can be distinguished from other people. The Veblen effect is characteristic of demonstrative consumption and is mainly associated with the influence of price, and it does not manifest itself in a standard way. From the point of view of classical supply-demand theorem - the increased demand for a certain product increases its price and, on the contrary, decrease in demand should decrease the price of a product. Search for price equilibrium in buying emerges also based on influence of others and their opinion[315]. Buyers can be guided not only by economic benefits when purchasing a product, but can also be influenced by some other factor. For example, if under the influence of advertising, several people will buy certain product, then some others will inevitably join in order to be comparable to them (bandwagon effect), while some others will buy a completely opposite product only because they do not want to be like everyone else (snobbism effect). Thus, purchasing decisions depend on the mental state of a person, as well as on psychological state at the moment. At some point advertising can psychologically influence a purchase, but at another not. A large amount of advertising

[312] Li, Tadelis, Zhou, op.cit.

[313]V. Shpakovskaya, *Psihological fenomen of ADS*. In V.S., Rubanov at al. (eds): *"Collection of competitive scientific works of students and undergraduates in two parts"*. BRGTU, Brest, 2018, pp. 235-238.

[314]H. Leibenstein, *Bandwagon, Snob and Veblen Effects in the Theory of Consumer Demand.* "Quarterly Journal of Economics", 1950, vol. 64(2), pp. 183-207.

[315]Shpakovskaya, op.cit.,

may cause rejection in some cases[316]. Based on all the above and the fact that advertising is rather necessary to encourage a person to buy, we can say that advertising does not always show the level of quality the product, but it is more of motivational and manipulation element in the process of buying. One research argues that medium level of advertisement expenditure is actually the indicator of good quality of goods[317].

Next sign of quality is feedback. In the information society, people can information themselves about anything instantly. Individual can today, before buying washing machine or vacuum cleaner can check feedback of previous buyers on-line. For example, web-page Trip advisor is extremely good demonstration of people providing feedback about hotel, coffee-place or museum etc and its influence for future customers. With developing of internet many stores organise their online platforms, where buyers can leave their opinions about purchased goods. Therefore, online comments, shared by consumers who have purchased and used the products, are particularly important for potential future consumers to make their purchase decisions[318]. According to the survey and research of CNNIC, 92% of potential consumers often search the on-line comments of relevant products before deciding on whether or not to make their own purchases. At the same time, 77.5% of them consider online comments as the main factor underlying their purchase decisions. By reading online comments, potential consumers acquire a more comprehensive understanding of the product specifications and performance, which helps reduce shopping uncertainties. A scale development study coming to the point that with the increasing functionality of online comment systems, consumers progressively make their purchase decisions by relying on online comments shared by previous consumers. Considering mismatches between what is offered in the marketplace and what is desired by consumers, a two-stage theoretical model can be established to explore the optional pricing and decision behaviour of an online retailer in different situations by identifying and characterizing the initial and additional

[316]V. A. Sindhya, V. A., *Study on the influence and impact of advertising to consumer purchase motive among student teachers.* "IOSR Journal of Research and Method in Education", 2013, vol. 2(4), pp. 1-5.
[317]R. Orzach, P. B. Overgaard, Y. Tauman, *Modest advertising signals strength.* "RAND Journal of Economics", 2002, vol. 33(2), pp. 340-358.
[318]T. Chen, P. Samaranayake, X.Y. Cen, M. Qi, *The Impact of Online Reviews on Consumers' Purchasing Decisions: Evidence From an Eye-Tracking Study.* "Frontiers in Psychology", vol.13, 2022, p. 865702.

comments[319]. Some web-sites, like Alibaba or Taobao started to use "Rebate for feedback" mechanism. If a seller offers a discount for purchasing their product if you leave a comment, it helps the buyer make a purchasing decision[320]. This shows that seller is so confident in the product that he/she is willing to pay for feedback about it. The seller does not want to receive a negative comment about the product, which means the possibility of a paid comment about the purchased product can also serve as a sign of the quality of the product.

Form of feedback is also information how many products were returned to the stores because of poor quality. This information is usually hidden from buyers. Nobody knows how many kettles or washing machines of a particular type break down during the warranty period. Sometimes producer can call back goods because of systemic issues during producing process. For example, in less than a month after the release of the Samsung Galaxy Note 7, at least 35 incidents with explosion of a device became known. As a result, Samsung had to publicly admit the critical battery defect and recall the entire batch of GALAXY[321]. When a product is recalled, a company can often spend a lot of money on it and incur large losses. This affects the company's' reputation, as we discussed above, rather than quality of company's other products. Moreover, a product recalls can persuade the buyers not to give up on company, because if a producer recalls purchased products before they break, then the company allegedly cares about its customers.

Price as a sign of quality

There is a popular belief that the more expensive a product is, the better it is. According to Gerstner[322], for many products the relations between quality and price is weak; hence for many products, higher price appears to be poor signals of higher quality. Consumers often assess the quality of a product based on its price, where higher prices allegedly

---

[319]S. Fernandes, R. C. Panda, V.G. Venkatesh, B. N. Swar, Y. Shi, *Measuring the impact of online reviews on consumer purchase decisions*. "Journal of Retailing and Consumer Services", vol. 68, 2020, p.103066.

[320]L. Li, E. Xiao, *Money Talks: Rebate Mechanisms in Reputation System Design*. "Management Science", vol. 60(8), 2014, pp.2054-2072

[321]Lenta.Ru (3), 23.12.2019 available at: https://lenta.ru/news/2019/12/23/fail/ (23.6.2024)

[322]E. Gerstner, *Do Higher Prices Signal Higher Quality*. "Journal of marketing research", vol. 22(2), 1985, pp. 209-215.

indicate higher perceived quality. Higher prices can potentially lead to higher demand for that product[323] (Petrović, Čolić, 2024,). On the one hand, it is clear that a product cannot cost less than its production expenses (even if there are such cases) and it has a reasonable price. However, we cannot see where is the limit to the growth of the price. An ordinary woman's handbag can cost anywhere from 10-15 euros and up to infinity. The production cost of a bag for 1000 euros is much lower and thus the price does not indicate the correlated quality of the product in comparison to bags priced at 15 euros, 40 euros or 100 euros. We thus assume that when determining quality, one cannot rely on the price of products.

Economical capacity of consumers in Slovenia

People are trying to secure life for themself and their family members who are not able or maybe just do not want to work. Maslow's[324] pyramid can be our orienteer in understanding not only how we fulfil our needs but also how we spend money. Initially, we need food, safety, love, etc. Many of the things necessary for the survival are payable. But how do we choose for what to pay? First of all, our buying capacity is based on amount of money which we earn. For understanding mathematical logic of it and for our purposes and possibility to count everything what is important for this work average person/family (in Slovenia) should be taken to the account[325].

In understanding of the average family (in Slovenia) there is an established stereotype about its composition, namely two adults and two children. According to SURS 1[326], average age when young generations (18-34 years) moving out from parents' house is 29,1 years. Slovenian statistics agency[327] provides following data regarding minimum which is considered necessary to survival for 2 (family without kids) or 4 people (family with 2 kids). For purposes of this article, we will consider basic household size as

[323]M. Petrović, L. Čolić, *The dual role of price in Consumer decision-making*. 7th International Conference on Management and Organization:Mananging paradoxes in and across organisations, Belgrade, 21-22.6.2024. pp193-195.
[324]A. H. Maslow, T*he instinctoid nature of basic needs*. "Journal of personality", *22,1954,* pp. 326–347.
[325]SURS 1 (2023) Available at: https://www.stat.si/StatWeb/News/Index/11262 (01.08.2024)
[326]SURS 1, op.cit.
[327]SURS (2024) Available at: https://www.stat.si/StatWeb/Field/Index/15 (01.08.2024)

2 adults and 2 kids. According to SURS[328], family with 2 kids should have 1.896 EUR net not to slide below poverty line. A tenth of employees received an average of less than minimal salary EUR 830, and 1% of employees received more than EUR 4,051 net per month. Amount of money people should get, or actually get to the pocket is different. The national average salary in Slovenia for this moment is 1480,90 eur net[329]. At the same time, 63,4 % of employees received an average monthly net salary, lower than the national average.

However, for the purposes of this article, we will take into the consideration aformenetioned average net salary. If two people in family with 2 kids are working, then they get together 2.961,8 EUR net per month or 35.541,6 EUR per year (we need to keep in mind that more then 63% of workers earn less). According to SURS[330] information on poverty, the family with two children needs 1.896 EUR net per month not to fall under the poverty threshold (yearly 22.752 EUR). This is what is needed not to be considered poor, and does not mean that covers the actual expenses of the family. According to SURS[331] average household expenditure in 2022 was 24.329 EUR. Expenditure for transport, food, non-alcoholic beverages and housing amounted to 12.593 EUR (more than 50% of household expenditure). Running costs, individual expenses and non-essential expenditures are excluded. In 2023 inflation was about 7% and, so that means that yearly expenditures would raise to 26.032,03 EUR. After the expenditures on the average in 2023 in average family should have excess revenue of about 9.500 EUR. This statistical presentation does not including the fact that almost two thirds of workers earn less than average salary.

If a family wants to live in their own apartments or house, we must take this into account and add the cost of a loan to purchase real estate. Also, if the family will rent living space, we need to take into account the cost of rent. The majority, 60 percent of two-room apartments, are being rented this year for 500 to 1,000 euros, last year the price of most started at 600 euros and reached up to 1,000 euros per month. The average price calculated per square meter was 14 euros in 2023, and more than 17 in 2024. Rents in

[328]SURS 2 (2023) https://www.stat.si/StatWeb/en/News/Index/11486 (01.08.2024)
[329]SURS 1, op.cit.
[330]SURS 2, op.cit.
[331]SURS, op.cit.

this segment of apartments jumped by almost 20 percent on average[332]. 500 EUR per month is 6000 EUR per year if people are renting in Ljubljana (however, it is necessary to note that for such price rented place is not suitable for family of four). In other cities price for rent can be lower, as well as the general standard. Loans are a way to overcome the current financial needs and prices of them can be different as well[333].

Table 1: Sizes of loans for residents of Slovenia.

Loan amount Interest rate	Consumer loans **15.000 €** 5 % p.a.		Housing loan **150.000 €** 3 % p.a.	
Return period Monthly instalment	4 years 345,44 €	7 years 212,01 €	15 years 1.035,87 €	20 years 831,90 €
Interests	1.581,09 €	2.808,73 €	36.457,04 €	49.655,14 €

Source: ZPS, 2024

This, it is possible to see that if a family of two adults and two children tries to live independently and if both adult family members receive an average salary (taking into the account that most of them they receive less), then it is possible to assume that there is almost no financial capacity to buy luxury items or more expensive things (more expensive that the average cost of the most purchased items). Due to limited resources, consumer's loans are the solution for unplanned purchases next to the strict financial management that, for the majority of people, does not permit purchases of goods of higher price.

Attempt to establish the price – quality equilibrium: Case of Slovenian online shopping

Life standard can be measured trough the purchases that people do. Not only on the level of housing, cars and luxury brands but also on the level of more daily products, which are

[332]K.N., *Ko misliš, da višje ne more iti, se zgodi podražitev za 20 odstotkov*. Available at: https://www.zurnal24.si/pod-streho/nepremicnine/ko-mislis-da-visje-ne-more-iti-se-zgodi-podrazitev-za-20-odstotkov-424581 (4.7.2024)

[333]ZPS, *Kako dolžina kredita vpliva na znesek obresti?,* Available at https://www.zps.si/nasveti-in-vodniki/kako-dolzina-kredita-vpliva-na-znesek-obresti-2024-04-22 (13.6.2024)

not considered to be absolutely daily products. Selling statistics is rather limited, so we are trying to relay on the data available. In Slovenian there are three main aggregating websites, that Slovenian residents can use to order various goods (excluding grocery products). These are Mimoverste.com, Ceneje.si, Enaa.com. On mimoverste.com, one can find a filter of the most purchased products of specific categories, which can give us insight in buying preferences. We will take several types of the products that households usually have and are spread between basic standard up to semi-luxury products. First we will present 10 most sold models of each of selected products, calculate their average price and further compare it to average price of all supply in the category. This way we will be able present the positioning the average price of ten most sold models of certain products compared to total average. This way, we will be able to determine also the acceptable level of quality, based on previously discussed assumption that price, at least partially, reflect the quality level. For the purpose of our work, we will take the following goods: refrigerator, washing machine, kitchen robot, smart TV. These items are selected because they are widespread in everyday life as well as they represent more (washing machine, refrigerator) or less needed products (smart TV, kitchen robot). Prices and name of items were taken on 25.06.2024.

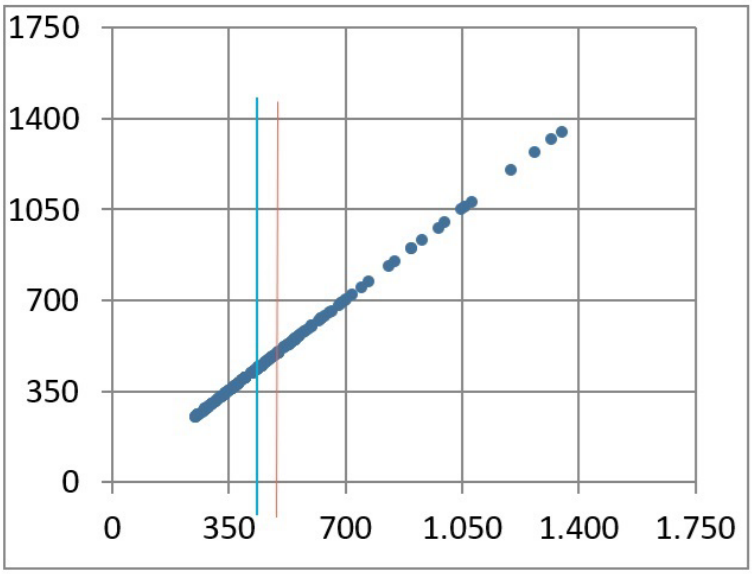
Table 2: Prices of most sold selected products in observed categories.

