Anna Makuch*

Raising public and private user awareness of the threats and risks related to cyberspace security

Abstract

Modern cybersecurity efforts require the identification ofthe risks and threats associated with the cyberenvironment by consistently increasing public awareness of the dual nature of cyberspace and its use for the purposes of cooperation, and for the purposes of warfare and crime. Raising awareness today means involving both public and private users in cooperationfor the sake of both the common good and common interests involving standards for the use of virtual space.

Key words: state security, cyberspace, data security

* Anna Makuch, PhD, Faculty of Political Science, Academy of Economics and Human Sciences in Warsaw, e-mail: a.makuch@vizja.pl, ORCID: 0000-0002-5222-4407.

Introduction

This paper is concerned with the identification ofthe opportunities, and the assessment of the scale of challenges, related to raisingthe internet user awareness of cybersecurity threats. The user group being analysed herein is limited to the national dimension, although the independent context of individual security and the global context will remain present as they are related to state security. The national scope covers users of Polish nationality who are residing within the physical boundaries of the country, and users residing outside its borders, holding Polish citizenship and identifying themselves through Polish culture and the Polish state.

The main objective will be achieved by using the analytical-critical method for key concepts, phenomena and categories, which will be functionally conceptualised. The resulting picture will serve as a guide to outline directions, methods and techniques for raising awareness in a current and future perspective among domestic users of cyberspace.

The importance of digitised space over the years and, as a consequence of current socio-political developments in the international environment, (the acceleration of the digitalisation of many areas as a result of pandemics, the Russian invasion, ultra-fast innovations, etc.) has been steadily increasing, giving cybersecurity strategic importance in documents of the state and alliances as well as in international law. The growth of this importance results from the practice and the use of the digital environment not only for peaceful purposes, but also on an ontological level – for the purposes of warfare („proxy war"[1]) and crime at every level (individual, group, regional, as part of hybrid warfare). Hence, historians and war theorists attempt to conceptualise new wars, noting key transformations (asymmetry, light weapons, the absence of the stage of declaring war, etc.), and as a result it is considered that today we are dealing with peace and war processes lasting for yearsoften at the same time and at variable intensities (*low intensity war*)[2]. In these processes, cyberspace plays an offensive and defensive role, in terms of data and information operations[3]. The dilemma regarding the cyberspace security paradigm is among some of the particularly significant strategic challenges of states.

1 Cf. R. Mucchielli, *La Subversion*, Paris 1976.
2 H. Münkler, *Wojny naszych czasów*, Kraków 2004, p. 36.
3 Cf. V. Volkoff, *Krótka historia dezinformacji. Od konia trojańskiego do Internetu*, Wrocław 2022.

The systematisation of the main concepts and categories

The category of awareness is one of the concepts that is quite vague and poses great definitional difficulties. Descartes associated awareness with self-awareness[4]; according to John Locke, human beingsare based not only on substantiality, but also on deeper introspection and a transition from a primary level to a reflective one, i.e. enriched by self-analysis on the timeline and in the spatial dimension („For since consciousness always accompanies thinking, and 'tis that, that makes every one to be, what he calls self; and thereby distinguishes himself from all other thinking things, in this alone consists personal identity, i.e. the sameness of a rational being: And as far as this consciousness can be extended backwards to any past Action or Thought, so far reaches the Identity of that Person"[5]). Awareness, therefore, implies the processual recognition[6] of the features of the object of attention, the operationalisation of the principles of functioning and the determination of the directions of development, taking into account the environment in the whole complex system of interdependencies.

Hence, raising awareness of the threats posed by cyber environment requires, first of all, the identifying of the features of the digitised space and outlining the directions of development, taking into account the implications of new tools or functions in the context of individual, group, state and global security as directly interconnected levels. Second, it requires recognising the human situation in the new digital environment, which has had a revolutionary impact on all planes of human functioning, from the economic through to social and political aspects, to cultural ones. This recognition should take into account the key determinants, including the technological aspect and the exact sciences, as well as the social aspects with disciplines that shape the information environment, such as social psychology, social communication, international relations and cultural foundations of security[7]. Only by outlining the perspective in this way is there some chance of developing a broad spectrum of strategies and tactics of raising the awareness of threats in cyberspace.

