Strategic and Political Responsibility in the Domain of Cybersecurity - Problems and Challenges

ANNA MAKUCH

Abstract Strategic and political responsibility which, based on the knowledge of the specific character of cyberspace, allows for a conscious and meaningful use of internet resources, is considered a key factor in eliminating threats to the digital data exchange environment. As contemporary infosphere promotes intuitive patterns of navigating and using open resources, it seems imperative to promote the principles of responsibility by popularising cyber hygiene and information ecology, which contribute to both the safety of users and system security within the national dimension of cyberspace.

Keywords: • responsibility • political system • security in cyberspace • information security

CORRESPONDENCE ADDRESS: Anna Makuch, Ph.D., Researcher-academic, University of Economics and Human Sciences in Warsaw, Faculty of Political Science, Department of Social Sciences, Ul. Okopowa 59, 01-043 Warsaw, Poland, e-mail: a.makuch@vizja.pl, ORCID: 0000-0002-5222-4407.

https://doi.org/10.4335/2022.2.5 ISBN 978-961-7124-11-8 (PDF)
Available online at http://www.lex-localis.press.

Not all soldiers are warriors and not all warriors are soldiers.
J.J. Patrick, 2018, the Art of Hybrid War.

1 Introduction

Attention is mainly focused on identifying the key challenges related to the strategic and political responsibility in the domain of cybersecurity (Pawłowski, Zdrodowski, Kuliczkowski, 2020: 38).

Such formulation of the topic suggests, firstly, that the concept of responsibility under analysis is important enough to make an effort to sort out the research issues; secondly, that attention will be focused on the specific character of responsibility in the digital space, taking into account both the architecture and infrastructure of this domain (Chałubińska-Jentkiewicz, 2019); and thirdly, that the dimension of responsibility has been undergoing transformation in the age of digitisation – just as digitisation has influenced the fundamental transformation of social, political, economic and cultural arrangements. This influence has manifested itself in a trend, visible for more than two decades, of shifting activities into digital space where information has become a more important commodity than tangible products (Castells, 2013: 25, Sartori, 2007).

The network of digital connections, being rhizomatic or nomadic according to Deleuze and Guattari (Deluze, Guattari, 1980), constitutes a "central nervous system" of the globalised information environment, in relation to which traditional forms of communication (paper press, radio news, television) appear to be secondary and retarded. The revolutionary dimension of this new intangible domain has not been limited to the function of storage in the created space, but has additionally resulted in a series of transformations in each area of human activity – in the field of media systems with new forms, i.e., hybridity and live participation in programmes, and in the field of social communication, e.g., social media.

The strategic and political perspective implies that the analysis of responsibility, in terms of the geography of digital space, exhibits two dimensions. The first dimension concerns the national system (Pawłowski, Zdrodowski, Kuliczkowski, 2020: 212) while the second one pertains to the level of international relations, encompassing interactions, decisions, and their social and political consequences affecting their participants. In the international dimension, the outcome of activities carried out by entities corresponds to the real effect induced by favourable decisions that match actual interests. At present, due to significant transformations of the public domain, the national dimension continues to gain importance. The outreach and use of cyberspace by individual users forms one of the factors influencing transformation in this domain – the launching of digital communication platforms has triggered a phenomenon of public diplomacy involving content resonance from each participant in the content exchange process. Modern techniques of information management enable individual users to build a platform of

influence covering a national or global system. It is not without essence that the objectives and motives of actions are authentic, as they are revealed in the course of activities and may expose manipulative or socially-harmful intentions.

Referring to the Congress of Vienna, during which a new balance of power was created through negotiations between a small circle of the political elite, the difference stems from the incomparably greater influence of individuals in the processes of interest aggregation, shaping public opinions through the exchange of messages, or influencing public views, especially if an organised destabilising activity is identified (Volkoff, 1991: 8). Therefore, as regards the national system security, individual users' activities should now be the focus of attention of dedicated services, given their potentially wide ranging influence.

