Krzysztof Drabik*

Cyberspace in a risk society

Abstract

The dynamic processes of modernization have affected the quantitative and qualitative dimensions of an unprecedented social transformation. It can be said that man has entered into hitherto unknown realms of abstraction. One of its dimensions is cyberspace with attributes that elude previous identifiers of physical three-dimensional space. The highly dynamized processes of technological progress have situated societies in new dimensions of risk. The likelihood of positive or negative events has been etiologically linked to the effects of „producing", processing, storing, and transmitting the information. This article aims to analyze the factors justifying the crystallization of a risk society, a key identifier of which is cyberspace, the associated risks, and security measures in the context of shaping cybersecurity.

Key words: cyberspace, cybersecurity, threat, infosphere

* Assoc. Prof. Krzysztof Drabik, PhD, University of Natural Sciences and Humanities in Siedlce, e-mail kfdrabik@gmail.com, ORCID: 0000-0002-6555-1124.

For centuries, risk has been a peculiar measure of human behavior and a component of a set of criterion-based determinants of decision-making processes[1]. This is not a new term, and at the same time, it is part of the efforts to avoid difficult situations (threats) on the one hand and to develop prospective strategies to shape a safe existence on the other. Risk has accompanied man since the dawn of time, coupled with a greater or lesser awareness of its occurrence, and thus the ability to estimate the probability of a particular event. The semantic scope of the term risk has not changed.

The dynamics of transformations adequate to the current conditions of late modernity[2] can be seen in the identification of new risk parameters, i.e. those factors that form the criterion basis for determining probability and risk management. The innovation of risk parameters mainly concerns their natural (nature) and cultural (civilization) etiology. The core or a kind of informational base in estimating the probability of threats in history has been knowledge of risk concerning adverse weather events, epidemics, and even wars[3]. „Traditional" parameters were characterized by significant human independence or, conversely, were purely individual, making it largely difficult to achieve a high degree of precision in risk estimation. At that time, it was mainly based on experience, the rule of repetition, and „habit", which the English philosopher David Hume made the main ingredient of his epistemological inquiries[4]. Late modernity has become an arena for reconfiguring risk parameters. The development of civilization has changed the understanding of risk in its ontological sense. According to the German sociologist Ulrich Beck, contemporary risks and threats differ significantly from the – outwardly often similar – threats of the medieval period by their global nature and

1 Risk comes from the Latin *risicum* meaning chance, probability of occurrence of a positive or negative event, S. Hahotko, *Ryzyko ekonomiczne w działalności gospodarczej*, Bydgoszcz 2001, p. 37–38.

2 Late modernity is a term for a stage of civilizational development, including economic, social and technical modernization accentuating the end of the industrial age. An indicator of the transition from modernity to late modernity (postmodernity) is the shift from the logic of production to the logic of risk. This marks a noticeable transformation of the uncompromising era of production into an era of threats – the side effects of production processes.

3 Throughout history, war has been viewed as one of the natural elements, as a necessary evil comparable to inevitable epidemics: A.J. Toynbee, *Wojna i cywilizacja*, Warszawa 2002, p. 22.

4 Causal inference is not, according to D. Hume, a work of reason but of habit. Man tends to perceive reality through the prism of repetitive events, W. Tatarkiewicz, *Historia filozofii*, vol. 2, Warszawa 2003, p. 113.

modern causes. We are talking about the risks associated with modernization. It is a lump sum product of the industrial machine of progress, and as it continues to develop, it is systematically increased[5]. Despite the invariability of the etymological scope itself, the information coefficients have changed. Referring to the terminology of research methodology, independent variables were replaced by dependent variables. In late modernity, risk assessment factors are closely correlated with the effects of human activity, specifically the effects of interference with natural processes in natural ecosystems. The transformation of risk parameters is currently reduced to the side effects of civilizational modernization in general.

The transformation outlined above concerns not only the qualitative parameters of risk inherent in the products of development processes. The quantitative parameter has also changed. Risk is not an inherent situation, objectively embedded in independent phenomena of nature, rather it is the effect of production, a permanent increase in the probability of undesirable events. In late modernity, risk is no longer identified with an act of fate over which humans have no or little influence; it is produced adequately to the degree of a person's dependence on their own creations, especially the creations of technology.