4 R. Descartes, *Rozprawa o metodzie*, Warszawa 1970, p. 39.
5 J. Locke, *Rozważania dotyczące rozumu ludzkiego*, vol. 1, Warszawa 1955, p. 472.
6 Cf. R. Ingarden, *Książeczka o człowieku*, Kraków 1987, p. 77.
7 Cf. J. Czaja, *Kulturowe czynniki bezpieczeństwa*, Kraków 2008.

Cyberspace is a modern globalised nervous system[8] devoid of clear boundaries and based on the principle of the free exchange of data, which is not only a dynamic space for interaction, but is, as shown in practice, fraught with the risk of increasing threats in terms of interference in the free circulation and the exchange of information[9] and the protection of data[10]. Cyberspace – „the space for processing and exchanging information created by communication and information systems"[11] – has introduced humans into the third stage of social communication (after direct communication i.e. based on personal communication and traditional media communication i.e. based on one-way sender-receiver communication) – the partnership communication on social media, in which the recipient has the opportunity to contact the sender through instant messaging as well as in real time of a programme, broadcast, podcast (comments, chat, Twitter – hashtags, etc.). The characteristics of the modern era of communication are: new media, the personalisation of channels, contact between audience and sender, the hybrid nature of media, and time and space convergence. According to Jan van Dijk, binary code, integration and interactivity define the modern model of the cybernetic contact formula[12].

The metaphors created by scholars of various disciplines similarly map the structure and nature of cyberspace, symbolically signalling a shift from a cultural paradigm based on paper sources to a paradigm of external cache memory[13]. Gilles Deleuze and Felix Guattari, for example, put forward the rhizome theory – a non-linear and discontinuous narrative whose boundaries are the physical object of the book and where each plateau constitutes an independent coherent whole. „A book has neither object nor subject; it is made of variously formed matters, and very different dates and speeds"[14] Contemporary fragmentary forms of creativity with a rhizomatic structure,

8 Cf.: J. van Dijk, *Społeczne aspekty nowych mediów*, Warszawa 2010, p. 35–63; M. Castells, *Władza komunikacji*, Warszawa 2013.

9 Cf.: K. Chałubińska-Jentkiewicz, *Dezinformacja jako akt agresji w cyberprzestrzeni*, „Cybersecurity and Law" 2021, no. 1, p. 9–24; P. Dela, *Teoria walki w cyberprzestrzeni*, Warszawa 2020.

10 Cf. F. Radoniewicz, *Przestępstwa komputerowe w polskim Kodeksie Karnym*, „Cybersecurity and Law" 2019, no. 1, p. 193–212.

11 *Cyberprzestrzeń* [in:] *Słownik terminów z zakresu bezpieczeństwa*, eds. J. Pawłowski, B. Zdrodowski, M. Kuliczkowski, Toruń 2020, p. 38.

12 J. van Dijk, op. cit., p. 16–17.

13 Cf. J. Assmann, *Pamięć kulturowa. Pismo, zapamiętywanie i polityczna tożsamość w cywilizacjach starożytnych*, Warszawa 2015.

14 G. Deleuze, F. Guattari, *Tysiąc plateau*, Warszawa 2015, p. 5.

those without beginning and end, correspond to the nomadic character of cyberspace, essentially sovereign over reality, which means that, considering cyberspace in terms of mimesis, the reproduction of layout and character of the real world is a fundamentally incorrect formula for capturing the essence of the digitised world. This is because it is an extrapolation of consciousness and the needs of humans, who do not need another real world, but a space for the realisation of economic, social or professional needs that transcend the barriers of time, space, cultural and linguistic differences through the platform being a metamedium – the internet. The leading objective of the internet is liberalisation, understood as the facilitation of a number of functions (the simplification of shopping procedures, personalisation of content – algorithms that suggest products, services or accounts to subscribe to or follow).