The combination of the political aspect with the strategic aspect seemingly only simplifies the taxonomy – on the one hand, it prescribes certain activities within the national system and, on the other hand, through the very structure of the internet, it triggers the need to take into account the global system, with which it forms the nomadic and deterritorialised network referred to by Deleuze and Guattari. As part of the national system, the constitutive features and objectives of the state, implemented through the structures and components of the political system, are considered a priority. These primarily include the category of the security of citizens forming a community, and security of the political system as a tool for implementing this generally formulated objective (from a philosophical point of view, security is composed of three levels: survival, elimination of threats, and development) (Świniarski, 1999: 13). While the subjective scope encompasses all citizens of a given state, the objective one has grown considerably, for instance, in comparison to the 19th century, giving rise to continually-developing sectoral areas (energy security, maritime security, ecological security, water resources security, to name a few).

Digital deterritorialisation in the 20th century was accompanied by the decreasing importance of physical state borders as a consequence of the ongoing globalisation processes which involved internationalisation, institutionalisation and integration of transnational processes. While technological progress made it possible, as the poet prophetically put it, „[t]o see a world in a grain of sand and a heaven in a wild flower / hold infinity in the palm of your hand, and eternity in an hour", the nature of the technological tool exposed some threats in the areas of personal, group, national and global security. At the same time, it became a catalyst for revealing numerous problems related to participating in cyberspace (Open Source Intelligence Investigation, 2016), which has become a field of competition between economic, political and other actors (Dela, 2020: 15). Problems arising from network use also relate to the violation of system security structures, financial and sexual crime (Internet Organised Crime Threat Assessment IOCTA, 2020), the right to privacy, and cyberterrorism (Soler: 2015, 497-499).

2 Responsibility – its philosophical, political and strategic dimensions – taxonomy

Since the beginning of European philosophical reflection, the category of political responsibility has created numerous problems in terms of meaning, definition and legislation. The dilemmas present over the centuries have not been exhaustively explained or resolved, while the circumstances changed by the digitisation of social life have posed new challenges.

Heywood divided the categories of responsibility into three main sections: 1) responsibility for someone or something (for oneself or society); 2) responsibility to someone, which is viewed as *stricte* political, as it refers to the supervisory body (Robertson, 2009: 281); and 3) responsibility as an ethical action regardless of certain influence or circumstances (e.g., the potential decline in popularity or support) (Heywood, 2008: 127). L. Strauss, in turn, noted that nowadays we attach a different meaning to the concept of responsibility – it implies, as a matter of fact, breaking with the tradition of defining and understanding responsibility as synonymous with "being just, right, virtuous" (Strauss, 1998: 258). Following the line of thinking adopted by L. Strauss, it can be assumed that the political dimension now prevails over the ethical dimension, which forms the main axis for contemporary arguments (Tinder, 2003: 133.158).

In the 20th century, reflections on responsibility were the main focus of attention for many fields and disciplines due to the experience of totalitarianism and the world wars. The exchange of ideas influenced the development of human rights and significantly diversified philosophical reflections, with the German-Austrian and French centres paving the way for leading trends (Filek, 2004). The themes taken up from various points contributed to the evolution of the 20th-century narration on responsibility towards a community-based or social perspective of responsibility, indicating its ethical dimension, escaping detailed characterisation. This was also the direction followed by H. Jonas who criticised the concept of "empty formal responsibility" (Filek, 2004: 208).

As part of the philosophical discourse on responsibility, the dimension of freedom conditioning the emergence of responsibility is emphasised. "If we deny the existence of freedom, we deny the existence of responsibility" (Nowicka-Kozioł, 1993: 25, Krąpiec, 1991: 272). In other words, freedom is required for responsibility to arise, and a sense of responsibility is fostered by freedom. This was an axiom which did not raise substantial doubt in the scientific literature of the 20th century, however, a few reservations could be found in this area. One of these was formulated by Hallowell, pointing to the 20th-century tendency of societies to escape responsibility. He wrote: "It was the previous rejection of the verdicts of conscience that enabled Hitler to rise to power" (Hallowell, 1993: 48). Hallowell's assessment did not take into account the difficult economic circumstances of

the post-war crisis, which proves that responsibility for social life was of fundamental importance for this researcher.