Washing machine	Price	Refrigerator	Price	Kitchen robot	Price	Smart TV	Price
Candy CS4 1272DE/1-S	264,9 €	VOX electronics KG 2710 F	209,99 €	Rosmarino Infinity PRO	99,90€	Hisense 55A69K 4K UHD DLED	349 €
Gorenje WNHEI62SAS	309,90€	VOX electronics KS1020F	129,99 €	Ruhhy 6,2 l, 2200 W Ruhhy 16745	76,90€	Philips The One 43PUS8558/12 4K UHD	399 €
Beko B3WFU78225WB	599 €	VOX electronics KS 0610 F	109,99 €	Bosch MUM58L20	229,90€	Samsung QE55Q60CAUXXH 4K	544,90 €
Bosch WGG14403BY	599 €	LORD R6	119,90 €	Gorenje MMC1500BS	289,90€	Hisense 32A5KQ F	229 €

Washing machine	Price	Refrigerator	Price	Kitchen robot	Price	Smart TV	Price
Bosch WAN28164BY	529 €	Hisense RR106D4CBF	179 €	Kenwood FDP22.130GY	69,99 €	Hisense 40A5KQ FHD QLED	269 €
Gorenje WNHEI72SAS	359,90€	Candy CDG1S514EW	259,99 €	Bosch MUM5X720	349,90€	Samsung UE43CU8072U XXH 4K	359,90 €
Beko B3WFU77225W B	339 €	Amica KGC15635B	469,90	CezarChef	174,95€	LG 55UR7800	399,99 €
Bosch WAN28270BY	549 €	Gorenje RF4142PW4	279,90 €	Gorenje MMC1005RW	169,90€	Samsung QE65S90CATX XH 4K	1.599 €
Candy CSO 6106TWMB6/1-S	399 €	Gorenje R492PW	224,90 €	Rosmarino Infinity PRO	99,90 €	TCL 55C645 4K	409 €
Beko WUE8622BXC W	399 €	-	-	Philips HR2665/96	299,99 €	Trevi 2409 LED	167,99 €

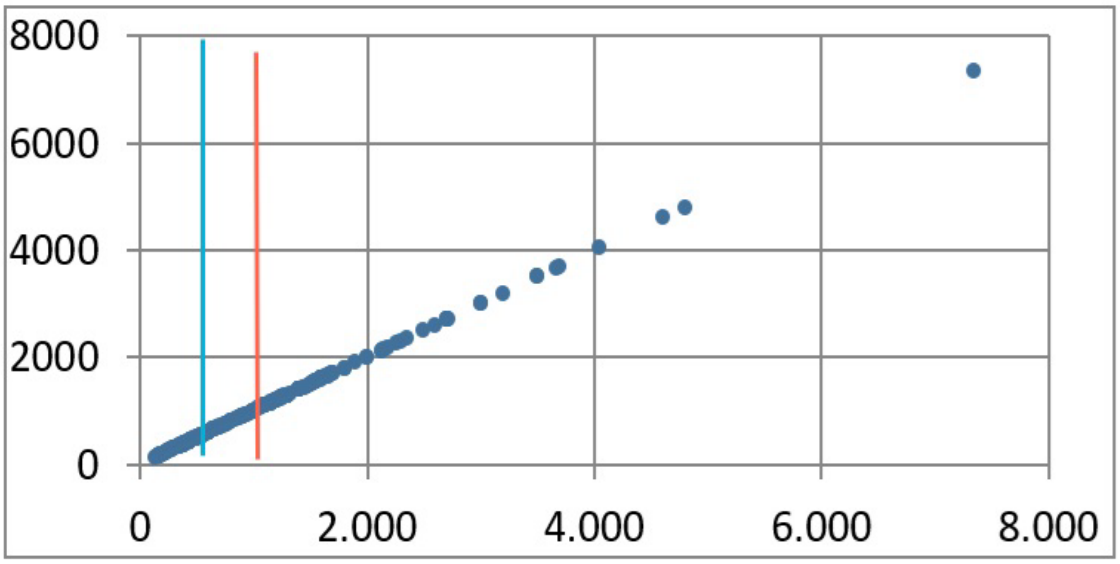
Source: mimovrste.com

Average price of 10 most bought washing machines is 435€. On Graph 1 it is marked with blue line. Average price of all available washing machines is 496 € (marked by red line), which is only 61 € different from the average price of 10 most sold washing machines. However, the purchased washing machines, according to information from the website, remain cheaper than the average price for a washing machine.



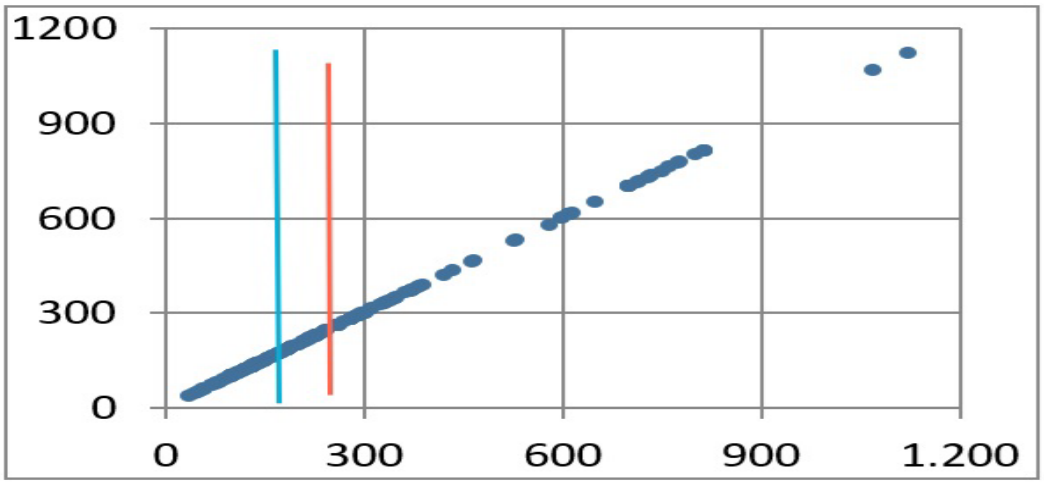
***Graph 1**: Prices of washing machine on mimovrste.com.*
Source: own presentation based on mimovrste.com. (25.6.2024)

Average price of the most bought SMART TV is 473 €. On Graph 2 marked by blue line. All prices above the average between all SMART TV prices is 1062 € (marked by red line), which is 589 € different from the average price for a Smart TV. The purchased SMART TV average, according to information from the website, remain cheaper than the average price of all available SMART TVs for a bit more than two times. That is mean people does not want to spent more money than approximately minimum on something which is not live important. This statement can be tested by checking kitchen robot, which can be also understood as not necessary device and refrigerator like important product.



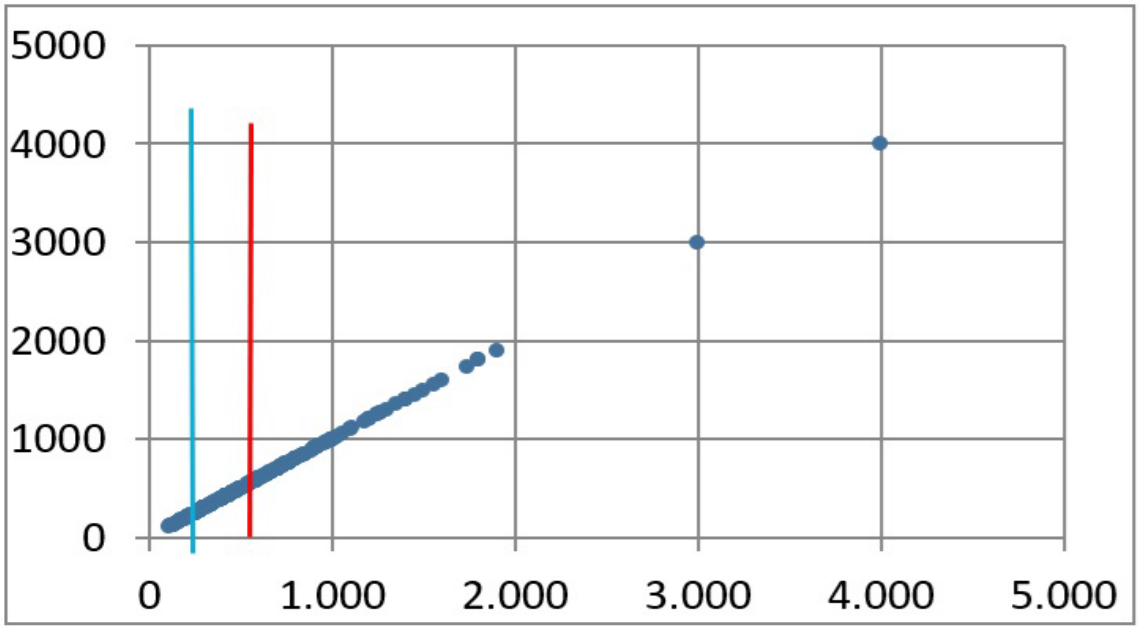
***Graph 2**: Prices of smart TV on mimovrste.com*
Source: own presentation based on mimovrste.com. (25.6.2024)

Average price of the most bought Kitchen robot is 186 euros. On Graph 3 it is showed by blue line. Thus, all prices above the average between all kitchen robot prices is 269 euros (marked by red line), which is 83 euros different from the average price for a kitchen robot. The purchased Kitchen robot, according to information from the website, remain cheaper than the average price for Kitchen robot. Here we did not see such a huge difference for the reason that there are many very new devices that affect the rest and, in general, this device cost less than SMART TV. This still indicates that people do not want to spent more money than approximately minimum on something which is not live important.



***Graph 3**: Prices of kitchen robots on mimovrste.com*
Source: own presentation based on mimovrste.com. (25.6.2024)

Average price of the most bought refrigerator is 221 euros. On graph 4, blue line indicates the average of most bought products, while red line shows the average price of all available refrigerators. Average price for all available refrigerators is 615 Eur, which is 394 Euros more than the average price of most sold refrigerators on analysed portal. The purchased refrigerator, according to information from the website, remain cheaper than the average price refrigerator for a bit more than two times.



***Graph 4**: Prices of refrigerators on mimovrste.com*
Source: own presentation based on mimovrste.com. (25.6.2024)

All graphs clearly show that people prefer to buy goods closer to the lower limit of their cost. Judging by the fact that they are included in the list of the most popular products on the site and people leave marks and reviews on them, we believe that the quality of this products is acceptable for people, or better that this is the level of quality that people understand acceptable based on their financial ability and expectation of performance. All four selected product types show that people prefer to buy under absolute average of the offer. And that people are more willing to spend closer to the product offer (so buy more expensive) in case of products that are considered as more basic within household (refrigerator and washing machine). In none of the cases, people in average buy higher end products (these with prices higher than average price of total supply available).

Conclusions

Article is based on the idea that quality is category of technical absolutism of perfection but it is in many ways negotiable, by branding on one side and by financial capacities on the demand side. Still the principle that more expensive goods are goods of higher quality remains valid. In this perspective we shortly presented Slovenian households' ability to spend money on products that we can consider high quality based on the price. Slovenian economic conditions (next to life priorities) reduce the ability of households to spend on high end products. Selection of four common products and analysis of the basic buying patterns in online store showed that Slovenians will buy under the average price of the products available also in online environment. This can be connected to lack of financial sources as well as to the assumption that even cheaper products will provide sufficient quality of the products in the perspective of the quality and durability. At the same time we can assume that, Slovenians behave rationally also in the case of on-line shopping, contrary to the general idea that people spend more foolishly in internet environment. There are many opportunities for future research here, namely on other aspects of living standards in Slovenia. Among more relevant questions arising is if buying "cheap" is only question of available finances or it might be actually question of national mentality.

REFERENCES

Aaker, D.A., *Managing brand equity: Capitalizing on the value of a brand name*. The Free Press, New York, London, Toronto, Sydney, 2009.

Aaker, D.A., Joachimsthaler, E. *Brand Leadership*, The free press, New York ,2012.

American Marketing Association Dictionary Archived 2012-06-11 at the Wayback Machine. Retrieved 2011-06-29. The Marketing Accountability Standards Board (MASB) endorses this definition as part of its ongoing Common Language in Marketing Project Archived 2019-04-05 at the Wayback Machine

Amir, O., Label, O., Ariely, D., *Making Consumption Decisions by following Personal Rules*. In E. S. Ratneshwar, M. D. Glen (eds.): *Inside Consumption*. London: Routledge. London, 2005, pp. 86-101.

Chen, T.,Samaranayake, P., Cen, XY, Qi, M.,*The Impact of Online Reviews on Consumers' Purchasing Decisions: Evidence From an Eye-Tracking Study*. "Frontiers in Psychology", 13, 2022, p. 865702.

Chillders, C.C., Lemon, L.L., Hoy, M.G., *Agency perspective on influencer marketing campaigns*. "Journal of Current Issues & Research in Advertising", 40 (3), 2019, pp. 258-274.

Fernandes, S., Panda, R. C., Venkatesh, V.G. Swar, B.N., Shi, Y., *Measuring the impact of online reviews on consumer purchase decisions*. "Journal of Retailing and Consumer Services", 68, 2020, p.103066.

Gerstner, E., *Do Higher Prices Signal Higher Quality*. "Journal of marketing research" 22(2), 1985, pp. 209-215.