The eternal need to be free from the influences of nature has been largely satisfied in late modernity. This was accompanied by a teleology of risk reduction throughout history determined by the natural world, as well as human-created risk in limited time and space. Indeed, the progress of civilization has greatly contributed to the minimization of threats permanently inscribed in the existential condition of man throughout history. An example is the knowledge of the etiology of many diseases decimating humanity, the discovery of effective methods of therapy, principles of prevention, and hygiene. The results of scientific research and their application to the rhythm of human life, the increase in hygiene, the culture of waste management, and finally the increase in awareness of the occurrence of risks, their etiology, anatomy, and function have increased the area of human autonomy on an unprecedented scale.

However, the above risk reduction process is not linear. In fact, the risk has not been eliminated, but, in line with the thesis formulated in the introduction of this article, its parameters have changed. Man has deconstructed risk by

5 U. Beck, *Społeczeństwo ryzyka. W drodze do innej nowoczesności*, Warszawa 2002, p. 30.

initiating changes in its parameters, involving the replacement of factors (variables) of natural etiology with factors (variables) of cultural (technical) etiology. The above problem of the change in the criteria for perceiving and understanding risk in late modernity was brilliantly captured by Urlich Beck, highlighting the negative effects of modernization processes. He interprets risk as not only having undergone a criterial transformation through changes in its parameters but has acquired a broader social meaning, becoming the foundation of a new kind of risk society. This type of society operates under a high probability of threats. These are not, however, threats that have determined the existential condition throughout history, but entirely new ones that are the product of modernization processes. In a risk society, the probability of hazards is not the result of some configuration of natural elements but is a product of complex mechanisms (technologies) of production. The risks inherent in the progress of civilization have become a substitute for „traditional" risk factors. A developmental paradox is embedded in modernization juxtaposed with increased risk. The source of probabilism is not nature itself but humans profoundly transforming it. It seems accurate to formulate the thesis that every product of the human mind (tangible and intangible) generates a new reality, and thus produces new risk parameters.

The above general statement on risk, and more specifically on the concept of risk society, is coupled with the dynamically developing contemporary information and communications space (cyberspace)[6]. Cyberspace is the scene for the consolidation of complex scientific theories in the field of control systems of communication processes, processes of information exchange, and their application into the practice of functioning of social structures in virtual space.

In the context of the risks of late modernity are inscribed threats, which are attributes of the production and transmission of information in the information and communications space. The important status of these threats is due to the widespread implementation of information technology into the practice of social life in virtually every dimension. The existing channels of information production and transmission have been largely replaced by virtual space, determining the ontological status of the infosphere[7]. Material

6 Writer William Gibson introduced the term cyberspace into social discourse. The author defined cyberspace as a consensual hallucination, experienced every day by billions of legitimate users in all countries, W. Gibson, *Neuromancer*, Poznań 1984, p. 53.

7 According to Juliusz Lech Kulikowski, the infosphere is the informational environment of man that includes those types of information that are available to them through the centers

reality has been determined by the processes of production and transmission of information in virtual reality.

This state of affairs can be qualified as the next stage of modernization evolution (revolution), its historical mechanism of building increasingly complex systems of civilizational support for the natural processes of human life. The phenomenon of the transformation of traditional social structures from the era of slavery, and feudalism, through the industrial society, service society, to the information society, falling into the more general category of risk society, is dynamic. The production of information and its transmission in complex and unlimited systems of virtual reality is coupled with the production of risk, growing in tandem with the degree of participation of information and communications space in the social fabric (institutional, organizational, economic, military, and others). The idealistic world present in philosophical theories, beginning with Plato's world of ideas, materialized in the form of an immaterial virtual reality. Plato's world of ideas could be juxtaposed with the world of information in an idealistically perceived cyberspace[8]. This space, like Plato's world of ideas, remains outside the realm of sensory cognition, yet