20th-century reflection touches upon the problem of the unlawful deprivation of the liberty of individuals in totalitarian systems as a result of the self-deprivation of responsibility, posing threats to the freedom of life and property. In the case commented on by Hallowell, we are dealing with the incorrect self-identification of the situation by citizens, which led to the collapse of the rule of law and the introduction of a state of emergency (Ryszka, 1974). It should be, nonetheless, emphasised that the consequence of the transfer of power in Western or Central European systems reflected an attempt made by citizens to diagnose the socio-political situation on the basis of the available electoral offer. Individual decisions affected society at large, which proved revolutionary as regards its consequences (M. Nowicka-Kozioł, 1993: 8). The transfer of responsibility was effected: 1) by virtue of the incorrect materialisation of the common good in the form of a charismatic leader, or 2) solely with the intention of giving up responsibility, as described by Hallowell, which is, in a way, automatically linked to giving up freedom.

The prevailing contemporary paradigm of the democratic rule of law rests on the foundation of what is considered a set of universal principles of human rights (Robertson: 2009, 343; Universal Declaration of Human Rights of 10 December 1948). The list of these rights has been greatly expanded over the centuries, and today one can even speak of fifth-generation human rights (Zubik, 2008: 6). In western civilisation, the rights to life, property, freedom of conscience, religion, opinion and assembly constitute an established set of principles and values. From a systemic point of view, in western culture the problem of unlawful deprivation of subjective freedoms, based on inalienable human rights intrinsically connected with human dignity, does not exist. One of the principles of a democratic system, namely mutual control based on responsibility, serves both the state and its citizens, forming the axis of a modern democratic governance pattern. It also supports the transparency of the human rights protection process.

The structure, character and ways of using cyberspace influence the reactions of political systems toward information security threats, including threats to data and content manipulation. The necessary element of self-identification of the situation from the angle of its possible consequences, which requires self-reflection, is unrealistic in an era of overproduced information, fast transmissions and huge amounts of information exceeding the capacity of human perception. A contemporary culture of connectivity, based on externalised data and portable databases (Assmann, 2019: 27), not only discourages self-reflection but also promotes a model of non-linear and nomadic culture, presenting the ballast of in-depth analysis as a burden of encyclopaedic knowledge that has become useless in an age of "social competence" and portable digital resources. In turn, being cut off from the deposit of memory and knowledge organised according to the principles of scientific cognition makes it impossible to analyse the problems of network use in an appropriate comparative context. Therefore, the contemporary environment of digital

information is actually becoming conducive to disinformation and manipulation (manipulation is "a way of exerting influence on other people or groups in order to induce changes in their behaviour and conduct. By definition, this mechanism is supposed to influence the subconscious mind of a manipulated person or group in a covert manner") (Harwas-Napierała, 2005: 287) of all activities to gain informational advantage corresponding to the ontological level of war. This non-military dimension is consistent with tactical recommendations by Sun Zi, emphasising the benefits of defeating an enemy at the lowest possible cost and even before a clash of arms. In cyberspace, non-military methods are used, based on psychological techniques of exerting influence, the effectiveness of which lies not in putting forward arguments for the recipient to evaluate them, but in a much more sophisticated method of shaping preferences according to the sender's intention. A separation from verification sources or a belief that they are unnecessary leads to a weakened resistance to psycho-manipulation and thus also to increased other-directedness, the latter being destructive for the sovereignty of the national system as it disturbs the communication balance within the system.