K.N. *Ko misliš, da višje ne more iti, se zgodi podražitev za 20 odstotkov*. Available at: https://www.zurnal24.si/pod-streho/nepremicnine/ko-mislis-da-visje-ne-more-iti-se-zgodi-podrazitev-za-20-odstotkov-424581 (4.7.2024)

Karev, E., *Mark them with my Mark': Human Branding in Egypt*. "The Journal of Egyptian Archaeology". 108(1-2), 2022, pp. 191-203.
Leibenstein, H., *Bandwagon, Snob and Veblen Effects in the Theory of Consumer Demand*. "Quarterly Journal of Economics", 64(2), 1950, pp. 183-207.
Lenta.Ru (3), 23.12.2019 available at: https://lenta.ru/news/2019/12/23/fail/ (23.6.2024)
Li, L., Tadelis, S., Zhou, X., *Buying reputation as a signal of quality: Evidence from an online marketplace*. "The RAND journal of economics", 51(4), 2020, pp. 965-988.
Li, L., Xiao, E., *Money Talks: Rebate Mechanisms in Reputation System Design*. "Management Science", 60(8), 2014, pp.2054-2072.
Maslow A.H., *The instinctoid nature of basic needs*. "Journal of personality", *22,1954,* pp. 326–347.
Moore, K., Reid, S., *The birth of brand: 4000 years of branding*. "Business History", *50(4), 2008,* pp. 419-432.
Minthiu, M.-K., *The buying decision process and types of buying behaviour, Economic sciences*. "Sibiu Alma Mater University Journals. Series A. Economic Sciences", 2(4), 2009, pp. 27-33.
Nelson, P. *Advertising as information,* "Journal of political economy", 82(4), 1974, pp. 729-754.
Orzach, R., Overgaard, P.B., Tauman, Y., *Modest advertising signals strength*. "RAND Journal of Economics", 33(2), 2002, pp. 340-358.
Petrović,M., Čolić, L., *The dual role of price in Consumer decision-making*. 7th International Conference on Management and Organization: Managing paradoxes in and across organisations, Belgrade, 21-22.6.2024. pp193-195.
Prosvirina I., *Price of brand: view of financial specialist*. "Journal Business Key", 5, 2008.
Ratneshwar, E. S., Glen M. D., *Inside consumption: Consumer Motives, Goals and Desires*; In E. S. Ratneshwar, M. D. Glen (eds.): *Inside Consumption*. London: Routledge. London, 2005.
Rizkova, M. *Connection of price and quality for goods*. "News of Tomsk Politechnic University. Georesources Engineering", 323(6), 2013, pp. 74-80.
Rozanova, N.M., *Modern consumer caught in the web of global economy, "*Bulletin of the Institute of Economics of the Russian Academy of Sciences". 2024(3), 2024 pp. 26-46.
Sindhya, V. A., *Study on the influence and impact of advertising to consumer purchase motive among student teachers. "*IOSR Journal of Research and Method in Education", 2(4), 2013, pp. 1-5.
Sokolova, A, Hajer K., *Instagram and YouTube bloggers promote it, why should I buy? How credibility and parasocial interaction influence purchase intentions. "Journal of retailing and consumer services",* 2020(53), 2020, p.101742.
Shpakovskaya, V., *Psihological fenomen of ADS*. In V.S., Rubanov at al. (eds): *"Collection of competitive scientific works of students and undergraduates in two parts"*. BRGTU, Brest, 2018, pp. 235-238.
SURS 1 (2023) Available at: https://www.stat.si/StatWeb/News/Index/11262 (01.08.2024)
SURS 2 (2023) https://www.stat.si/StatWeb/en/News/Index/11486 (01.08.2024)
SURS (2024) Available at: https://www.stat.si/StatWeb/Field/Index/15 (01.08.2024)
Zhang, C., Laroche, M., *Brand hate: a multidimensional construct*, "Journal of Product & Brand Management", 30(3), 2020, pp. 392-414.
ZPS, (2024): *Kako dolžina kredita vpliva na znesek obresti?* Available at https://www.zps.si/nasveti-in-vodniki/kako-dolzina-kredita-vpliva-na-znesek-obresti-2024-04-22 (13.6.2024)
Wondwesen, T.; B.P. Wood, *Followers' engagement with instagram influencers: The role of influencers' content and engagement strategy*. "Journal of retailing and consumer services" 2021(58), 2021, p.102303.
Wright, I. (2023): *The Most Loved and Hated Brands From Every Country*. Available at: https://merchantmachine.co.uk/loved-and-hated-brands/ (20.6.2024)
Internet sources
Ceneje.si, available at http://www. Ceneje.si (20.6.2024)
Enaa.com, available at http://www.enaa.com (21.2024)
Mimovrste.com, available at http://www.mimoverste.com (22.6.2024)

„dot.pl" - czasopismo Rejestru domeny .pl

HOMO GEPETENS. Człowiek i sztuczna inteligencja: karzeł na ramionach olbrzyma?

Kazimierz Krzysztofek

Uniwersytet SWPS (Emeritus), Wydział Nauk Społecznych Warszawa
ORCID: https://orcid.org/0000-0002-1772-8861
E-mail: kkrzysz1@swps.edu.pl

Od kilkunastu miesięcy, po udostępnieniu GPT, ludzie pod każdą szerokością geograficzną zadają sobie pytania, czy stajemy się karłem na ramionach olbrzyma, czy gatunkiem skazanym na wyginięcie jak wiele innych w toku ewolucji? Byłoby to szóste wielkie wymieranie.

Słowa kluczowe: sztuczna inteligencja, czat GPT, systemy AI

Na początek potrzebny jest jednak krótki rzut oka na historię technologii intelektualnych. Kreślę ten szkic, elementarz rozwoju technologii informacyjno-komunikacyjnych, aby pokazać, że bez przełomów w tej dziedzinie nie byłoby inteligencji sztucznej. To truizm niewymagający szerszej opowieści.

Rozwój cywilizacji to kamienie milowe w pozyskiwaniu danych z otoczenia, ich destylowanie, kontekstualizowanie, interpretowanie oraz budowanie na nich wiedzy o człowieku i przyrodzie. Pojedynczy

ESEJ

Received: 15.04.2024
Accepted: 19.05.2024
Published: 27.05.2024

Cite this article as:
K. Krzysztofek
"HOMO GEPETENS. Człowiek i sztuczna inteligencja: karzeł na ramionach olbrzyma?"

DOT.PL, no. 1/ 2024,
10.60097/DOTPL/189310

Corresponding author:
Kazimierz Krzysztofek,
Uniwersytet SWPS, Wydział Nauk Społecznych
E-mail: kkrzysz1@swps.edu.pl

egzemplarz homo pre-sapiens i sapiens miał ograniczoną możliwość gromadzenia danych i tworzenia wiedzy, mógł polegać tylko na własnych zmysłach i spostrzeżeniach, co limitowało zakres wiedzy i szanse podejmowania optymalnych decyzji, czyli w istocie ograniczało inteligencję ludzką rozumianą jako adaptację do otoczenia, uczenia się, myślenia oraz rozwój intelektu rozumianego jako kreowanie reprezentacji świata, idei i całej sfery *episteme*. Do poszerzenia zasobu danych, informacji i wiedzy konieczna była multiplikacja umysłu przez umysł dzięki komunikacji intercerebralnej, bez której człowiek byłby skazany na ślepotę swego umysłu, swoisty autyzm. Rozwój cywilizacji to właśnie rozwój narzędzi komunikacji. Nie wiemy, jakie były one w fazie przedludzkiej, ale to one właśnie uczłowieczały. Kiedy człowiek osiągnął postawę wyprostną mógł uwolnić ręce i opowiadać o świecie, jak go sobie wyobrażał m. in. w malowidłach naskalnych. Kolejne przełomy w komunikacji wykładniczo zwielokrotniały współpracę i współdzielenie umysłów. Mówimy tu o przełomach, ale to były procesy ciągnące się przez setki tysięcy lat. Z czasem się one skracały i w czasach najnowszych liczone są już w latach, czy nawet miesiącach. Człowiek znalazł się w akceleratorze wielkiej mocy. Pierwszym takim wielkim przełomem było powstanie mowy artykułowanej, syntaktycznej, dzięki której dokonywał się przekaz wiedzy w czasie rzeczywistym, a także przekaz międzypokoleniowy. W kulturach plemiennych taką rolę łączników między pokoleniami odgrywali grioci, których zadaniem było zapamiętywanie dziedzictwa przodków – umiejętności, wiedzy, norm społecznych i in.

Wynalazek pisma pozwolił na rozszerzenie komunikacji i akumulację poznania w czasie i w przestrzeni. Rewolucyjną rolę odegrał alfabet, który pozwolił zapisać wiedzę w różnych językach w dwudziestu kilku znakach i umieścić pamięć na zewnętrznym nośniku – tabliczkach glinianych, papirusach, papierze. W nieporównanie większym stopniu uczynił to druk, drukowanie pamfletów, pism ulotnych, książek w formacie kodeksowym, jaki dzisiaj znamy. Druk utorował drogę Oświeceniu. Druga rewolucja w dziedzinie druku, czyli powstanie maszyny rotacyjnej w XIX w. pozwoliło na rozwój wielkonakładowej prasy i bezprecedensową demokratyzację czytelnictwa.

Te wynalazki w zakresie narzędzi komunikacji wymagały jednak środków transportu[334] do przekazu informacji. Książkę, gazetę, fotografię, film, muzykę trzeba było fizycznie transportować. Komunikacja ustna dokonywała się tylko w zasięgu głosu. Pierwszym wynalazkiem, który uwolnił komunikację na dalsze odległości od materialnych środków transportu były - nie licząc sygnałów dymnych – telegraf i telefon. Wiek XX to narodziny mediów elektronicznych, najpierw radia, potem kina i telewizji, a także narzędzi zapisu dźwięku i obrazu na nowych nośnikach płycie winylowej, taśmie magnetycznej, błonie światłoczułej (to jeszcze w XIX w.) i taśmie filmowej. Za przyczyną tych mediów doszło do narodzin komunikacji globalnej i globalnej transmisji danych, informacji, wiedzy w postaci tekstowej, alfanumerycznej, głosowej i wizualnej.

Wiek XX to także wynalazek kodu binarnego, w którym wszystko można zapisać. Dzięki niemu powstała w latach 40. XX w. maszyna cyfrowa – komputer, najpierw jako wielki moloch lampowy, z czasem w latach 80. personalizowany i miniaturyzowany do postaci PC-ta, a następnie laptopa, tabletu, smartfona i smartwatcha. Wynalazkowi komputera towarzyszył rozwój interfejsów: od tekstowego przez graficzny (Windows), haptyczny, głosowy aż po neuronalny. Protokół WWW stworzony przez Tima Bernersa-Lee przyniósł nam na początku lat 90. Internet, jaki znamy w dzisiejszej postaci, a wraz z rozwojem technologii mobilnych ze smartfonem na czele stał się masowy w skali globalnej, dzięki m. in. serwisom społecznościowym. Paradygmat sieciowy zmienił nasze myślenie.

Ponad pół wieku temu słownik technologiczny wzbogacił się o pojęcie sztucznej inteligencji. Miało to oczywiście związek z rozwojem technik komputerowych. Zastępowały one pewne funkcje umysłu – z dzisiejszej perspektywy w bardzo ograniczonym stopniu - kalkulacyjną, pamięciową, procesoryczną. To wystarczyło, aby to nazwać sztuczną inteligencją, bo jak nie nazwać, skoro to były „mózgi elektronowe”. Nazwa bardzo na wyrost.

[334] Pomijam tu rozwój środków transportu**. Mówiliśmy tu o komunikacji za pośrednictwem symboli, ale wielką role odegrała także komunikacja fizyczna czyli rozwój transportu Dzięki nim człowiek poszerzał swoją wiedzę o świecie i komunikował ją innym.**

Od tego czasu AI zaczęła nam towarzyszyć w wielu działaniach, była cichym agentem, obecnym „wszędzie i nigdzie". W odróżnieniu od widzialnych technik przemysłowych które nie ukrywały swojego istnienia, technologie intelektualne związane z komputerem były niewidoczne, stały się inteligencją tła (*ambient intelligence*)**.** Kiedy narzędzie wrasta w nas, „zagnieżdża się", przestajemy je dostrzegać. Tak było do czasu pojawienia się silnika GPT, zwłaszcza w jego czwartej wersji (dziś jest to zaawansowana darmowa wersja Chat GPTomni), zasilającego chat. W ciągu kilku tygodni zanotował on bezprecedensowy *hype*.

Tak doszliśmy do najnowszego etapu AI – GPT, którą by można nazwać 2.0 mamy bowiem do czynienia z nową jakością, przejściem fazowym. Ale po kolei. Akronim GPT nie brzmi wdzięcznie ani heroicznie, a na to zasługuje. Fonetycznie brzmi DżiPiTi, a to kojarzy się z „Dżepetto", który wystrugał Pinokia. GPT też został „wystrugany" tyle że z Big Data, wielkiej mocy obliczeniowej i zaawansowanych algorytmów. Bez tych trzech rzeczy by go nie było. I też nie wiadomo, co z niego wyrośnie.

