Andrzej Pieczywok*

Cyber threats and challenges targeting man versus his education

Abstract

Modern man strongly emphasizes the need for security in all aspects of social and individual life. The content of the article concerns the threats and challenges for men in cyberspace. The author shows the relations and relationships between security and education. He devotes a lot of space to the characteristics of threats in cyberspace. Facing dynamically changing reality, the author makes the reader pay special attention to modern ways of counteracting threats generated from cyberspace. The article shows how broadly understood prevention and education in all possible stages of the human use of cyberspace are an important aspect of human life.

Key words: threats, challenges, education for safety, sense of security, human, society, prevention, teacher, the media, globalisation

* Dr hab. prof. nadzw. Andrzej Pieczywok, Uniwersytet Kazimierza Wielkiego w Bydgoszczy, e-mail: a.pieczywok@wp.pl.

Introduction

We live in times that are extremely difficult to describe, define, and unambiguously incorporate into the existing paradigm of knowledge. It is even more difficult to identify universal social mechanisms and rules that will allow, even to a small extent, to predict actions, behaviors, processes or directions of social change. The saying "we live in a culture of acceleration and information revolution" already sounds like a cliché. The social reality of the early 21st century is a challenge for many of its researchers and observers.

It is worth noting that people today create society and culture largely through symbols, patterns and stories borrowed from the media coverage. This is how everyday reality is shaped and changed . Media recipients borrow ready-made patterns and behaviour patterns, and often also language expressions, which they transpose to the reality of everyday life. Thus, they create a global identity mediated through the media, global brands and companies, as well as marketing activities. The consequence of these phenomena is experiencing reality through the media coverage. Naturally, this is not the only way to receive and experience reality, but it certainly is a very important aspect of the modern existence and perception of the world by people.

People nowadays spend a lot of time consuming the media. Everyday life of ordinary people has never been so dominated by the "reality" learned through both the old media (television, radio, press, outdoor advertising) as well the new ones (global information and telecommunication network). Therefore, the paradox of the modern media is that as a result of the excess information taken out of context and as a result fascination with the extreme and the unique, people feel lost, and their actual, real knowledge of the world is getting poorer. Instead of increasing his knowledge of the world *and* events, a man loses orientation and ability to objectively assess facts.

The development of communication technologies, such as mobile communications and the internet, has caused major changes in the functioning of societies. It contributed to the creation of a new framework for the organization of human activities in individual, collective and global dimensions[1].

1 W przedmiocie nowych technologii komunikacyjnych i zagrożeń z nimi związanych zob. szerzej: K. Chałubińska-Jentkiewicz, M. Karpiuk, *Prawo nowych technologii. Wybrane zagadnienia*, Warszawa 2015; M. Karpiuk, K. Chałubińska-Jentkiewicz, *Prawo bezpieczeństwa*

Computers streamline and make it easier for people to do any job, and the internet offers inexhaustible abundance of information on virtually any topic and connects people in a way that no other means of communication has ever provided. Thus, people with different levels of education and social status, often belonging to different cultures, using different languages, and attached to different religions can exchange thoughts and views with the help of the internet.

Broadly understood cyberspace[2] is not only a place where people work, gain knowledge, communicate with each other, and seek entertainment. It has also become a place where people are exposed to various threats.

Education is therefore one of the basic ways of developing security in cyberspace for humans and it affects their attitudes, values, messages and skills necessary to prevent threats, cope with emergencies and remove their effects. The conclusion is that it is through education, based however on a new paradigm, learning the ways and opportunities to acquire knowledge necessary for good functioning in a variable and risk-stressed reality is a way to a better knowledge and understanding of cyberspace.

Education can be defined as all processes that aim to change people, especially children and young people, according to the ideals and educational goals prevailing in a given society[3]. On the one hand, education is a factor in shaping human identity, and on the other, an indispensable creative condition for man's natural development. Depending on the theoretical premises and socio-political conditions, education is treated as: a process of human permanent life-long learning: the right and, at the same time, civic duty of a human and a social imperative; an instrument of political power to meet specific social, political party-related, union, national, cultural interests and goals; the area of social self-regulation, the main factor in the development of human capital, the quality of life of societies or civilization: a type of symbolic

informacyjnego, Warszawa 2015; K. Chałubińska-Jentkiewicz, M. Karpiuk, *Informacja i informatyzacja w administracji publicznej*, Warszawa 2015.