Manipulation in an environment preventing the verification and unbiased assessment of delivered content presents serious ground for making attempts to identify a direction to counteract both information and systemic threats in cyberspace. A component anticipating threats – based on the principles of effective operation (Sennet, 2010), or belonging to the indirect operation strategy (Liddell-Hart, 1959: 13), i.e., promoting a culture of the responsible use of cyberspace, could be considered crucial. Ingarden's "source of decisions" – the person – relies on the understanding of a given situation and a determination to act – in opposition to intuitive action (Ingarden, 1987: 77), while the contemporary navigation of cyberspace is based on an intuitive model of action, cutting to a minimum the need to perform a situation analysis. The speed, dynamics and overproduction of data do not favour moments of self-reflection or verification, and according to philosophical schools of thought, these are the *sine qua non* conditions of responsibility which is indispensable for ensuring strategic and political security and without which it is impossible to achieve.

The challenge of formulating ways to support political and strategic responsibility, as a factor contributing to network security at individual and national levels, is becoming a pertinent matter.

3 The notion of responsibility vs. cybersecurity

The internet, as a meta-medium brought into common use, has blurred the boundaries between the private and public spheres of communication and data acquisition – by having a mobile device with access to a network at our disposal, we automatically become participants of the global exchange of data and messages, whether passive or active, thus influencing the information environment, the centre of which is cyberspace, where the object of attention is information. A user is able to combine his/her professional duties

and private interests in one place and with one medium (i.e., to book a concert ticket while at work, to draw up a report during breaks from taking care of the children, etc.). Over the years, the dynamics of sharing content via online portals or social networks has been increasing. The high rate of network subjectification and the perception of one's own participation as negligible and strictly private influences self-positioning in the digital space in terms of a sense of security and anonymity (Baran, Cichocka, Maranowski. and Pander, 2016). This illusory sense underpins the success of cybercrime which exploits the unawareness of cyberthreats among individual users and employees who disseminate personal or company data in cyberspace. The methods and techniques employed by cybercriminals against individual users are more often simple, which confirms the fact that elementary cybersecurity mechanisms for network users are far from widespread (Kronenberg Foundation, 2020).

The nature and essence of the internet, as a rhizomatic networked matrix of connections, contributes to a reduced sense of responsibility with respect to the vastness of content and apparent user anonymity. Relatively cheap access to data resources makes the internet a tool for facilitating work, learning and entertainment. In the field of data exchange infrastructure (e.g., e-government, remote work), the internet performs the function of somehow liberalising professional life although this type of a resource is also the subject of cyber warfare within OSINT activities. As regards social life, commerce and politics, the internet offers not only a means of free participation and favourable solutions for data administration, services, commerce and entertainment, but it also opens up multiple opportunities for the manipulation of information, preferences and attitudes by means of Big Data and by implementing AI algorithms.

In view of the above considerations, it appears justified to take measures aimed at strengthening political and strategic responsibility as a factor that exerts a positive impact on the security of network use and the systemic security of the state. The notion of strategy, as defined by Liddell-Hart (Liddell-Hart, 1959: 13) stands for "general command" and "day-to-day management of military forces", but the decision to use them, as Liddell was right to note, is dependent on politicians and the custodians of national system security. Given the competitive nature of cyberspace, disseminating the principles of security contradicts the interests of those entities which hope for the citizens to remain credulous and to ignorantly share valuable personal data (Chałubińska-Jentkiewicz, Nowikowska, 2021). It is required: 1) to popularise the perception of the internet as being by nature a disinformation tool; 2) to promote actions in the statutory area (the National Cyber Security System Act of 5 July 2018); 3) to take tactical and operational action in terms of building an information culture based on the principles of cyber hygiene and information ecology (Taraszkiewicz, 2014).

Cyberspace is a reflection of users' interests and needs, rather than of reality (Dela, 2020: 20). The mechanisms that foster a responsibility culture in which decisions and evaluations reflect judgements, rational calculations, the mapping of possible

consequences on a timeline, and the choice of a favourable direction, require a broad promotion of knowledge about the contemporary information environment and the possible consequences of imprudent participation.