OpenAI, twórca GPT 3 i jego kolejnych wersji 3,5, 4 a w niedługiej perspektywie 5 (już karmionej danymi) choć był pionierem w dziedzinie wielkich modeli językowych (LLM), to nie ma monopolu na rozwijanie zawansowanej sztucznej inteligencji. Nowe modele rosną w ostatnich latach jak grzyby po deszczu by wymienić Barda, Gemini (Google), Lama i in.. Znamionuje to najważniejszy makrotrend cywilizacyjny, jakim jest postęp w rozwoju sztucznej inteligencji. To stwierdzenie to dziś banał. O sztucznej inteligencji mówi się już od kilkudziesięciu lat, ale to wiek XXI zostanie zapewne kiedyś nazwany wiekiem AI. Jest wiele mikrotrendów o różnych wektorach, ale ich wypadkową wyznacza AI. Choć dziś oczywiście nie wiemy jeszcze na pewno, jak nazwiemy *tempus nostrum* , nazwy wiekom, epokom nadaje się ex post. Na razie wydaje się, że pierwsze lata trzeciej dekady naszego stulecia zapowiadają przełom, choć do końca XXI w. jeszcze daleko i może być wiele przełomów. Przełom goni przełom.

Przypomnijmy kilka faktów. Jako pierwszy słowa „inteligencja" w kontekście maszyn użył w 1950 r. Ojciec komputera, Allan Turing, w artykule pt. „Computing Machinery and Intelligence". Pięć lat później amerykański informatyk, McCarthy, laureat Nagrody

Turinga, i po raz pierwszy użył określenia „sztuczna inteligencja” w 1956 roku podczas konferencji zorganizowanej przez Dartmouth College w New Hampshire. Zdefiniował w następujący sposób: „konstruowanie maszyn, o których działaniu dałoby się powiedzieć, że są podobne do ludzkich przejawów inteligencji”. Już wtedy puszczano wodze fantazji i posuwano się do tak śmiałych określeń jak to, że AI to system, który **świadomie** (sic!) postrzega otoczenie i reaguje na nie tak, aby zmaksymalizować swoje szanse powodzenia”. Kilkadziesiąt lat później nikt nie ma odwagi mówić o świadomej AI, bo takiej po prostu nie ma i można tylko fantazjować, czy kiedykolwiek będzie.

Przy kolejnych osiągnięciach w tej dziedzinie mówiono, że to już jest szczyt, po czym okazywało się, że był relatywnie niewielki krok w porównaniu do tego, co się dzieje dziś, gdy rozwój AI to prawdziwy rollercoster, jazda bez trzymanki. Bo to w największym stopniu może zadecydować o przewadze technologicznej, ale także oczywiście biznesowej, militarnej, geostrategicznej. Kto rozwinie AI szybciej ten zapewni sobie większe bezpieczeństwo w każdej istotnej dziedzinie. Im szybszy postęp technologiczny tym szybsze starzenie się kolejnych generacji technologii.

Poniżej kilka luźnych refleksji o tym, czy mamy do czynienia z wielką zmianą cywilizacyjną, a jeśli tak to jaką.

Chat GPT3 udostępniono użytkownikom pod koniec 2022 r. Zaskoczył on wszystkich, tempem ekspansji – 100 mln użytkowników w ciągu 2 miesięcy bijąc na głowę wszystkie poprzednie wynalazki w dziedzinie komunikacji, czy szerzej – technologii. Odnosi się wrażenie, że ten GPT jako silnik chata miał znamionować narodziny sztucznej inteligencji (dalej: AI), co oczywiście byłoby nieprawdą, bo w istocie nie jest on tak bardzo przełomowy. Chatbotów od czasów słynnej Elizy z lat 60. było bez liku.

Tak więc sztuczna inteligencja jest z nami już od lat 50. ub. wieku, ale Chat GPT gwałtownie wtargnął w nasze życie. Rewolucja polega na udostępnieniu AI masom, tak jak PC w latach 80. Internetu WWW na początku lat 90. A wcześniej druku, prasy, mediów elektronicznych, samochodu i in. AI w wersji GPT jest najszybszą i największą zaadaptowaną społecznie technologią w dziejach ludzkich. Dzięki chatowi ludzie są świadomi interakcji z AI, wcześniej uprzedmiotowiona AI była niewidoczna, były

samochody autonomiczne, chatboty, asystenci głosowi, m.in. w smsach, ale z tego korzystał relatywnie niewielki procent. Chat GPT, generatywny przetrenowany transformer to radykalnie zdemokratyzował.

Człowiek osiągał rozwój umysłowy dzięki trenowaniu swej inteligencji, naturalnych algorytmów, dostarczaniu jej *feedu* – opanowywał język ojczysty, uczył się języków obcych, poezji na pamięć itp. Teraz trenuje AI coraz mniej trenując swoje algorytmy w głowie. Czy to nie jest prosta droga do porażki człowieka?

Sztuczna inteligencja stała się gwiazdą leksykalną wypierając wszystkie inne. Należę do pokolenia boomersów , które się fascynuje AI i ciągle się dziwi, że to działa. Dla pokolenia internetowego to oczywiste; podobnie było z samochodem czy samolotem, radiem.

Można na AI patrzeć ze wszystkich perspektyw, bo przenika ona każdą sferę ludzkiej egzystencji: z perspektywy inżynieryjnej, psychologicznej, socjologicznej, politologicznej, biologicznej, kognitywistycznej i in. I oczywiście, a może przede wszystkim – komunikacji we wszystkich wymiarach: międzyludzkim, ludzi z maszynami i maszyn z maszynami. Bo już kilku dekad nie możemy się ograniczać tylko do komunikacji między ludźmi. Nie wchodzę tu w szczegółowe dziedzinowe omawianie natury sztucznej inteligencji, pokuszę się jedynie o luźne refleksje socjologa z ciągotkami do filozofii społecznej.

Powstało od lat 60. ub. wieku mnóstwo teorii objaśniających istotę i konsekwencje zwrotu cyfrowego, w tym sztucznej inteligencji, sieci neuronowych, przetwarzania języka naturalnego i in., ale one nie tłumaczą wszystkiego, zwłaszcza uznawanego za przełom w rozwoju sztucznej inteligencji transformera GPT.

Dlaczego zatem tak wielki *hype*? Przyczyn może być wiele i zapewne jest. W przeszłości było wiele przełomów komunikacyjnych, ale najbardziej uczłowieczające nasz gatunek było powstanie mowy artykułowanej, syntaktycznej. Język najbardziej kojarzymy z inteligencją, czy wręcz świadomością. Nie mamy lepszego narzędzia komunikacji niż język naturalny (który w istocie jest produktem, ale i „silnikiem"). Dlatego wielkie modele językowe, w tym Chat GPT uznajemy za przełom, największy postęp w dziedzinie sztucznej inteligencji. Widać w języku, jakim ją nazywamy i opisujemy. AI w wydaniu GPT personifikujemy jak nigdy wcześniej: mówimy, że ona czuje, myśli, rozumie itp.. Można

oczywiście się upierać, że to nadużycie, ale trzeba się zgodzić z potoczną prawdą, że rzeczy nie mają się tak, jak się mają, ale jak się ludziom wydaje, że się mają. Ważna jest *episteme*, jako wiedza zweryfikowana, ale także *doxa* – „mniemanologia stosowana". Musimy zatem postrzegać i badać AI nie tylko jako twór techniki, ale także jako byt z pespektywy psychologii czy etyki, jak osobę. Okazuje się, że inteligencja, która wyewoluowała na substracie białkowym nie musi być niepowtarzalnym zjawiskiem. Jest coraz mniej kompetencji umysłowych człowieka, którymi AI by nie potrafiła zawładnąć. Nie jest przy tym istotne, czy ona jest świadoma, tylko czy jest tak odbierana. Staje się wszechobecna - *ubintelligence*, jest wszędzie i nigdzie, cichy agent. Nie da się z niej wyłączyć, nawet jeśli ktoś nie zechce z niej korzystać, to i tak będzie miej wpływ na jego/jej życie. *Ubintelligence* to stróż nocny w wersji cyfrowej; niewidzialna ręka rynku i władzy.

Rozwój sztucznej inteligencji był budowany na emulowaniu ludzkiej, choć porównywanie jej w skali 1 do 1 nie ma sensu (gdy np. mówimy, że jest ona dziś na poziomie ośmioletniego dziecka). To jest porównywanie jabłek do bananów. Nie ma więc większego sensu twierdzenie, że AI jest na tyle mądra na ile my jesteśmy mądrzy. Wielki postęp dokona się już nie tyle przez naśladowanie ludzkiej inteligencji i przetwarzaniu wiedzy człowieka o sobie i przyrodzie, ile na odkrywaniu inteligencji samej natury, bo ulega wątpliwości, że ona (inteligencja) zapewnia przyrodzie ład i harmonię. Nie wiemy jeszcze czy jesteśmy już w fazie przejścia od wąskiej AI do AGI (*artificial general intelligence*), a w dalszej perspektywie Super AI oznaczającej nadejście osobliwości (singularity), jak wieszczy Kurt Kurzweil. Na horyzoncie pojawia się Qstar (Q*) – nowa generacja AI, która „zhakuje" matematykę, co by oznaczało, że wejdzie ona w rolę fizyków, chemików, astronomów, biomedyków i innych przedstawicieli twardych nauk – *scientists*, dla których matematyka jest królową wszystkiego. Być może wtedy powstanie tak wytęskniona ogólna teoria wszystkiego. Wszystkie tajemnice natury zostaną rozwikłane. Kosmos będzie widać jak na dłoni. Człowiek zawsze wydzierał tajemnice naturze, ale w tym wydzieraniu zastąpi go sztuczna inteligencja nowej generacji zasilana komputingiem kwantowym.

Interesującą intuicją wykazał się Jean Baudrillard (2001), którego zdaniem nasza rzeczywistość, środowisko życia zapośredniczone przez media, technologie cyfrowe,

staje się coraz bardziej „obsceniczna", symulakryczna. Obscenizacja i symulakryzacja rzeczywistości biorą się stąd, że technologie cyfrowe czynią ją bardziej widzialną niż rzeczywistość fizyczna, staje się ona *hyperreality*, wydzierając tajemnice ludziom, przyrodzie, światu. Nic się już przed nimi nie ukryje, ani priony, ani bakterie czy kopulujące mszyce. Owa nakładka cyfrowa na ludzi, przyrodę, kosmos, dno oceanów itp., ma ujawniać potencjalnie wszystkie sekrety. Jest to coś w rodzaju uniwersalnego, przekraczającego wszystkie epoki Wiki Leaks.

AI kreuje nowy typ relacji i interakcji między człowiekiem i narzędziem, tak jak go opisał zmarły niedawno amerykański filozof nauki i technologii, Don Ihde (2009). Pierwszy typ to narzędzia na zewnątrz człowieka, jak np. kij czy młotek, czy bardziej zaawansowane jak np. termometr za oknem. Drugi typ to narzędzia i technologie wchodzące do wnętrza człowieka (jak rozrusznik serca), albo będące symbiotyczną ekstensją jego organów czy zmysłów (protezy kończyn, okulary). Typ trzeci to technologie tła, wysoce zaawansowane inżynieryjnie będące wytworem rewolucji przemysłowej (elektryczność, której nie widzimy, urządzenia AGD). Typ czwarty to ekstensje umysłu epoki informatycznej w postaci komputera, smartfona, czy obecnie sztucznej inteligencji. Ich cechą jest to software emigruje z umysłu na zewnętrzne nośniki. W tym typie relacji technologie nie są już w tle, dotyczy to zwłaszcza AI, stają się niejako partnerem komunikacyjnym, interaktorem, już nie przedmiotem, a INNYM. Natura - kultura wyposażyła nas do interakcji z innym człowiekiem i tak skłonni jesteśmy traktować AI

Zdaniem Harolda Innisa (1951) w każdej epoce dziejów ludzkich społeczeństwo, gospodarka, kultura posiadały system komunikacji oparty o dominujące medium. W każdym społeczeństwie istniały punkty węzłowe, w których akumulowano i przekazywano wiedzę o gospodarowaniu, kulturze, polityce itp. Przez wieki takimi węzłami były szkoły, uniwersytety, biblioteki, instytucje kościelne (zwłaszcza niektóre zgromadzenia zakonne) później media masowe. Obecnie funkcję takiego mega węzła zaczyna pełnić AI. Ci, którzy sprawują kontrolę nad tymi węzłami punktami, posiadają również władzę. W społeczeństwie masowym takimi punktami były wyłącznie duże instytucje hierarchiczne: rządy państw, przedsiębiorstwa, koncerny medialne itp. AI sprawia jednak, że punkty takie ulegają rozproszeniu i zwielokrotnieniu. W rezultacie dostęp do wszelkich informacji jest

łatwiejszy, a instytucje hierarchiczne tracą pozycję informacyjnego monopolu, choć stare monopole informacyjne zostały zastąpione przez nowe (GAFAM).

Zadajemy sobie pytanie, dlaczego w tak krótkim czasie udało się skonstruować coś, co tak udatnie symuluje ludzką inteligencję. Widocznie myślenie, mowa, rozumowanie nie są aż tak skomplikowane skoro w ciągu krótkiego czasu w porównaniu do ewolucji mózgu da się to naśladować.

Czas na konstatację, że w społeczeństwie nasyconym sztuczną inteligencją wielkie kompleksy ekonomiczno-kulturowe rodzą się już nie pod wpływem wynalazków, wykorzystywanych następnie do produkcji dóbr materialnych (jak np. samochód), ale pod wpływem generatywnych transformerów wykorzystanych do przetwarzania symboli. Technologie AI nie są tylko medium komunikacji, ale także narzędziem kreowania nowego ekosystemu społecznego, w którym znajduje ujście coraz więcej energii ludzi we wszystkich sferach ich aktywności: ekonomii, polityce, kulturze, edukacji, rozrywki itp.