of higher nervous activity, J.L. Kulikowski, *Człowiek i infosfera*, „Problemy" 1978, no. 3, p. 2–6. Luciano Floridi, on the other hand, states that the infosphere describes the entire information environment, which consists of all the information entities, as well as the information factors of their properties, interactions, processes and mutual relations, L. Floridi, *A look into the future impact of ICT on our lives*, „The Information Society" 2007, no. 23, p. 59. The infosphere should not be reduced to the technical component, expressed in the creation, transmission, storage and processing of information in information systems. The infosphere constitutes the informational environment of the subject, influencing its attitudes, behaviors, types of activity and developmental directions. The infosphere is increasingly determining transformations within culture. Stanislaw Jarmoszko defines the concept of security infosphere in the dimension of information utilitarianism for the benefit of security in general. According to the author, the security infosphere is the manner and scope of using the information itself, as well as information instruments (infrastructure) to create the generally understood security of a given entity in all its subject planes, S. Jarmoszko, *Anthropology of Security. Contours of scientific identity*, Siedlce 2015, p. 237. All interpretations point strongly to the technical determinants of the emergence and development of the infosphere, while at the same time emphasizing the social effects of exploiting the potential offered by new information and communication technology solutions.

8 In a major simplification, due to some attributes, Plato's world of ideas can be juxtaposed with contemporary digital space situated outside of traditional physical-spatial criteria. The axis of Plato's parallel world are hierarchical ideas, at the top of which is the idea of good, which is very difficult to see, but whoever sees it will realize that it is the cause of everything that is right and beautiful, that in the visible world, light and its master come from it, and in the world of thought it rules and gives birth to truth and reason, and that it must be seen by anyone who is to act wisely in private or in public life, Platon, *Państwo*, Kęty 2003, p. 224.

it is an ontological entity. The ontological status of cyberspace is an extremely interesting problem not only within the philosophical inquiry. The platonic idea is a real entity that, through its characteristic of ideality, remains beyond the reach of sensuality, and falls within the realm of rationality. Piotr Sitarski rightly states that virtual reality has all the features of the real world, except one – existence[9]. The circulation of information takes place in an unlimited space with an increasing number of repeatedly interconnected feedback info channels.

Cyberspace is not just a focal area for the effects of advanced information technology development in the space of information production and transmission. It is a turning point in cultural transformations, and worldviews, it reforms lifestyles, manners of activity both in the private and public (professional) spheres. The process of implementing cyberspace into the standards of human life introduces new dimensions of risk. This is due to the dialectical regularity of progress and even the general essence of evolutionary change, which was the subject of philosophical reflection by Georg W.F. Hegel. Every thesis, in this case, related to the development of information technology, clashes with the antithesis, the threats associated with the disintegration of this informational virtual space. The clash of the thesis and antithesis in the perspective of the functioning of cyberspace and its threats are intended to lead to the formation of the security of subjects (human beings, social groups) in the conditions of a highly developed digital infosphere[10].

Virtual reality, the creation of a global information space, the digital infosphere, has become the beginning of a new post-modern quality of life, importantly increasingly susceptible to all kinds of adverse turbulence. The deeper a person penetrates the parallel information and communications space, the more they generate the risk of adverse phenomena and events

9 P. Sitarski, *Rozmowy z cyfrowym cieniem. Model komunikacyjny rzeczywistości wirtualnej*, Kraków 2002. Cyberspace is referred to in the literature as the fifth dimension of security next to the „traditional" dimensions identified in geospatial form: land, air, sea and space, M. Szyłkowska, *Piąty wymiar bezpieczeństwa*, Kraków 2019, p. 17.

10 Positive and negative contexts of the functioning of cyberspace lead to the development of a synthesis, i.e. security, which will not only be identified with the existence of a person in virtual reality, but, above all, will be the basis for further development. The above dialectical regularity inherent in the process of shaping cybersecurity in a developmental perspective is reflected in Hegel's phenomenological reflection on the dialectical principle of the concept. The higher dialectic of the concept consists in considering the term not merely as a limitation and a contradiction but also in such a way as to extract from that term a positive content and a positive result, for only in this way is the dialectic an unfolding, an immanent forward movement, G.W.F. Hegel, *Zasady filozofii prawa*, Warszawa 1969, p. 53.