4 Conclusions

The reactivation of the culture of strategic and political responsibility will produce a tangible effect through disseminating knowledge of the nature of the internet and the threats it poses, among which the following issues are important: 1) knowledge of the functioning and specificity of the digital infosphere environment – positioning the user as an object of attention of commercial and political actors in order for them to be included in Big Data analysis systems and acquired for particular purposes (commercial and political persuasion); 2) knowledge of the viability of displayed content and its importance in the context of OSINT activities or the cybercrime sector (e.g., phishing); sharing knowledge about one's private life (a new car, a trip) constitutes valuable information which enables building a user's profile for personalised commercial offers, but it also provides criminals with information regarding access to one's real estate; 3) awareness regarding the impact of the overproduction of stimuli and information violence, which both affect the functioning of the human brain (a loss of abstract thinking skills or the reduced ability to process information impulses), decreased ability to concentrate, irritability, information addiction, desensitization, infotainment-related threats (Babik, 2014: 7-19); 4) disseminating knowledge of systemic security tools (two-step security codes, firewalls); 5) attaching adequate importance to regulations and rules which accompany granting consent to use resources, and which point out the potential danger of granting consent to access one's personal data; 6) emphasising how important personal data are these days and the fact that they constitute knowledge capital for commercial entities, media houses, analysts of political life, etc.

The popularisation of knowledge about the digital infosphere has the potential to strengthen the defence mechanisms in society and the level of resistance to threats, and thus to foster the tendencies of increasing responsibility for the content shared and received in the political and strategic dimension, which concludes the arguments presented in this paper.

References:

Assmann, J. (2019) *Pamięć kulturowa. Pismo, zapamiętywanie i polityczna tożsamość w cywilizacjach starożytnych* (Warszawa: Wydawnictwa Uniwersytetu Warszawskiego).

Babik, W. (2014) O konsumpcji informacji w e-społeczeństwie z punktu widzenia ekologii informacji, In: Taraszkiewicz, B. (ed.) *Ekologia informacji w e-społeczeństwie* (Słupsk: Stowarzyszenie Bibliotekarzy Polskich - Zarząd Oddziału Słupskiego, Biblioteka Uczelniana Akademii Pomorskiej w Słupsku, Pedagogiczna Biblioteka Wojewódzka w Słupsku), pp. 7-25, available at:

https://depot.ceon.pl/bitstream/handle/123456789/17699/Ekologia%20informacji%20-%20Taraszkiewicz.pdf?sequence=1&isAllowed=y (September 20, 2021).

Baran, M., Cichocka, E., Maranowski, P. & Pander, W. (2016) *Cybernauci – diagnoza wiedzy, umiejętności i kompetencji dzieci i młodzieży, rodziców i opiekunów oraz nauczycieli w zakresie bezpiecznego korzystania z internetu. Raport podsumowujący badanie ex-ante* (Warszawa: Fundacja Nowoczesna Polska), available at: https://www.civitas.edu.pl/wp-content/uploads/2016/06/Raport-v.6.1.pdf (September 19, 2021).

Blake, W. (1994) *Wiersze i poematy* (Warszawa: Świat Literacki).

Castells, M. (2013) *Władza komunikacji* (Warsaw: Wydawnictwo Naukowe PWN).

Chałubińska-Jentkiewicz, K. (2019) *Cyberodpowiedzialność* (Toruń: Wydawnictwo Adam Marszałek).

Chałubińska-Jentkiewicz, K. & Nowikowska, M. (2021) *Ochrona danych osobowych w cyberprzestrzeni* (Warsaw: Akademia Sztuki Wojennej, War Studies University).

Dela, A. (2020) *Teoria walki w cyberprzestrzeni* (Warsaw: Wydawnictwo Akademii Sztuki Wojennej).

Deleuze, G. & Guattrai, F. (1980) *A Thousand Plateau. Capitalism and Schisophrenia* (London: University of Minnesota Press).