Czy stoimy w obliczu czwartej detronizacji człowieka? Pierwsza była Kopernikańska – planeta ludzi przestała być centrum wszechświata wokół której kręciło się słońce i wszystko inne w przestrzeni pozaziemskiej; druga, Darwinowska teoria ewolucji ogłosiła zwierzęce pochodzenie człowieka; trzecia, Freudowska - nie ma wolnej woli, rządzi człowiekiem podświadomość, w której umiejscowione są mroczne popędy biologiczne, silnik psychodynamiczny. Czwartą detronizacją ma być nie tyle samo stworzenie sztucznej inteligencji przez człowieka, ile jej wyemancypowanie się ze świata ludzkiego i przewyższenie ludzkiej. Wedle niektórych poglądów detronizacją będzie sztuczne życie: człowiek odbierze stwórcy, czy jak to woli naturze monopol kreowania życia. Nas razie udało się stworzyć sztuczną bakterię. Pewną namiastką są ksenoboty – programowane algorytmami hybrydy żywych organizmów (żaby afrykańskiej).

Pytania graniczne

Jak żyć w chaosie niesionym przez zaburzające technologie? Co to w ogóle jest chaos? To procesy w nas i wokół nas, które są niekontrolowane i niezarządzalne. Kiedy procesy są logiczne i długofalowe, to można je przewidywać i przystosowywać się do nich, żeby żyć w jakim takim komforcie. Jednostka nie ma na nie większego wpływu. Działają wielkie i

silne wektory, które składają się na wypadkową pchającą nas w jakimś kierunku. Te wielkie procesy tworzą ład, który trzeba znać, żeby wiedzieć, jak się w nim poruszać. Żeby nie być niesionym przez nieznane i nie być wziętym przez zaskoczenie. Inaczej jest w chaosie; drobny czynnik może wywołać wielką zmianę, jak przysłowiowy ruch skrzydełek motyla. Wielką sztuką jest wiedzieć, gdzie jest *locus of control*. Najlepiej, jeśli kontrola umiejscowiona jest w nas, wtedy jesteśmy wewnątrz- a nie zewnątrzsterowni. Kiedy nie mamy kontroli nad własnym życiem, to tak jakby odjechał nam już nie tylko pociąg, ale peron, czy cały dworzec.

Jak sobie z tym radzić? Jak przywrócić ład we wszechświecie na naszą małą skalę? Najprostsza odpowiedź: wyspać się, najeść do syta i wypić drinka. Są jednostki, którym to nie wystarcza i próbują zmagać się ze światem, znaleźć doń klucz, zhakować chaos. Dziś wszyscy wszystkich i wszystko hakują. Co to znaczy hakować? Przejąć nad czymś kontrolę, włamać się do systemu, aby nim sterować. Dla misji, fantazji, zabawy, przetestowania własnych zdolności, często po prostu dla widzimisię.

Mamy trzy warstwy mózgu, najstarszy – gadzi - odpowiada za podstawowe funkcje życiowe, przetrwanie organizmu, tu dokonuje się *gros* przetwarzania danych i informacji, które nie są rejestrowane na poziomie świadomości – czymkolwiek ona jest, bo nie mamy satysfakcjonującej definicji. Najstarsza znana mi pochodzi od Johna Locke (ok. 1680 r.), który rozumiał świadomość, ściślej: samoświadomość, jako zdolność osobnika postrzegania tego, co się dzieje w jego własnym umyśle. Jakiego osobnika – czy tylko ludzkiego? Tego nie wiemy; może pozwoli nam się o tym dowiedzieć sztuczna inteligencja.

Gadzi mózg będzie potrzebny, dopóki gatunek ludzki pozostanie biologiczny i mózg będzie odpowiedzialny za jego przetrwanie, za funkcje fizjologiczne. Jeśli kiedyś człowiek będzie budowany z jakichś kompozytów, to już nie będzie fizjologia a syntetyka, mechanika i informatyka. Czy w takim razie będzie to jeszcze życie? To jest pytanie o istotę człowieczeństwa.

Dopóki będziemy ludźmi, to potrzebny będzie też mózg ssaczy regulujący układ limbiczny, a więc m.in. emocje, relacje międzyosobnicze i in. Zdanie wielu teoretyków umysłu i poznania, kognitywistów, inteligencja wyewoluowała głównie dzięki temu, że z potrzeby

przetrwania ludzie musieli rozpoznawać emocje u innych, aby się domyślać, czego się po nich spodziewać. Stąd potrzeba rozpoznawania wzorca, zwłaszcza twarzy, na której malują się emocje i mikroekspresje. Nasza wyobraźnia podsuwa nam podobizny twarzy, nawet jeśli to nie są twarze a jakieś obrazy wygenerowane w naszym umyśle jako twarzopodobne. Sztuczna inteligencja już nas wyprzedziła w rozpoznawaniu twarzy, potrafi zarejestrować i zinterpretować ponad 20 ekspresji i mikroekspresji – podstawowe emocje obecne we wszystkich rasach i kulturach (radość, smutek, wstręt, strach, zaskoczenie i złość, w rozszerzonej wersji jeszcze: dumę, wstyd, zażenowanie i podniecenie) i wiele emocji drugiego rzędu. Psychologia ewolucyjna twierdzi, że do rozwoju inteligencji w dużym stopniu przyczyniło się kłamanie, kłamstwo bowiem wymaga jej o wiele więcej niż mówienie prawdy.

Trzeci mózg, czy ścisłej trzeci jego sektor, najmłodszy i najcieńszy to złożona z sześciu warstw kora nowa zwana neokorteksem (25-30% całej puli neuronalnej). To ona decyduje o tym, że wznieśliśmy się na wyżyny *homo sapiensa* (który jednak dziś z różnych przyczyn jest homo ledwo sapiens). W niej lokują się pokłady najbardziej zaawansowanej inteligencji. To ta kora mózgowa odpowiedzialna jest za rozumowanie, planowanie przyszłości i za wszystkie czynności związane z myśleniem. Dzięki niej odczuwamy akceptację przez innych i tworzymy z nimi relacje. Płat czołowy jest odpowiedzialny za pomysły, koncepcje, decyzje, myślenie abstrakcyjne i procesy językowe. Sieci neuronowe w tej korze to jeden wielki model językowy przewyższający – nie wiadomo jak długo – generatywne transformery - modele językowe jak chat GPT kreowane przez sztuczne sieci neuronowe.

Jest paradoksem, że sztuczna inteligencja imituje najłatwiej procesy zachodzące w korze nowej, a nie w mózgu gadzim czy ssaczym. Wyjaśnia to Paradoks Moraveca, amerykańskiego informatyka czeskiego pochodzenia. Zdaniem Hansa Moraveca wbrew tradycyjnym przeświadczeniom, wysokopoziomowe rozumowanie wymaga niewielkiej mocy obliczeniowej, natomiast niskopoziomowa percepcja i zdolności motoryczne wymagają olbrzymiej mocy obliczeniowej. Rozwój neokorteksu odpowiedzialnego za intelekt, myślenie logiczno-matematyczno-analityczne jest relatywnie świeżej daty w porównaniu do trwającej setki milionów lat ewolucji motoryki ciała, aparatu

percepcyjnego i układu limbicznego wyższych organizmów żywych, w tym człowieka w różnych jego fazach ewolucyjnych. Dlatego o wiele łatwiej wygenerować chatbota niż skonstruować robota, który by imitował zdolności ruchowe człowieka, jak tańczenie czy choćby wchodzenie na schody. Upraszczając: ewolucja, jeśli chodzi intelekt, niezbyt się napracowała. Powstał zachwycający pod względem AI GPT4, ale nadal nie mamy sprawnego robotycznego hydraulika. Mamy więc wyjaśnienie, dlaczego dokonuje się tak szaleńczy postęp w kreowaniu systemów sztucznej inteligencji w porównaniu do fizycznych robotów.

Do czasu upowszechnienia się chata GPT i systemów AI, m.in. generatora obrazów Dal-E2 czy Midjourney i wielu innych byliśmy święcie przekonani, że inteligencja maszynowa może nas zastąpić we wszystkim, ale nie w kreatywności. Zawody twórcze zawsze będą się mieć dobrze. Znikną zawody bazujące na powtarzalności, rutynie itp. Owszem wiele z nich znika, ale zagrożone są także zajęcia twórcze. Na ulice nie wychodzą protestować hydraulicy, masażyści, piekarze czy fryzjerzy a autorzy scenariuszy filmowych, jak to miało miejsce w Stanach Zjednoczonych. Myślę, że w kolejce do protestów ustawią się niedługo graficy, informatycy, programiści, kompozytorzy i inni „kreatywni".

Na koniec tego wątku taka oto metarefleksja.

Obserwując ekspansję AI można odnieść wrażenie, że jakby kierowała się ona maksymą „czyń sobie człowieka poddanym". Sztuczna inteligencja wieńczy, a posthumaniści, twierdzą, że kończy rozwój ludzki, być może jest ostatnim wynalazkiem człowieka, wszystkie następne będą już jej dziełem. Stosunek ludzi do sztucznej inteligencji pokazuje pewną prawdę o człowieku: kiedy czegoś nie rozumiemy traktujemy to jak coś magicznego, mistycznego, uwznioślamy, sublimujemy, Mamy tu do czynienia z jakimś cyklem: przed epoką Oświecenia ludzie czuli się we władzy sił nadprzyrodzonych. Oświecenie dało im poczucie władzy nad przyrodą, wiarę w rozum a władzę na tym padole sami sobie wybierali i na nią zrzucali odium za nieudolność. W wieku AI, której nie rozumiemy, mamy doń nabożny stosunek i skłonni jesteśmy ją traktować jako nowe bóstwo i godzić się na kontrolę nad nami. Słowem, tak jak przed wiekami ludzie nie mieli poczucia władzy nad przyrodą, dziś nie maja poczucia władzy nad technologią. Można

jednak mieć nadzieję, że w miarę upowszechnienia wynalazek ten spowszednieje, ulegnie banalizacji nie będziemy się zastanawiać, jaki „diabeł w nim siedzi".

Zakończenie

Nauki o człowieku stoją w obliczu teoretycznego przetworzenia kilku ważkich problemów oscylujących wokół relacji sztuczna inteligencja – człowiek, a w istocie stworzenia nowego paradygmatu. Im bardziej technologia przyspiesza, tym mniej jesteśmy pewni co do tego, kim jesteśmy zarówno jako gatunek jak i indywidua. Coraz mniej wiemy, co to znaczy być człowiekiem. Niemal codziennie nowe odkrycia i wynalazki zmuszają nas do bolesnego przewartościowywania fundamentalnych aspektów naszej egzystencji. To powoduje bóle adaptacji. Rodzi się coś nowego, co się samonapędza, przekroczyliśmy jako ludzkość granicę, kiedy już nie ma powrotu do przeszłości, w której wszystko było znane. Nie mamy dokąd wracać, ciągle jednak nie mamy także dobrego pomysłu na przyszłość, a nawet na współczesność.

Nowe światy tworzą nowych ludzi, pisze David Weinberger w książce *Small Pieces Loosely Joined* (2003). Zdaniem autora nie jesteśmy w stanie zdefiniować siebie bez nakreślenia obrazu naszego świata, a zarazem nie możemy opisać naszego świata bez opisania, kim jesteśmy jako ludzie. Kiedy pojawia się nowa rzeczywistość, kiedy wkraczamy do nowego świata, to stajemy się nowymi ludźmi. Nowi ludzie w nowym świecie nie bardzo wiedzą, jak się w nim poruszać, a nie mogą się dowiedzieć od starszych pokoleń, ponieważ one zostały ukształtowane przed epoką cyfrową.

Bibliografia

J. Baudrillard, *Przed końcem*, Rozmawia Phillipe Petit, Warszawa, 2001 Sic!
V. Flusser, *Into the Universe of Technical Images,* Minneapolis-London: University of Minnesota press, 2011
D. Ihde, *Postphenomenology and Technoscience*, The Peking University Lectures, Albany, SUNY Press, 2009
H. Innis, *The Bias of Communication,* University of Toronto Press, Toronto, 1951
D. Weinberger, *Small Pieces Loosely Joined,* Basic Books, New York, 2003
H. Moravec, *Moravec's Paradox: When Robots Struggle with Simple Tasks*, MIT Technology Review, Cammbrige, MA, 1978

„dot.pl" - czasopismo Rejestru domeny .pl

Konteneryzacja - nowoczesna metoda utrzymywania usług

Mateusz Kozłowski
ORCID: https://orcid.org/0009-0005-6899-0244
E-mail: kontakt@matkoz2.dev

Received: 05.05.2024
Accepted: 25.05.2024
Published: 27.05.2024

Cite this article as:
M. Kozłowski, „Konteneryzacja - nowoczesna metoda utrzymywania usług"

DOT.PL, no. 1/ 2024,
10.60097/DOTPL/189321

Corresponding author:
Mateusz Kozłowski
E-mail: kontakt@matkoz2.dev

Streszczenie

Technologia konteneryzacji staje się coraz popularniejsza. Ewolucja na przestrzeni lat, wpłynęła na dojrzałość oraz łatwość korzystania z rozwiązania. Wzrost zainteresowania konteneryzacją spowodował, że narzędzie to staje się standardem na rynku. Artykuł ma na celu przybliżyć historię konteneryzacji oraz zaprezentować najważniejsze cechy, które wpłynęły na jej popularność.

Omówione zostaną również korzyści, które płyną z wykorzystania technologii konteneryzacji w dziedzinach tj. wytwarzanie oprogramowania oraz utrzymywanie aplikacji.

Słowa kluczowe: kontenery, docker, podman, bezpieczeństwo, izolacja, administracja aplikacjami

Abstract

Containerization technology is becoming increasingly popular. Evolving over the years, it has influenced the maturity and ease of use of the solution. The increased

interest in containerization has made this tool a standard on the market. This article aims to provide an overview of the history of containerization and present the key features that have influenced its popularity. It also discusses the benefits of using containerization technology in areas such as software development and application maintenance.