in this space. This supports the thesis formulated earlier that humanity is creating new parameters of risk through progress, and the infosphere and cyberspace are one of the increasingly significant components of this risk. Advanced information creation and processing technology is subject to the laws of the dialectical polarity of thesis and antithesis. The positive role of information in building stable social structures and the negative dangers of information disintegration. The threats inherent in cyberspace modernization processes are subject to the same principles that imply the advantages of the information and communications technology realm. One of the most important attributes of the dynamic development of cyberspace is massiveness, both in terms of potential sources of information as well as its audience. Massiveness, universality, and globality are all features of contemporary information that is polarizingly confronted with the same massiveness of potential threats. One dimension of these threats is not only technical interference with the proper functioning of cyberspace as originally intended but also interference with the qualitative aspects of the information itself. It is associated with the dissemination of false information, manipulation, cognitive interference, or simply the spread of ideologized propaganda. In addition to the so-called pure information shaping minds in the society, stable cyberspace is a guarantee of well-functioning institutional structures of the state, including above all critical infrastructure. With a high degree of scientific integrity, it can be said that cyberspace has in many ways escaped the scrutiny calculated to achieve the specific goals behind its creation. This is because there is a paradox inherent in it, if only in the term „space" itself, often associated with defining some boundary in a three-dimensional system. Of course, space can be equated with an infinite three-dimensional area, but cyberspace cannot be reduced to a three-dimensional area. Thus, the use of the term „space" to describe the digital infosphere is rather purely conventional.

Given the above, the following features of cyberspace can be distinguished: 1) accidentality; 2) immateriality; 3) limitless; 4) universality and commonness; 5) interactivity; 6) dynamism; 7) flexibility; 8) unpredictability; 9) liberality[11].

11 The creation, processing, and storage of information in cyberspace is characterized by commonness, global access, and spatial unlimitedness. Thus, it can be concluded that cyberspace is a platform for the spread of freedom in virtual reality. The idea of liberalism is consistent with the assumption of universal access to information not artificially restricted, not blocked by authoritarian and totalitarian political regimes, such as Russia today, or North Korea for decades. According to Francis Fukuyama, the development of technology at the end of the twentieth century has greatly benefited liberal democracy. This is not

Therefore, it is not surprising that there is the tendency to strengthen cybersecurity, to form procedures of protective mechanisms against interference with sensitive information processing networks necessary for the functioning of institutional elements of the state. In general, the scope of risk has greatly increased through the development of the digital infosphere and consequently spawned the need for the dynamic development of cybersecurity. The concept of national cybersecurity is defined among others in the Republic of Poland's Cybersecurity Doctrine from 2015: Cybersecurity is the process of ensuring secure functioning in cyberspace of the state as a whole, its structures, natural persons, and legal entities, including entrepreneurs and other entities without legal personality, as well as information and telecommunications technology systems and information resources at their disposal in the global cyberspace[12]. The growing importance of cyberspace and cybersecurity strategies is reflected in the 2020 National Security Strategy of the Republic of Poland, where one of the main tasks of the state is to increase the level of resilience to cyber threats and to increase the level of protection of information in the public, military, private sector, and to promote knowledge and good practices that enable citizens to better protecţ their information[13].

Cyberspace and the closely related category of cybersecurity are setting new parameters for risk in late modernity. This is another space vulnerable to threats, and it is all the more important the more broadly it affects not only large global economic and political elites, but the particular human being using both modern technology and, above all, the existing artifacts of technology, energy receipt and other elements that are highly digitized. In reflecting on the risks accompanying the dynamics of the expansion of the ICT space, it is worth emphasizing that each additional parameter of this risk, in this case, cyberspace, dramatically increases the probability of negative events (threats). Ulrich Beck emphasizes that risk is pervasive. It connects things that are distant from each other in content, space, and time into a threatening relationship. Dealing with risk forces an all-encompassing view that is not subject to distinctions between theory and practice, does not fall within disciplinary boundaries

because technology as such promotes political freedom and equality, but because the areas of technology developed at the end of the twentieth century (especially those related to information) were among the technologies of freedom, F. Fukuyama, *Koniec człowieka*, Kraków 2002, p. 29.

12 *Doktryna cyberbezpieczeństwa RP*, Warszawa 2015, p. 7.

13 *Strategia bezpieczeństwa narodowego RP*, Warszawa 2020, p. 20.

and transcends specialized expertise[14]. Risk, therefore, involves the broader dimension of threats implied by holistically understood disruptions to the proper (consistent with the original peace and freedom tenets) functioning of cyberspace. It should be assumed that the digital infosphere will continue to undergo dynamic modernization processes, which will consequently result in the adequate development of methods and means of shaping cybersecurity.