Contemporary models of creativity and the paradigm of the internet--connectivity culture have moved markedly away from the model whose graphic representation is a tree; the seed is the beginning, whose continuation is the trunk, branches and leaves. In this view, Plato is the seed of a philosophical school whose branches are disciples and continuators. And the forest would be a figure of the accumulated stock of human knowledge. Realising (nomen omen) the model of modern network culture in opposition to tree culture leads naturally to an attempt to frame the human situation in the new environment in terms of security. The postmodern paradigm of pluralistic attitudes has developed into post-postmodern relativism, making distinction in the information environment much more difficult. A return to the positivistic paradigm, according to which one believed in objective reality[15], is now clearly unrealistic. As can easily be seen, a communication space constructed and functioning in this way lacks the causal sequences characteristic of the development of science based on the dialogue of traditional cultural memory and the methodological apparatus that allows for substantive dialogue based on sources. The order of cyberspace discourse is random in nature and the constitution of binding truth does not depend on the will of Truth, but on the will and persuasive power of the sender[16]. Thus, the construction of cyberspace has become an ally of the „new wars" based not so much on traditional black propaganda as on shaping perceptions through manipulative techniques[17].

15 Cf. E. Babbie, *The Practice of Social Reseach*, Wadsworth 2010, p. 31–61.
16 Cf. M. Foucault, *Porządek dyskursu*, Gdańsk 2002, p. 15–21.
17 Cf. A. Huxley, *Nowy wspaniały świat 30 lat później. Raport rozbieżności*, Warszawa 2018.

The objectives and means of raising awareness of threats in cyberspace

An informed attitude in the new environment of cyberspace not only means raising the stock of knowledge and the ability to qualify events as threatening or affecting security, but also involves restoring a sense of accountability, which in effect, as philosophers point out, always has a social dimension[18]. Accountability is not limited to the individual and shows a far broader resonance of the effect of a decision or even an attitude, for an attitude will sooner or later find expression in interaction[19]. The paradoxical atrophy of accountability in the age of democratisation demands, in the opinion of critics, the restoration of the moral principle of accountability in place of the „formal-empty" one criticised by one of the most prominent experts on the subject, Hans Jonas[20], whose direction was supported by Leo Strauss[21]. The seemingly anonymous digital environment is conducive to freeing users from a sense of accountability for the export and resonance of content – facilitated by today's infotainment-based „fast-paced communication" formula. Developing awareness of digital work and entertainment tools will foster caution and accountability among users for the sake of personal safety and to avoid the use of exported content for commercial, ideological or criminal purposes. From a state security perspective, user prudence translates into less obvious profiling of the user base and socially or culturally sensitive topics based on unclassified sources available to unfriendly actors.

The processuality of raising awareness and accountability corresponds to the processual nature of cyberspace and the analysis of situations in light of possible consequences. In view of the impossibility of creating a closed catalogue of cyberspace characteristics (it is still developing though), and, consequently, a closed catalogue of threats to data storage and transmission

18 Cf. J. Kozielecki, *Koniec wieku nieodpowiedzialności. Eseje humanistyczne*, Warszawa 1995, p. 64.

19 Andrew Heywood points out three meanings of accountability: 1) for oneself or society, 2) to somebody, strictly political variety, refers to controlling authority, 3) as an ethical action regardless of the circumstances – A. Heywood, *Klucz do politologii. Najważniejsze ideologie, systemy, postaci*, Warszawa 2008, p. 127.

20 H. Jonas, *Teoria odpowiedzialności: podstawowe rozróżnienia* [in:] idem, *Filozofia odpowiedzialności XX wieku*, ed. T. Filek, Kraków 2004, p. 208.

21 Cf. L. Strauss, *Wykształcenie liberalne i odpowiedzialność* [in:] idem, *Sokratejskie pytania*, Warszawa 1998, p. 258.

and the export and management of information, raising awareness of threats cannot be limited to the classification and knowledge of current techniques and tools, but should equip users with the ability to recognise new risks based on accumulated resourcesalong with theoretical and practical knowledge, becoming the basis for raising social resilience to cyber threats.