Keywords: containers, docker, podman, security, isolation, applications maintenance

Nazwy takie jak „Docker", „Podman" czy „Kubernetes", na przestrzeni ostatnich lat stały się coraz bardziej popularne. Wzrost zainteresowania konteneryzacją zawdzięczamy korzyściom, jakie za sobą niesie. Są to m.in. wygoda, łatwość korzystania, przyśpieszanie procesu wytwarzania oprogramowania oraz szeroka dostępność na główne systemy operacyjne, tj. Linux, MacOS lub Windows. Coraz więcej dostawców oprogramowania decyduje się na dostarczanie swojej aplikacji w kontenerze lub przynajmniej zapewnia taką opcję jako alternatywną do standardowego wdrożenia.

Sama idea konteneryzacji nie jest nowa. Pierwszym rozwiązaniem, które stało się podstawą do aktualnie znanych nam technologii, jest narzędzie *chroot*[335]. Zostało ono wprowadzone do systemu operacyjnego UNIX w 1979 roku. Narzędzie to pozwala na uruchomienie aplikacji w określonym katalogu, który z jej perspektywy staje się dla niej katalogiem głównym (z ang. *rootem - "/"*). Każdy kolejny proces potomny uruchomiony w ramach aplikacji, również zostaje uruchomiony ze zmienioną ścieżką główną. Korzystanie ze wspomnianego narzędzia wymaga od użytkownika dodatkowej wiedzy oraz doświadczenia. Przytoczona izolacja wymusza załączanie wszystkich zależności w katalogu docelowym, ponieważ uruchomiony proces nie ma dostępu do standardowych ścieżek w systemie operacyjnym hosta. Zazwyczaj sprowadza się to do konieczności odwzorowania struktury katalogów znajdujących się na hoście[336].

[335] Manual. Chroot-invocation, https://www.gnu.org/software/coreutils/manual/html_node/chroot-invocation.html dostęp: 20.05.2024.
[336] J. Bressers, *Is chroot a security feature?* https://www.rredhat.com/en/blog/chroot-security-feature, dostęp: 20.05.2024.

Kolejnym rozwiązaniem, będącym próbą stworzenia czegoś na wzór mechanizmu, który dziś znamy pod nazwą konteneryzacji, były *FreeBSD Jails*[337]. Narzędzie to zostało zaprezentowane w 2000 r. Był to mechanizm inspirowany ideą *chroot*, jednak autorzy postanowili pójść krok dalej i zaproponowali technologię, która nie ograniczała się jedynie do izolacji na poziomie plików, ale również przestrzeni użytkowników oraz sieci. Mechanizmy te gwarantowały separację pomiędzy aplikacjami uruchamianymi w ramach różnych *Jails*. Dzięki nowemu podejściu, a w zasadzie rozbudowie *chroot,* autorzy rozwiązania zaproponowali narzędzie pozwalające na bardziej szczegółową izolację oraz kontrolę aplikacji działającej w ramach środowiska *Jail*. Niestety rozwiązanie ograniczało się jedynie do systemu FreeBSD, przez co nie zdobyło tak dużej popularności, żeby stać się powszechnie wykorzystywanym[338].

Następnym etapem popularyzacji konteneryzacji było zaprezentowanie w 2004 r., przez ówczesną firmę *Sun Microsystems* (aktualnie *Oracle Corporation*), technologii *Solaris Containers*[339]. Co do zasady było to rozwiązanie, podobne do wcześniej wspomnianego *FreeBSD Jails,* przy czym zawierało kilka ulepszeń, tj. możliwość alokacji zdefiniowanej ilości zasobów. W tym przypadku rozwiązanie również było ekskluzywne dla systemu Solaris, przez co nie zdobyło aż tak dużej popularności, żeby stać się standardem.

Przełom nastąpił w 2006 roku, kiedy to firma Google zaprezentowała rozwiązanie *Process Containers*, które w roku 2007 zostało nazwane *Control Groups* (*cgroups*) i pod tą nazwą znane jest do dziś. Inżynierowie firmy Google pokazali światu mechanizm, który umożliwiał przydzielanie zasobów sprzętowych oraz nadawanie priorytetów procesom. Następnie w 2008 r. rozwiązanie to zostało włączone do jądra Linuxa, przez co zyskało na popularności i pozwoliło na utworzenie *Linux Containers* (LXC)[340].

Linux Containers jest pierwszym mechanizmem, który przypomina kontenery w dzisiejszym tego słowa znaczeniu. Technologia ta została stworzona przez firmę Canonical i stała się powszechna oraz włączona do wielu popularnych dystrybucji

---

[337] Free BSD Handbook, https://docs.freebsd.org/en/books/handbook/jails, dostęp: 20.05.2024.

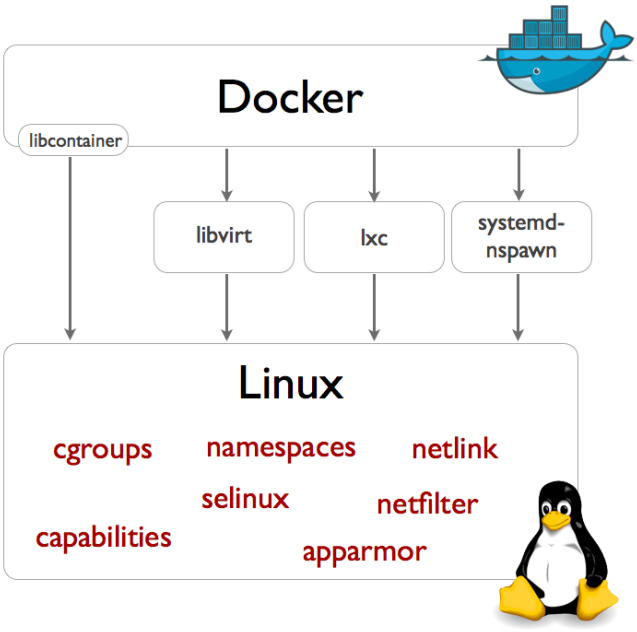
[338] K. Dabik, *Cyberprzestrzeń - zagrożenia i wyzwania*, [w:] M. Karpiuk (red.), *Cyberbezpieczeństwo – aspekty krajowe i międzynarodowe*, Warszawa 2024, s. 9 i n.

[339] Solaris containers, https://www.oracle.com/solaris/technologies/solaris-containers.html, dostęp: 20.05.2024.

[340] History containers, https://www.redhat.com/en/blog/history-containers, dostęp: 20.05.2024.

systemu Linux[341]. Technologia LXC realizowała to zadanie poprzez uruchomienie wielu procesów, które z perspektywy aplikacji działającej w środku, symulowały całkowicie niezależny od hosta system operacyjny. Z tego też względu rozwiązanie to jest określane mianem „lekkich maszyn wirtualnych”[342]. Kontenery LXC były mechanizmem stosunkowo zaawansowanym, przez co wymagały wiedzy od użytkownika. Fakt ten spowodował, że konteneryzacja LXC zyskała na popularności, ale tylko w kręgach osób zaznajomionych oraz doświadczonych w pracy z systemem Linux[343].

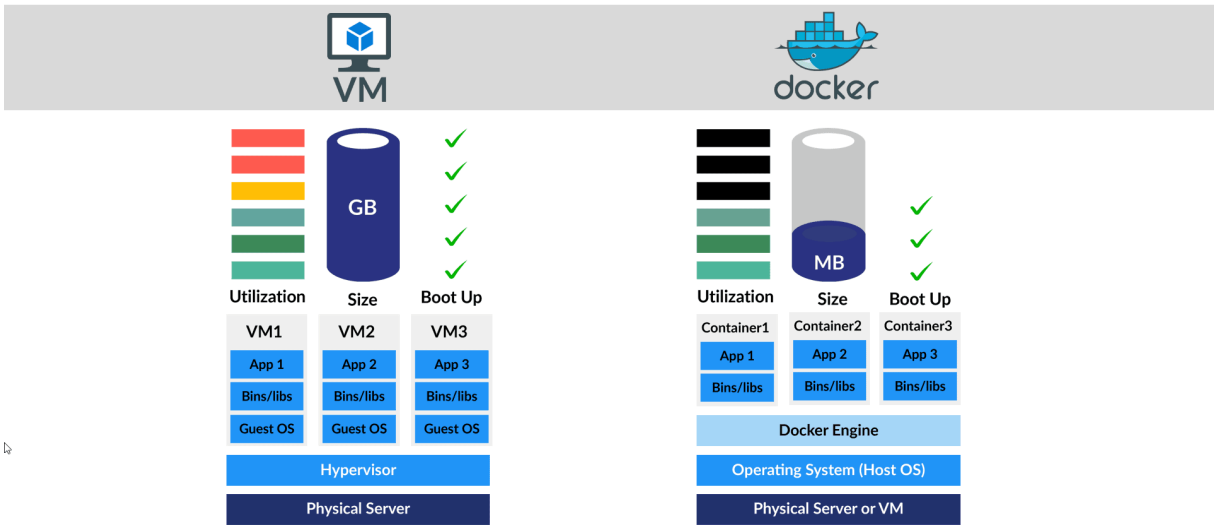
Po kolejnych kilku latach, w 2013 roku, podczas krótkiego wystąpienia w trakcie konferencji *PyCon,* Solomon Hykes przedstawia światu rozwiązanie Docker[344]. Technologia ta pierwotnie bazowała na LXC, jednak autorzy postanowili wprowadzić własną implementację w 2014 r. pod nazwą *libcontainer*[345], która dawała im większą kontrolę nad projektem.



[341] D. Naprawa, *Docker vs LXC – czym to się różni?* https://szkoladockera.pl/czym-rozni-sie-docker-od-lxc, dostęp: 20.05.2024.
[342] Ibidem.
[343] R. Weber, *Legal safeguard for cloud computing*, [in:] A. Cheung, R. Weber (eds), *Privacy and Legal Issues in Cloud Computing*, Massachusetts 2016, s. 43 i n.
[344] The future of Linux Containers, https://www.youtube.com/watch?v=wW9CAH9nSLs, dostęp: 20.05.2024.
[345] Docker Desktop 0.9: Introducing Execution Drivers and libcontainer, https://www.docker.com/blog/docker-0-9-introducing-execution-drivers-and-libcontainer, dostęp: 20.05.2024.

Rysunek 1: *Schemat przedstawiający komunikację rozwiązania Docker z komponentami systemu, źródło: https://www.docker.com/blog/docker-0-9-introducing-execution-drivers-and-libcontainer (dostęp: 20.05.2024)*

Ogromną zaletą rozwiązania Docker była łatwość jego użytkowania. Postawiono na prostotę, która w poprzednich implementacjach konteneryzacji, tj. FreeBSD Jails lub LXC, nie była oczywista. Dzięki Dockerowi, uruchomienie kontenera sprowadzało się do wydania prostego polecenia w linii komend ***docker run NAZWA_OBRAZU KOMENDA***. Obrazami w tym przypadku są wcześniej przygotowane pliki, które zawierają w sobie docelową funkcjonalność.
To właśnie obraz uruchamiany jest w ramach konteneryzacji, co może w pewnym sensie kojarzyć się z pojęciem wirtualizacji. W przypadku kontenerów należy jednak pamiętać, że nie występuje emulacja jak przy standardowej wirtualizacji. Dostęp do zasób systemowych hosta jest izolowany przy pomocy specjalnych mechanizmów[346].



Rysunek 2: *Różnica pomiędzy wirtualizacją, a konteneryzacją. Źródło: https://k21academy.com/docker-kubernetes/docker-vs-virtual-machine/ (dostęp: 20.05.2024)*

Konteneryzacja z wykorzystaniem narzędzia Docker wymusza, choć są od tego odstępstwa, stosowanie zasady *Single Concern Principle*, która zmienia dotychczasowe

[346] D. Naprawa, *Historia konteneryzacji – czy było coś wcześniej przed Dockerem?*, https://www.youtube.com/watch?v=FAIZPF3Q80k, dostęp: 20.05.2024.

podejście do konteneryzacji w rozumieniu LXC. Jak wcześniej wspomniano, w ramach Linux Containers uruchomiano wiele procesów, celem zasymulowania całego systemu operacyjnego. Z kolei w Docker aplikacje powinny być rozbijane na poszczególne funkcjonalności tak, żeby jeden kontener odpowiadał jednemu procesowi lub inaczej mówiąc, był odpowiedzialny tylko za konkretną funkcjonalność. Zasada znacząco porządkuje oraz ułatwia zarządzanie aplikacją, a w szczególności jej zasobami, uprawnieniami oraz bezpieczeństwem. Podejście to ułatwia również proces aktualizacji, który ogranicza się jedynie do komponentu, który tego wymaga.

Kolejnym założeniem, na którym opiera się konteneryzacja w rozumieniu tego, co znamy pod nazwą Docker, to tworzenie aplikacji w taki sposób, żeby wszystkie zależności były zawarte w obrazie przygotowanym do uruchomienia. Ma to na celu uniknięcie problemu, który występował w przypadku korzystania z *chroot*. Wykorzystanie tego rozwiązania wymagało od użytkownika linkowania lub kopiowania zależności docelowego katalogu startowego.

Nowoczesne zasady konteneryzacji wymagają od twórców przestrzegania reguły niezmienności zawartości kontenera. Reguła ta polega na tym, że wszystkie dane, które powinny zostać zapisane, należy wynosić poza kontener, wykorzystując tzw. Volume[347]. Mechanizm należy traktować jako nieulotną przestrzeń dyskową, która gwarantuje nam, że najważniejsze dane nie zostaną utracone w przypadku usunięcie kontenera[348].