Summarizing the above reflection, it is worth emphasizing that cyberspace is exposed to the impact of many threats and dangers, but the greatest threat in my opinion is the ideologization of production, processing, and transmission of information, i.e. its operation that will be tantamount to supporting some teleologically oriented social engineering for the needs of narrow political (economic) interest groups[15]. The significant increase in access to information, speed of its processing, automation of production systems, provision of services facilitating and accelerating routinized activities of a particular person and whole societies imply the number and level of the destructiveness of threats in disrupting and disintegrating processes occurring in cyberspace. This dimension of the threat in the area of production, transmission, and storage of information in the perspective of a broader cultural process of evolution of culture was pointed out by Teresa Grabińska. The hitherto dominant gene in the evolution of nature is gradually finding its substitute in the meme as the primary element in the replication of culture. The author states that genetics is to be replaced by memetics. This leads to far-reaching consequences parallel to the dangers in genetics from the practice of replicating genes in different combinations. Since the information contained in genes can already be manipulated and limit the randomness of the outcome of gene combinations, since knowledge of the genotype already allows for programming individuals with the desired genotype, all the more reason meme evolution will be on-demand[16].

14 U. Beck, op. cit., p. 90.

15 Social engineering harnessing the world of the digital infosphere into its cogs can lead to the generation of threats in educational processes, applications of propaganda and highly ideologized anti-humanistic content. The essence of the above threat closely correlates with the reflection on the condition of philosophy in Hegel's terms: "If theory does indeed transcend its time, if the individual constructs for himself the world as it ought to be, then this world does indeed have an existence, but only in their mind – in an overly susceptible element, which can be freely persuaded to believe in anything, G.W.F. Hegel, op. cit., p. 19.

16 T. Grabińska, *Bezpieczeństwo osoby i wspólnoty. Ochrona bytu osobowego w obliczu ideologii i praktyki transhumanizmu*, Wrocław 2018, p. 20.

Bibliography

Beck U., *Społeczeństwo ryzyka. W drodze do innej nowoczesności*, Warszawa 2002.
Floridi L., *A look into the future impact of ICT on our lives*, „The Information Society" 2007, no. 23.
Fukuyama F., *Koniec człowieka*, Kraków 2002.
Gibson W., *Neuromancer*, Poznań 1984.
Grabińska T., *Bezpieczeństwo osoby i wspólnoty. Ochrona bytu osobowego w obliczu ideologii i praktyki transhumanizmu*, Wrocław 2018.
Hahotko S., *Ryzyko ekonomiczne w działalności gospodarczej*, Bydgoszcz 2001.
Hegel G.W.F., *Zasady filozofii prawa*, Warszawa 1969.
Jarmoszko S., *Anthropology of Security. Contours of scientific identity*, Siedlce 2015.
Kulikowski J.L., *Człowiek i infosfera*, „Problemy" 1978, no. 3.
Platon, *Państwo*, Kęty 2003.
Sitarski P., *Rozmowy z cyfrowym cieniem. Model komunikacyjny rzeczywistości wirtualnej*, Kraków 2002.
Szyłkowska M., *Piąty wymiar bezpieczeństwa*, Kraków 2019.
Tatarkiewicz W., *Historia filozofii*, t. 2, Warszawa 2003.
Toynbee A.J., *Wojna i cywilizacja*, Warszawa 2002.

Cyberprzestrzeń w społeczeństwie ryzyka

Streszczenie

Dynamiczne procesy modernizacji wpłynęły na niespotykany w dziejach ilościowy i jakościowy charakter przeobrażeń społecznych. Można stwierdzić, że człowiek wkroczył w nieznane dotąd rewiry abstrakcji. Jednym jest cyberprzestrzeń o atrybutach wymykających się dotychczasowym identyfikatorom fizycznej trójwymiarowej przestrzeni. Wysoce zdynamizowane procesy postępu technologicznego usytuowały społeczeństwa w nowych wymiarach ryzyka. Prawdopodobieństwo wystąpienia pozytywnych bądź negatywnych zdarzeń zostało etiologicznie powiązane ze skutkami produkcji, przetwarzania, magazynowania i przekazywania informacji. Celem artykułu jest analiza czynników uzasadniających krystalizowanie się społeczeństwa ryzyka, którego głównym identyfikatorem jest cyberprzestrzeń, związane z nią zagrożenia oraz działania zabezpieczające w kontekście kształtowania cyberbezpieczeństwa.

Słowa kluczowe: cyberprzestrzeń, cyberbezpieczeństwo, zagrożenie, infosfera