Hence, raising awareness is a „process of reasoning"[22], a total or „holistic" view of assessing capabilities and about making measured choices; it is also the realisation of the suggestions of both Sun Zi and Beaufry, according to whom the preparation stage and pre-emptive action show a significant advantage over a reactive strategy[23] because of the efficiency and cost of the action. Increasing awareness is not restricted to the technological aspect, just as „No artist has ever painted a picture by following a complete set of theoretical rules"[24]. It is a complex process that requires architects to take a multidisciplinary approach, imposing an obligation to combine the technological aspects with the humanistic and social aspects. The practice of a plan outlined this way, i.e. the application of the strategy requires measures that simplify but also preserve the multidimensional nature of cyber threats.

Raising user awareness can be organised by the criterion of the objectives to be achieved: 1) the objective to systematise, i.e. to organise the accumulated knowledge in a nomothetic and idiographic arrangement, accumulating experience and knowledge into a resource that takes into account the leading trends of development and threats, but also individual cases. Given the transnational challenges to the collective security formula, systematics should address the experience of similar actors in other legal and political systems. Given the criterion of data, one can take the level of protection of data and the level of protection of the freedom of communication space and realise thatpublic and non-public entities conducting systematisation activities in the indicated areas do not create a common database, a portal collecting data specifications and links to individual activities and entities. It seems that an attempt to organise the resources and the participation of the widest possible circle of participants would have a positive impact on the public perception of the content and the growth of public trust, which will be discussed more broadly hereunder; 2) the objective to normalise and create norms – i.e. to influence the production of the mechanisms of cooperation, action and

22 A. Beaufre, *Wstęp do strategii. Odstraszanie i strategia*, Warszawa 1968, p. 25.
23 Ibidem, p. 51.
24 Ibidem, p. 52.

response procedures of all participants in accordance with national security interests and in the interests of all users of cyberspace within the framework of the state and international regulatory systems[25]; 3) the objective to dynamise, i.e. to influence the efficiency of the results obtained and to improve the dynamics of action corresponding to the dynamics of the evolution of the digital environment. The specificity of cyberspace, which involves Surface Web, Deep Web and Dark Web, in terms of resources and speed of response, points to the fundamental differences based on moral and normative standards observed (or not). Users of, for instance, Dark Web manage a hermetic space, the use of which is not subject to control by any norms, in which the space there is of a freedom to act outside the international sphere of binding regulations and rules. Given the above, the reinvigorating objective should be an equivalent element of the project's component objectives.

The objectives can be pursued through actions or activities involving, in a more or less formalised way, the cooperation of public and private user communities, the actors of the national system that are aware of how important it is to protect cyberspace in their own interests and in the perspective of state security. This type of the whole-of-society approach is considered to match the level of threats and is appropriate as a starting point for building resilience and digital competence. Public-private cooperation for cyberspace is becoming a sine qua non, where a new type of warfare involves aggressive activity in both state and private enterprises. Actually, in terms of the objective, the actions to be taken should include: 1) periodic open training/webinars on the levels of security and threats in cyberspace, i.e. the physical, technical, IT, normative and cultural levels. The training should cover the assessment of national and international cybersecurity strategies, defensive alliance cyberstrategies and available documents making up programmes of entities hostile to or threatening the security of the Republic of Poland and the collective formula of global security, cultural determinants of security (strategic policy, assessment of the level of social capital of trust etc.), current research results of leading scientific and expert centres and case study analysis; 2) building long-term partnerships through joint ventures, the exchange of knowledge, experience, procedures, responses, strategies, tactics and techniques of operation. Partnership relations mainly pursue the objective to normalise, which is

25 Cf. J. Sobczak, *Przestępczość w cyberprzestrzeni między przepisami polskimi a międzynarodowymi*, „Cybersecurity and Law" 2019, no. 1, p. 159–192.