2 Tym terminem określa się zwykle ogół narzędzi sprzętowych i programowych związanych z technikami gromadzenia, przetwarzania, przesyłania i udostępniania informacji, wykorzystywanych przez ludzi do pozyskiwania wiedzy oraz do komunikacji z innymi ludźmi. ##This term is usually used to describe all hardware and software tools related to techniques for gathering, processing, transmitting and sharing information used by people to acquire knowledge and to communicate with other people. ##Najważniejszym, chociaż nie jedynym, składnikiem cyberprzestrzeni jest obecnie internet. The most important, though not the only, component of cyberspace is currently the internet.

3 W. Okoń, *Nowy słownik pedagogiczny*, Warszawa 2012, s. 44.

violence imposing the culture of the dominant group on the representatives of other social groups, thus, the factor of social stratification, which generates mechanisms and opportunities for social promotion as well as selection and marginalization; a "screen of culture" explaining the complexity of its field of meanings and symbols; type of a normative discourse, presenting particular mental perspective, enabling one to take sides with world-view, ideological or moral conflicts[4].

Relationships between cyberspace security and education can be described at different levels that are interrelated. The starting point is the importance of security of the individual (personal security). Shaping of a man in the education process - regardless of whether it is institutionalized (school, police, fire, city, army, workplace, etc.) or natural (in the family, in the closer and more distant social environment) or by self-education – is aimed at helping a human individual to know and understand himself, to know and understand the world of cyberspace surrounding him, to develop his own abilities and interests, to shape his own character, worldview, and attitudes towards himself and cyberspace.

Cyber security is one of the elements of the security system of a state. Nowadays it occupies an important role within this system and is a dynamically developing field[5].

4 B. Suchodolski, S. Mazur, *Edukacja dla bezpieczeństwa. Materiały międzynarodowej konferencji naukowej*, Katowice 2015, s. 26.

5 W przedmiocie bezpieczeństwa, w tym bezpieczeństwa państwa, zob. szerzej: M. Czuryk, K. Dunaj, M. Karpiuk, K. Prokop, *Bezpieczeństwo państwa. Zagadnienia prawne i administracyjne*, Olsztyn 2016; M. Karpiuk, K. Prokop, P. Sobczyk, *Ograniczenie korzystania z wolności i praw człowieka i obywatela ze względu na bezpieczeństwo państwa i porządek publiczny*, Siedlce 2017; M. Karpiuk, *Zadania i kompetencje zespolonej administracji rządowej w sferze bezpieczeństwa narodowego Rzeczypospolitej Polskiej. Aspekty materialne i formalne*, Warszawa 2013; W. Kitler, M. Czuryk, M. Karpiuk (red.), *Aspekty prawne bezpieczeństwa narodowego RP. Część ogólna*, Warszawa 2013; M. Karpiuk, *Konstytucyjna właściwość Sejmu w zakresie bezpieczeństwa państwa*, „Studia Iuridica Lublinensia" 2017, nr 4; M. Czuryk, K. Drabik, A. Pieczywok, *Bezpieczeństwo człowieka w procesie zmian społecznych, kulturowych i edukacyjnych*, Olsztyn 2018; M. Karpiuk, *Ograniczenie wolności uzewnętrzniania wyznania ze względu na bezpieczeństwo państwa i porządek publiczny*, „Przegląd Prawa Wyznaniowego" 2017, t. 9; M. Karpiuk, N. Szczęch, *Bezpieczeństwo narodowe i międzynarodowe*, Olsztyn 2017; M. Karpiuk, *Miejsce samorządu terytorialnego w przestrzeni bezpieczeństwa narodowego*, Warszawa 2014; M. Bożek, M. Karpiuk, J. Kostrubiec, *Zasady ustroju politycznego państwa*, Poznań 2012; M. Karpiuk, *Właściwość wojewody w zakresie zapewnienia bezpieczeństwa i porządku publicznego oraz zapobiegania zagrożeniu życia i zdrowia*, „Zeszyty Naukowe KUL" 2018, nr 2; M. Karpiuk, *Służba wojskowa żołnierzy zawodowych*, Olsztyn 2019.