Filek, J. (ed.) (2004) *Filozofia odpowiedzialności XX wieku* (Kraków: Wydawnictwo Uniwersytetu Jagiellońskiego).

Fundacja Kronenberga (2020) *Złapani w sieć – Jak Polacy radzą sobie w cyberprzestrzeni*, available at: https://www.citibank.pl/poland/kronenberg/polish/files/Raport-cybersecurity.pdf (September 22, 2021).

Hallowell, J.H. (1993) *Moralne podstawy demokracji* (Warszawa: PWN).

Harwas-Napierała, B. (2005) Etyczne aspekty manipulacji, *Poznańskie Studia Teologiczne*, (18), pp. 247-259.

Heywood, A. (2008) *Klucz do politologii. Najważniejsze ideologie, systemy, postaci* (Warsaw: PWN).

Ingarden, R. (1987) *Książeczka o człowieku* (Kraków: Wydawnictwo Literackie).

Europol (2021) *Internet Organised Crime Threat Assessment (IOCTA) 2020*, available at: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020 (September 24, 2021).

Krąpiec, M.A. (1991) *O rozumienie filozofii* (Lublin: KUL).

Liddell-Hart, B.H. (1959) *Strategia. Działania pośrednie* (Warsaw: Wydawnictwo Ministerstwa Obrony Narodowej).

Nowicka-Kozioł, M. (1993) *Odpowiedzialność w świetle alternatyw współczesnego humanizmu* (Warsaw: Wydawnictwo WSPS).

Babak, A., Saskia, P., Bayerl, P. & Sampson, F. (eds.) (2016) *Open Source Intelligence Investigation* (New York: Springer).

Patrick, J.J. (2018) *The Art of Hybrid War* (London: Cynefin Road).

Robertson, D. (2009) *Słownik polityki* (Warszawa: PWN).

Ryszka, F. (1974) *Państwo stanu wyjątkowego* (Wrocław: Zakład Narodowy im. Ossolińskich).

Sartori, G. (2007) *Homo videns. Telewizja i postmyślenie* (Warsaw: Wydawnictwo UW).

Sennet, R. (2010) *Etyka dobrej roboty* (Warsaw: Wydawnictwo Literackie Muza S.A.).

Pawłowski, J., Zdrodowski, B. & Kuliczkowski, M. (eds.) (2020) *Słownik terminów z zakresu bezpieczeństwa* (Toruń: Wydawnictwo Adam Marszałek).

Soler, U. (2015) Technologie sieciowe vs terroryzm – czy mogą być społecznie szkodliwe?, *Zeszyty Naukowe Politechniki Śląskiej*, (85), pp. 495-506.

Strauss, L. (1998) *Sokratejskie pytania* (Warsaw: Fundacja Aletheia).

Świniarski, J. (1999) *Filozoficzne podstawy edukacji dla bezpieczeństwa* (Warsaw: Departament Społeczno-Wychowawczy Ministerstwa Obrony Narodowej).

Taraszkiewicz, B. (ed.) (2014) *Ekologia informacji w e-społeczeństwie* (Słupsk: Stowarzyszenie Bibliotekarzy Polskich - Zarząd Oddziału Słupskiego, Biblioteka Uczelniana Akademii Pomorskiej w Słupsku, Pedagogiczna Biblioteka Wojewódzka w Słupsku), available at: https://depot.ceon.pl/bitstream/handle/123456789/17699/Ekologia%20informacji%20-%20Taraszkiewicz.pdf?sequence=1&isAllowed=y (September 19, 2021).

Tinder, G. (2003) *Myślenie polityczne* (Warsaw: PWN).

Volkoff, V. (1991) *Dezinformacja. Oręż wojny* (Warsaw: Wydawnictwo Delikon).

Zubik, M. (2008) *Wybór dokumentów prawa międzynarodowego dotyczących praw człowieka* (Warsaw: Biuro Rzecznika Praw Obywatelskich).