accompanied by the integration of partners; 3) activity in industry network organisations of regional, national or international scope; such activity involves participation through the implementation or planning, observation; initiating and developing contacts, maintaining good relations. Activity has a practical, task-based and, at the same time, relational dimension understood as building contacts for efficient and effective cooperation and communication; 4) the creation of competence networks to coordinate and integrate communities, initiate and implement solutions at local and national levels, as well as at the levels of international cooperation. Creating competence networks in a more or less formalised manner will improve the exchange of information and technical solutions for the creation of security systems; 5) given the inherently threatening nature of the DarkWeb, the activity of criminal and terrorist circles and organised disinformation campaigns, it seems reasonable to attach importance to making the communication formula between participants and partners more flexible through a communication platform that allows real-time interaction of project participants and the agreement on planned strategies and procedures for action.

The above proposals should be accompanied by a commentary that is essential from the point of view of the project, taking into account the cultural context of security, meaning national culture, strategic culture and political culture. Why the need to raise this issue? Cyber operations rely not only on technical reconnaissance of the network environment, but equally importantly on knowledge of the adversary, its mentality and cultural code, which is the starting point in planning, for example, disinformation operations[26]. Hence the need to consider strategic culture from a philosophical perspective that takes into account two aspects: I – the past, and II – the future. They constitute the obverse and reverse – the past closed ontologically, open epistemologically; the future open ontologically, closed epistemologically. The present is the result of a creative analysis of cause and effect, which should bring about the maximisation of security[27].

Polish national culture and political culture[28] are characterised by lability, pluralism, individualism, the persistence of romantic myth and

26 Cf. V. Volkoff, *Dezinformacja – oręż wojny*, Warszawa 1991.

27 J. Świniarski, *Filozoficzne podstawy edukacji dla bezpieczeństwa*, Warszawa 1999, p. 126–127.

28 D. Robertson, *Słownik polityki*, Warszawa 2009, p. 206–209.

noble anarchism[29]. The ability to manage emotions based on these enduring topoi gives a quantifiable assessment of the effectiveness of disinformation operations, which should be planned taking into account the possible directions of reaction and social resonance. Polish society is deeply pluralised, the media remain tied to political circles, and the level of social capital remains too low[30]. Given the above, the success of the key objective is related to building the broadest possible platform for cooperation between institutional and business users, which would improve the level of trust in the content presented.

Conclusions

One of the currently applicable methodological approaches in social sciences involvesthe still useful paradigms: conflict and Darwinism. According to the former, conflict is a driving force for development, while according to the latter, security and development depends on adapting to the opportunities and constraints of the social environment in order to maximise causative power, to influence reality in accordance with one's own interests and values. Darwinism points to the important determinant of the superiority of the subject, prescribing the development of instruments to enhance influence, that is, the active transformation of the environment, not only for survival and the elimination of threats, but to secure development understood as the relative freedom to choose directions of action. Given the current threats in cyberspace and the use of cyberspace for more than peaceful coexistence, the component of raising user awareness is among the superior objectives of the network security project, equipping participants with „meta" skills to concretise and develop competencies based on the fundamental systematisation of recognition of the nature and functionality of cyberspace.

29 R.R. Ludwikowski, *Polska kultura polityczna. Mity, tradycje i współczesność*, Wrocław 1980, p. 18–26; J. Garlicki, *Tradycje i dynamika kultury politycznej społeczeństwa polskiego* [in:] *Dylematy polskiej transformacji*, ed. J. Błuszkowski, Warszawa 2007, p. 163.

30 *Wartości i zaufanie społeczne w Polsce w 2015 r. (Notatka informacyjna na podstawie Badania spójności społecznej)*, https://stat.gov.pl/files/gfx/portalinformacyjny/pl/defaultaktualnosci/5486/21/1/1/wartosci_i_zaufanie_spoleczne_w_polsce_w_2015r_.pdf [access: 14.07.2021].