Stosując powyższe zasady (choć nie są to jedyne zasady dotyczące konteneryzacji), zarządzanie aplikacjami staje się wygodne oraz uporządkowane. Powyższe możliwości wynikające z wykorzystania konteneryzacji są jedynie częścią korzyści, które wpłynęły na sukces narzędzia. Wykorzystanie tej technologii pozwoliło również ujednolicić proces uruchamiania aplikacji poprzez rozwiązanie problemu ze zgodnością wersji oprogramowania zainstalowanego na systemie operacyjnym hosta.

Kolejnym ułatwieniem, które miało ogromny wpływ na popularność rozwiązania, było narzędzie Docker Desktop, które pozwalało zarządzać kontenerami z wykorzystaniem interfejsu graficznego. Rozwiązanie Docker jest dostępne na wszystkie kluczowe systemy

[347] Volumes, https://docs.docker.com/storage/volumes, dostęp: 20.05.2024.
[348] B. Ibryam, *Principles of container-based application design*, https://kubernetes.io/blog/2018/03/principles-of-container-app-design/, dostęp: 20.05.2024.

operacyjne tj. Linux, MacOS oraz Windows. Wszystko to powoduje, że uruchomienie oraz korzystanie z narzędzia nie wymaga specjalistycznej wiedzy.

Należy również pamiętać, że sam Docker to nie tylko narzędzie do zarządzania kontenerami. Firma uruchomiła wiele interesujących produktów, które przyciągają coraz to większe zainteresowanie, a są to m.in.:

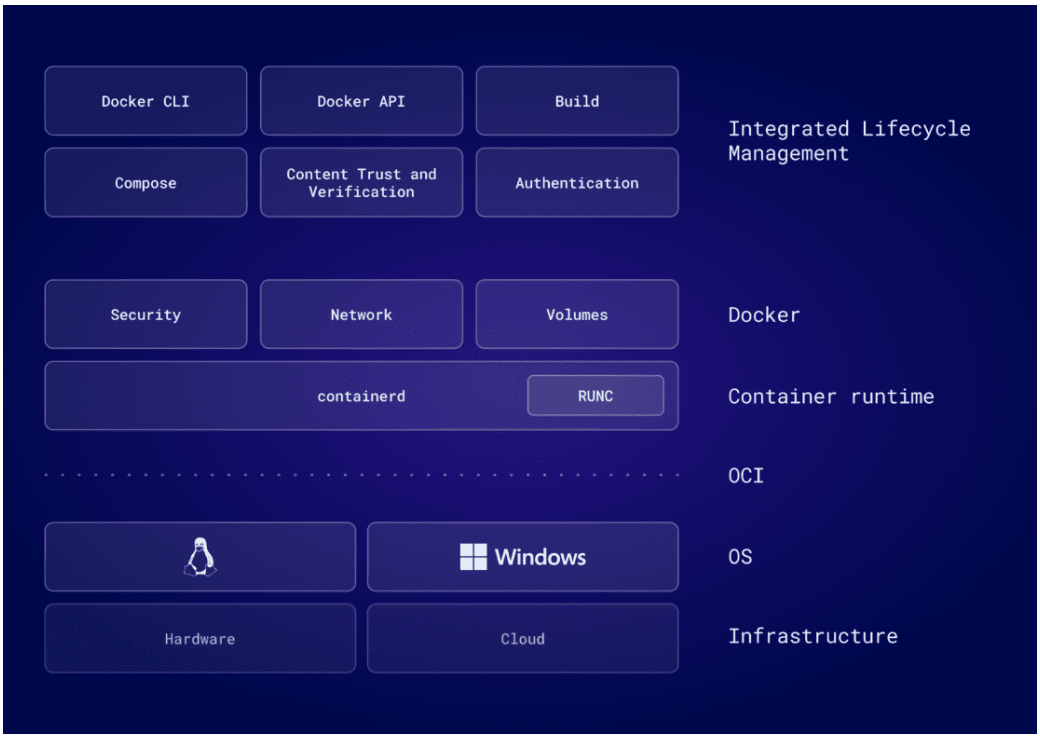
- Docker Hub[349] - centralny punkt dystrybucji obrazów, który umożliwia twórcom publikowanie swoich aplikacji
- Docker Scout[350] - skaner podatności w obrazach kontenerów;
- Docker Compose[351] - narzędzie pozwalające na zdefiniowanie aplikacji zawierającej w sobie wiele powiązanych ze sobą kontenerów, które opisane są z wykorzystaniem dedykowanej składni w pliku YAML.

Konteneryzacja znacząco wpłynęła na podejście do procesu wytwarzania oraz utrzymywania aplikacji. Wiele firm posiadających w swoich strukturach programistów, testerów oraz administratorów, zaobserwowało w tej technologii możliwość optymalizacji czasu, który był zajmowany przez liczne procedury, takie jak: testowanie oprogramowania oraz jego wdrażanie. W ten sposób, w kontekście konteneryzacji, zaczęto kierować się zasadą *Site Reliability Engineering*, która zakładała łączenie funkcji dotychczas traktowanych jako oddzielne, w obowiązkach należących do jednej osoby. Konteneryzacja sprawdziła się świetnie jako element uzupełniający to zadanie. Technologia pozwoliła rozszerzyć dotychczasową odpowiedzialność programisty o dodatkowe elementy tj. uruchomienie aplikacji i ewentualną obsługę błędów. Było to realne dzięki możliwościom oferowanym przez kontenery, a w szczególności przez fakt, że kontener funkcjonuje identycznie na dowolnym obsługiwanym hoście. Podejście to stanowczo skróciło proces obsługi i naprawy błędów, poprzez przybliżenie osób odpowiedzialnych za tworzenie kodu do jego obsługi w systemach docelowych.

Wraz ze wzrostem pojęcia konteneryzacji, rozpoczęto prace nad kolejnymi standardami, które miały na celu przyśpieszenie dotychczas stosowanych procesów. W ten sposób na rynku pojawiło się pojęcie *Cloud Native*, które miało na celu uporządkowanie kwestii

[349] Docker Hub, https://docs.docker.com/docker-hub, dostęp: 20.05.2024.
[350] Docker Scout, https://docs.docker.com/scout, dostęp: 20.05.2024.
[351] Docker Compose, https://docs.docker.com/compose, dostęp: 20.05.2024.

związanych z wytwarzaniem oraz utrzymywaniem aplikacji. Ważnym elementem składającym się na ww. zagadnienie było uniezależnienie się od konkretnego dostawcy usług. Wiele firm było przywiązane do konkretnego operatora, przez co migracja była czasochłonna lub wręcz niemożliwa. Z upływem czasu wymyślono podejście *Infrastructure as Code,* które zakładało, że cała infrastruktura aplikacji zostaje opisana w formie kodu. To z kolei miało zagwarantować brak przywiązania do konkretnego dostawcy, ponieważ co do zasady opis infrastruktury pozwala na jej automatyczne odtworzenie w identycznej formie u dowolnego operatora lub w modelu *on-premise*[352].



Rysunek 3: *Poglądowy rysunek zależności pomiędzy poszczególnymi komponentami składającymi się na uruchomienie kontenera. Źródło: https://www.docker.com/blog/containerd-vs-docker/ (dostęp: 20.05.2024)*

Popularyzacja technologii spowodowała również rozwój konkurencji w postaci rozwiązań alternatywnych tj. Podman, które aktualnie rozwijane jest przez firmę RedHat Inc. W przypadku tego narzędzia wprowadzono również kilka innych innowacji tj. konteneryzacja *rootless* oraz narzędzie *Podman Quadlet*. Wszystkie ww. narzędzia mają na celu

[352] *Infrastructure as Code (IaC)*. (2023, 11 30). Retrieved from https://glossary.cncf.io/infrastructure-as-code/, dostęp: 20.05.2024.

zwiększenie wygody użytkownika, zautomatyzowanie procesów oraz podniesienie bezpieczeństwa[353].

Kontenery rootless pozwoliły odejść od standardowego podejścia, które wymagało uruchomienia tzw. demona, który odpowiadał za zarządzeniem kontenerami. Zmiana ta znacznie wpłynęła na bezpieczeństwo konteneryzacji, ponieważ nie wymagała uruchamiania procesów z uprawnieniami administracyjnymi i w przypadku pojawienia się błędu umożliwiającego „wyjście" z kontenera, atakujący działał na uprawnieniach zwykłego użytkownika.

	Root Outside	**User Outside**

Root Inside	# whoami
	root
	
	# podman run -it ubi8 bash
	# whoami
	root
		$ whoami
		fatherlinux
		
		$ podman run -it ubi8 bash
		# whoami
		root

User Inside	# whoami
	root
	
	# podman run -itu sync ubi8 bash
	$ whoami
	sync
		$ whoami
		fatherlinux
		
		$ podman run -itu sync ubi8 bash
		$ whoami
		sync

Rysunek 4: *Porównanie uprawnień procesu kontenera w zależności od uprawnień, z jakimi został uruchomiony. Źródło: https://www.redhat.com/en/blog/understanding-root-inside-and-outside-container (dostęp: 20.05.2024)*

W skład narzędzia Podman wchodzi również komponent o nazwie *Quadlet*[354]. Rozwiązanie to ułatwia opisywanie kontenerów przy użyciu kodu. Mechanizm można porównać do rozwiązania Docker Compose, które pozwala opisywać wielokontenerowe aplikacje poprzez definiowanie ich w specjalnie przygotowanym pliku YAML. Wdrożenie tej funkcjonalności jest na potrzebę dostosowania się do zasady zawartej w Cloud Native, która zakłada, że uruchamiane aplikacje powinny być niezależne od dostawcy konkretnego usług cyfrowych i możliwe do bezproblemowej migracji. Poniżej znajduje się

[353] C. Banasiński, *Podstawowe pojęcia i podstawy prawne bezpieczeństwa w cyberprzes*trzeni, [w:] C. Banasiński (red.), *Cyberbezpieczeństwo*, Warszawa 2018, s. 27.

[354] Podman system, https://docs.podman.io/en/latest/markdown/podman-systemd.unit.5.html, dostęp: 20.05.2024.

przykład definicji prostego kontenera opisanego z wykorzystaniem rozwiązania Podman Quadlet.

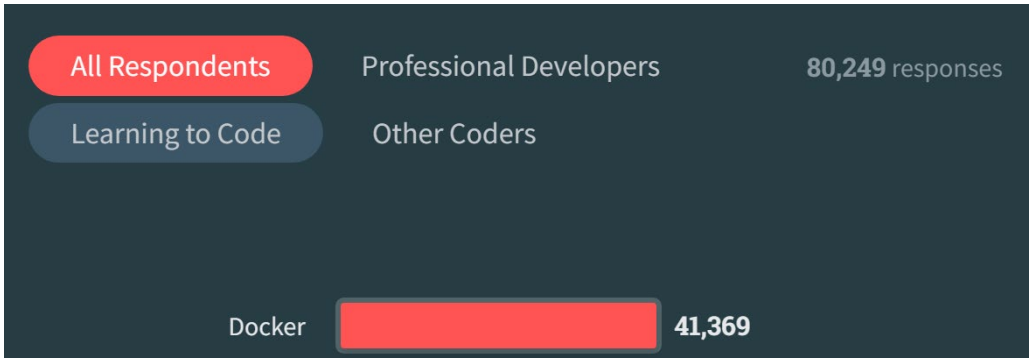
```
[Container]
ContainerName=busybox1
Image=docker.io/busybox
Exec=/bin/sh
```

Rysunek 5: *Definicja kontenera z wykorzystaniem Podman Quadlet, opracowanie własne.*

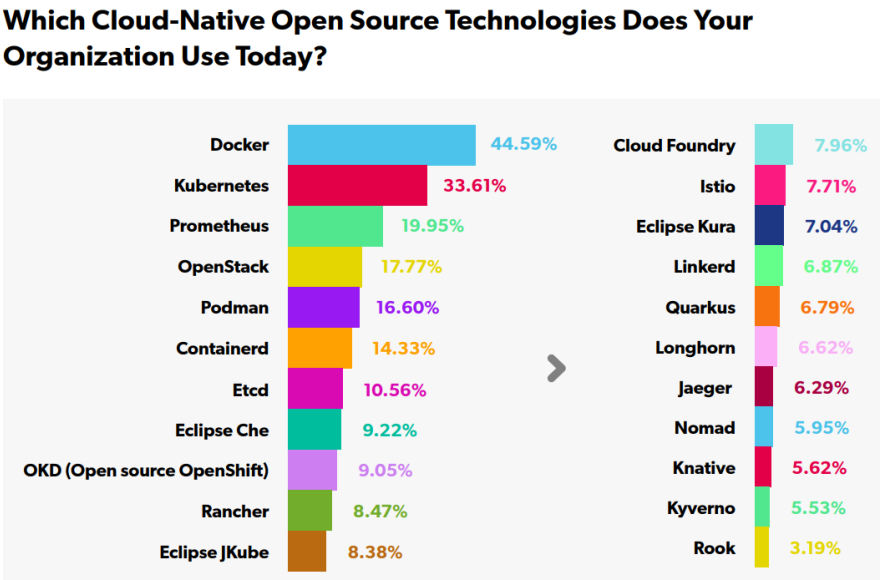
Dzięki zaangażowaniu dużych firm w technologię konteneryzacji, na rynku pojawiają się kolejne narzędzia ułatwiające pracę w tym środowisku. Giganci technologiczni sami wdrażają kontenery, w swoich strukturach. Są przez to zmotywowani do rozwijania narzędzi, które im to ułatwią. W ten sposób powstało wiele interesujących projektów, które zostały udostępnione bezpłatnie dla całej społeczności. Przykładowymi rozwiązaniami, które zostały stworzone przez duże przedsiębiorstwa i są stosowane przez użytkowników na skalę globalną są: Kubernetes[355], Google Distroless[356], OKD[357], Fedora CoreOS[358]. Wszystkie te narzędzia są rozwijane i mają na celu popularyzację technologii konteneryzacji.