Bibliography

Assmann J., *Pamięć kulturowa. Pismo, zapamiętywanie i polityczna tożsamość w cywilizacjach starożytnych*, Warszawa 2015.
Babbie E., *The Practice of Social Reseach*, Wadsworth 2010.
Beaufre A., *Wstęp do strategii. Odstraszanie i strategia*, Warszawa 1968.
Castells M., *Władza komunikacji*, Warszawa 2013.
Chałubińska-Jentkiewicz K., *Dezinformacja jako akt agresji w cyberprzestrzeni*, „Cybersecurity and Law" 2021, no. 1.
Cyberprzestrzeń [in:] *Słownik terminów z zakresu bezpieczeństwa*, eds. J. Pawłowski, B. Zdrodowski, M. Kuliczkowski, Toruń 2020.
Czaja J., *Kulturowe czynniki bezpieczeństwa*, Kraków 2008.
Dela P., *Teoria walki w cyberprzestrzeni*, Warszawa 2020.
Deleuze G., Guattari F., *Tysiąc plateau*, Warszawa 2015.
Descartes R., *Rozprawa o metodzie*, Warszawa 1970.
Dijk van J., *Społeczne aspekty nowych mediów*, Warszawa 2010.
Dylematy polskiej transformacji, ed. J. Błuszkowski, Warszawa 2007.
Foucault M., *Porządek dyskursu*, Gdańsk 2002.
Heywood A., *Klucz do politologii. Najważniejsze ideologie, systemy, postaci*, Warszawa 2008.
Huxley A., *Nowy wspaniały świat 30 lat później. Raport rozbieżności*, Warszawa 2018.
Ingarden R., *Książeczka o człowieku*, Kraków 1987.
Jonas H., *Filozofia odpowiedzialności XX wieku*, ed. T. Filek, Kraków 2004.
Kozielecki J., *Koniec wieku nieodpowiedzialności. Eseje humanistyczne*, Warszawa 1995.
Locke J., Rozważania dotyczące rozumu ludzkiego, vol. 1, Warszawa 1955.
Ludwikowski R.R., *Polska kultura polityczna. Mity, tradycje i współczesność*, Wrocław 1980.
Mucchielli R., *La Subversion*, Paris 1976.
Münkler H., *Wojny naszych czasów*, Kraków 2004.
Radoniewicz F., *Przestępstwa komputerowe w polskim Kodeksie karnym*, „Cybersecurity and Law" 2019, no. 1.
Robertson D., *Słownik polityki*, Warszawa 2009.
Sobczak J., *Przestępczość w cyberprzestrzeni między przepisami polskimi a międzynarodowymi*, „Cybersecurity and Law" 2019, no. 1.
Strauss L., *Sokratejskie pytania*, Warszawa 1998.
Świniarski J., *Filozoficzne podstawy edukacji dla bezpieczeństwa*, Warszawa 1999.
Volkoff V., *Dezinformacja – oręż wojny*, Warszawa 1991.
Volkoff V., *Krótka historia dezinformacji. Od konia trojańskiego do Internetu*, Wrocław 2022.
Wartości i zaufanie społeczne w Polsce w 2015 r. (Notatka informacyjna na podstawie Badania spójności społecznej), https://stat.gov.pl/files/gfx/portalinformacyjny/pl/defaultaktualnosci/5486/21/1/1/wartosci_i_zaufanie_spoleczne_w_polsce_w_2015r_.pdf [access: 14.07.2021].

Budowanie świadomości publicznych i prywatnych użytkowników w zakresie zagrożeń i ryzyk związanych z bezpieczeństwem cyberprzestrzeni

Streszczenie

Współczesne działania w obszarze bezpieczeństwa cyberprzestrzeni wymagają rozpoznania środowiska cyber pod kątem ryzyk i zagrożeń poprzez systematyczne budowanie świadomości społecznej dotyczącej dwoistej natury cyberprzestrzeni i jej wykorzystywania do kooperacji i celów wojenno-przestępczych. Budowanie świadomości współcześnie oznacza zaangażowanie użytkowników publicznych i prywatnych kooperujących w imię wspólnego dobra i wspólnych interesów dotyczących standardów użytkowania przestrzeni wirtualnej.

Słowa kluczowe: bezpieczeństwo państwa, cyberprzestrzeń, bezpieczeństwo danych