Najnowsze badania pokazują, że technologia konteneryzacji jest aktualnie bardzo popularna. Została pozytywnie przyjęta przez osoby zajmujące się zagadnieniami z dziedziny informatyki. Zainteresowanie technologią sugeruje, że na przestrzeni kolejnych lat konteneryzacja stanie się standardem w procesie utrzymywania aplikacji. W przypadku przestrzegania dobrych praktyk związanych z tworzeniem kontenerów, użytkownicy powinni zaobserwować poprawę wydajności oprogramowania oraz zwiększyć wygodę jego utrzymywania. Trend ten powinien również przełożyć się na ogólną redukcję kosztów, jak i poprawę bezpieczeństwa uruchamianych aplikacji.

[355] Production-Grade Container Orchestration, https://kubernetes.io, dostęp: 20.05.2024.
[356] Google container tools, https://github.com/GoogleContainerTools/distroless, dostęp: 20.05.2024.
[357] The Community Distribution of Kubernetes that powers Red Hat OpenShift, https://www.okd.io, dostęp: 20.05.2024.
[358] Fedora CoreOS Documentation, https://docs.fedoraproject.org/en-US/fedora-coreos, dostęp: 20.05.2024.



Rysunek 6: *Wyniki ankiety przeprowadzonej przez firmę Stack Exchange Inc. wskazującej zainteresowanie technologią Docker w 2023 roku, źródło: https://survey.stackoverflow.co/2023/#section-most-popular-technologies-other-tools (dostęp: 20.05.2024)*



Rysunek 7: *Wyniki ankiety przeprowadzonej przez firmę Perforce Software, Inc. wskazującej zainteresowanie technologią Docker w 2023 roku. W ankiecie wzięło udział 2046 osób. źródło: https://www.openlogic.com/resources/state-of-open-source-report (dostęp: 20.05.2024)*

Konteneryzacja oraz technologie powstające wokół niej pozwalają uprościć oraz przyśpieszyć wiele procesów, które do tej pory były czasochłonne. Kontenery pozwalają ujednolicić pracę programistów poprzez zagwarantowanie spójności środowiska uruchomieniowego. Kolejny etap, który staje się łatwiejszy dzięki ww. technologii to testy aplikacji. Dzięki spójności środowiska, gotowa aplikacja może trafić do testera, który po prostu ją uruchomi bez konieczności rozwiązywania problemów z zależnościami.

Konteneryzacja pozwala również, ze względu na swoje założenia, przyśpieszyć proces wdrożenia aplikacji, który co do zasady sprowadza się do pobrania obrazu, przygotowania konfiguracji oraz uruchomienia aplikacji. Dodatkowo, warty uwagi jest fakt, że konteneryzacja zapewnia izolację aplikacji od hosta, co przekłada się na zwiększone bezpieczeństwo całego środowiska.

Konteneryzacja w każdym roku zyskuje na popularności i wydaje się, że trend ten będzie utrzymany. Jest to zjawisko pozytywne, ponieważ technologia ta rozwiązuje wiele problemów i wpływa korzystnie na wiele aspektów utrzymywania aplikacji, przez co stanowi świetną alternatywę dla standardowego podejścia wytwarzania oraz utrzymywania aplikacji, jakie było znane dotychczas.

Bibliografia

J. Bressers, *Is chroot a security feature?,* https://www.redhat.com/en/blog/chroot-security-feature, dostęp: 20.05.2024.

C. Banasiński, *Podstawowe pojęcia I podstawy prawne bezpieczeństwa w cyberprzestrzeni*, [w:] C. Banasiński (red.), *Cyberbezpieczeństwo*, Warszawa 2018.

K. Dabik, *Cyberprzestrzeń - zagrożenia i wyzwania*, [w:] M. Karpiuk (red.), *Cyberbezpieczeństwo – aspekty krajowe i międzynarodowe*, Warszawa 2024.

Docker Compose, https://docs.docker.com/compose, dostęp: 20.05.2024.

Docker Desktop 0.9: Introducing Execution Drivers and libcontainer, https://www.docker.com/blog/docker-0-9-introducing-execution-drivers-and-libcontainer, dostęp: 20.05.2024.

Docker Hub, https://docs.docker.com/docker-hub, dostęp: 20.05.2024.

Docker Scout, https://docs.docker.com/scout, dostęp: 20.05.2024.

Fedora CoreOS Documentation, https://docs.fedoraproject.org/en-US/fedora-coreos, dostęp: 20.05.2024.

Free BSD Handbook, https://docs.freebsd.org/en/books/handbook/jails, dostęp: 20.05.2024.

Google container tools, https://github.com/GoogleContainerTools/distroless, dostęp: 20.05.2024.

History containers, https://www.redhat.com/en/blog/history-containers, dostęp: 20.05.2024

B. Ibryam, *Principles of container-based application design*, https://kubernetes.io/blog/2018/03/principles-of-container-app-design/, dostęp: 20.05.2024.

Infrastructure as Code (IaC), https://glossary.cncf.io/infrastructure-as-code/, dostęp: 20.05.2024.

LXC containers. (n.d.), https://ubuntu.com/server/docs/lxc-containers, dostęp: 20.05.2024.

Manual. Chroot-invocation, https://www.gnu.org/software/coreutils/manual/html_node/chroot-invocation.html dostęp: 20.05.2024.

D. Naprawa, *Docker vs LXC – czym to się różni?*, https://szkoladockera.pl/czym-rozni-sie-docker-od-lxc, dostęp: 20.05.2024.

D. Naprawa, *Historia konteneryzacji – czy było coś wcześniej przed Dockerem*, https://www.youtube.com/watch?v=FAIZPF3Q80k, dostęp: 20.05.2024.

Podman system, https://docs.podman.io/en/latest/markdown/podman-systemd.unit.5.html, dostęp: 20.05.2024.

Production-Grade Container Orchestration, https://kubernetes.io, dostęp: 20.05.2024.

Solaris containers, https://www.oracle.com/solaris/technologies/solaris-containers.html, dostęp: 20.05.2024.

The Community Distribution of Kubernetes that powers Red Hat OpenShift, https://www.okd.io, dostęp: 20.05.2024.
The future of Linux Containers, https://www.youtube.com/watch?v=wW9CAH9nSLs, dostęp: 20.05.2024.
R. Weber, *Legal safeguard for cloud computing*, [in:] A. Cheung, R. Weber (eds.), *Privacy and Legal Issues in Cloud Computing*, Massachusetts 2016.
Volumes, https://docs.docker.com/storage/volumes, dostęp: 20.05.2024.

Wykaz rysunków

Rysunek 1: Schemat przedstawiający komunikację rozwiązania Docker z komponentami systemu, źródło: https://www.docker.com/blog/docker-0-9-introducing-execution-drivers-and-libcontaine, dostęp: 20.05.2024.

Rysunek 2: Różnica pomiędzy wirtualizacją, a konteneryzacją. Źródło: https://k21academy.com/docker-kubernetes/docker-vs-virtual-machine, dostęp: 20.05.2024.

Rysunek 3: Poglądowy rysunek zależności pomiędzy poszczególnymi komponentami składającymi się na uruchomienie kontenera. Źródło: https://www.docker.com/blog/containerd-vs-docker, dostęp: 20.05.2024.

Rysunek 4: Porównanie uprawnień procesu kontenera w zależności od uprawnień, z jakimi został uruchomiony. Źródło: https://www.redhat.com/en/blog/understanding-root-inside-and-outside-container, dostęp: 20.05.2024.

Rysunek 5: Definicja kontenera z wykorzystaniem Podman Quadlet, opracowanie własne.

Rysunek 6: Wyniki ankiety przeprowadzonej przez firmę Stack Exchange Inc. wskazującej zainteresowanie technologią Docker w 2023 roku, źródło: https://survey.stackoverflow.co/2023/#section-most-popular-technologies-other-tools, dostęp: 20.05.2024.

Rysunek 7: Wyniki ankiety przeprowadzonej przez firmę Perforce Software, Inc. wskazującej zainteresowanie technologią Docker w 2023 roku. W ankiecie wzięło udział 2046 osób. źródło: https://www.openlogic.com/resources/state-of-open-source-report, dostęp: 20.05.2024.

Sprawozdanie z corocznego spotkania Partnerów Rejestru domeny .pl

NASK nagrodził najlepsze firmy działające na rynku domen

- Nikt tak dobrze nie obsługuje klientów końcowych jak Partnerzy. Stworzony w NASK Program Partnerski się sprawdza i tak już zostanie – powiedział Radosław Nielek, dyrektor NASK, otwierając tegoroczne spotkanie Rejestru domeny .pl z Partnerami, które odbyło się 27 maja 2024 w Jachrance.

Dyrektor Nielek w swoim wystąpieniu podkreślał, jak ważne jest bezpieczeństwo domeny .pl w dobie rosnącej liczby ataków i większego zagrożenia dla użytkowników sieci. Poinformował o pakiecie działań NASK, zmierzających do zapewnienia bezpiecznego środowiska cyfrowego, w ramach projektu bezpieczna domena .pl – Zmiany są nieuniknionym procesem, bo przed nami nowy obszar regulacji prawnych związanych m.in. z NIS 2, które obejmą zarówno Rejestr domeny. pl, jak i Partnerów NASK. Jesteśmy otwarci na dialog, tak by nowe zasady współpracy były satysfakcjonujące dla wszystkich – mówił Radosław Nielek. Jednocześnie dyrektor wręczył coroczne nagrody związane z działalnością na rynku domen.

Wyróżnienia dla liderów Rynku domeny .pl w 2023 r.:

Kategorie wyróżnień:

• Procentowy udział w obsłudze nazw domeny .pl w 2023 r.

• Procentowy udział w rejestracjach nazw domeny .pl w 2023 r.

• Procentowy udział w obsłudze nazw domeny .pl zabezpieczonych DNSSEC w 2023 r.

• Wolumen odnowień – wzrost rok do roku (2023 vs 2022).

• Wolumen rejestracji – wzrost rok do roku (2023 vs 2022).

I miejsce w poszczególnych kategoriach:

• Procentowy udział w obsłudze nazw domeny .pl w 2023 r.

OVH SAS, Francja

• Procentowy udział w rejestracjach nazw domeny .pl w 2023 r.

Aftermarket.pl Limited, Cypr

• Procentowy udział w obsłudze nazw domeny .pl zabezpieczonych DNSSEC w 2023 r.

nazwa.pl sp. z o.o., Polska

• Wolumen odnowień – wzrost rok do roku (2023 vs 2022).

PERSKIMEDIA Szymon Perski, Polska

• Wolumen rejestracji – wzrost rok do roku (2023 vs 2022).

Hosting Concepts B.V., Holandia

– W imieniu całego zespołu OVHcloud serdecznie dziękujemy za zaproszenie i za organizację warsztatów. Wspaniałe położenie oraz perfekcyjna organizacja przyczyniły się do sukcesu tego wydarzenia, a nasza firma znalazła się w gronie nagrodzonych Partnerów – za co serdecznie dziękujemy! Z niecierpliwością czekamy na kolejne spotkania z Rejestrem Domeny .pl – powiedziała Małgorzata Kielar, Registry Liaison Manager w OVHcloud.

II miejsce w poszczególnych kategoriach (dyplomy):

• Procentowy udział w obsłudze nazw domeny .pl w 2023 r.

Aftermarket.pl Limited, Cypr

• Procentowy udział w rejestracjach nazw domeny .pl w 2023 r.

Home.pl S.A., Polska

• Procentowy udział w obsłudze nazw domeny .pl zabezpieczonych DNSSEC w 2023 r.

Aftermarket.pl Limited, Cypr

• Wolumen odnowień – wzrost rok do roku (2023 vs 2022).

LH.pl Sp. z o.o., Polska

• Wolumen rejestracji – wzrost rok do roku (2023 vs 2022).

LH.pl Sp. z o.o., Polska

III miejsce w poszczególnych kategoriach (dyplomy):

• Procentowy udział w obsłudze nazw domeny .pl w 2023 r.

Home.pl S.A., Polska

• Procentowy udział w rejestracjach nazw domeny .pl w 2023 r.

OVH SAS, Francja

• Procentowy udział w obsłudze nazw domeny .pl zabezpieczonych DNSSEC w 2023 r.

OVH SAS, Francja

• Wolumen odnowień – wzrost rok do roku (2023 vs 2022).

Metaregistrar B.V., Holandia

• Wolumen rejestracji – wzrost rok do roku (2023 vs 2022).

OVH SAS, Francja

Katarzyna Chałubińska-Jentkiewicz dyrektorka ds. Rejestru Domen Internetowych NASK podsumowała 2023 rok, podkreślając, że liczby są niezwykle ważne, bo pokazują, jak rynek się rozwija.
– Lubimy analizować dane, ale też skupiamy się na planach, bo przed nami czas zmian. Zmienia się internet, zmienia się świat. Każdy z nas funkcjonuje w świecie cyfrowym i naszym zadaniem jako Rejestru jest, aby rynek jeszcze lepiej się rozwijał i aby środowisko, w jakim funkcjonuje domena .pl, było jak najbardziej bezpieczne – dodała Katarzyna Chałubińska-Jentkiewicz.

Pierwszy dzień konferencji z partnerami NASK to także premiera numeru specjalnego czasopisma dot.pl, w którym znalazło się podsumowanie minionego roku rynku nazw domeny .pl oraz przeprowadzone po raz pierwszy badanie: „Internet oczami ekspertów z branży DNS".
Podczas konferencji Katarzyna Chałubińska-Jentkiewicz ogłosiła uruchomienie strony nowego czasopisma naukowego NASK, dostępnej pod adresem journaldot.pl.

Monika Balcerzak
Komunikacja i marketing