The purpose of the article is to characterize the most important threats lurking in cyberspace and affecting the level of personal and structural security, as well as presenting ways (challenges) of using various forms and methods of security education to counteract these threats.

Cyber threats targeting man

Unfortunately, as cyberspace becomes a virtual reflection of the physical reality, negative forms of human activity penetrate it as well. Created to enable scientific cooperation, the internet network gives a great sense of anonymity, and it is used by criminals, terrorists, as well as some countries to conduct illegal activities or aggression against other entities.

Threats related to cyberspace concern the possibility of information theft (which exposes the robbed site to losses), the possibility of intentional and illegal change of information (which disturbs this sphere of professional or private activity that depends on the accuracy and timeliness of information which has changed), the possibility of limiting access to information up to and including complete blocking (which may paralyze certain spheres of action with sometimes catastrophic consequences), etc. The number of threats to which every cyberspace user may be exposed is very large, and the scale of their harmfulness is constantly increasing due to the phenomenon of increasing migration to cyberspace, so, in order to give further considerations a more specific dimension, we will briefly assess the scale of this migration.

Generally, the source of threats in cyberspace can be technology or people. The threats posed by the technology are obviously serious, because a computer failure can disable the activities of an important institution (for example, a bank), depriving it of the expected profits and prestige.

In any IT system, even after a short time of its operation, a situation arises that the data stored in the computer's memory is worth much more than the computer alone. Meanwhile, this data may be lost due to a technical failure (physical damage to the disk), due to a faulty software or due to the erroneous actions of people operating the system.

Human-generated damage and threats in cyberspace arise from a variety of reasons. The most important of them include: 1) reading someone else's letters for fun; 2) testing the security of foreign systems, theft of information; 3) understanding the strategic secrets of competitors; 4) willingness to improve one's own image and prestige; 5) embezzlement of the company

money; 6) revenge for getting laid off; 7) interception of credit card numbers; 8) getting to know military and industrial secrets.

To describe the conflict situation involving net work organizations, the name "network war", defined as "emerging form of social conflict (and crime), less intense than traditional armed struggle, in which protagonists use network forms of organizations and related doctrines, strategies and technologies adapted to the information age"[6] has been employed. As B. Bolechów emphasizes: "characteristic for the conflicts fought by networks is the blurring of divisions, which hierarchical structures generally consider to be very important. The boundaries between what is external and internal, what is legal and illegal, criminal and military, related to war and peace, private and public are becoming less clear. Similarly, the border between defensive and offensive actions becomes blurred (the network actors may, for example, attack in the name of a defense or, defending at the strategic level, attack at the tactical level), or between violence and influence (cyber terrorism is such a border phenomenon – it seems to be more connected with disruptive rather than destructive actions). Blurring borders may cause helplessness and paralysis of traditional hierarchical structures, in which areas of competence are determined according to clear divisions. Meanwhile, the opponent (in addition to functioning on a transnational level) also operates in the internal "gray areas", in which the competences of individual hierarchical structures overlap or are not included, which leads to a clinch or competence gap, respectively"[7].

The internet creates new communication possibilities and is the pillar of the modern network society. It provides its users with opportunities: creating networks, creating social relations, expressing opinions, creating social movements, managing projects. At the same time, it also creates new challenges related to freedom, information processing, forms of employment, and possible exclusion from the network. Network society influences various areas of human life – among some it raises fear and questions about education, employment, lifestyles, social inequalities, while others see it as an opportunity

6 J. Arguilla, D. Ronfeldt, *The Aduent of Netwar* [w:] J. Arguilla, D. Ronfeldt (red.), *Networks and Netwars. The Future of Terror, Crime and Militancy*, Santa Monica 2001, s. 9.

7 B. Bolechów, *Sieci przeciwko hierarchiom – wyzwania dla suwerenności państw* [w:] Z. Leszczyński, S. Sadowski (red.), *Suwerenność państwa we współczesnych stosunkach międzynarodowych*, Warszawa 2005, s. 165.

and hope for better organization of their own lives. Network society raises new challenges people have to confront.

Cyberspace is also used by terrorists as a tool for conducting politically motivated activities. Due to controversy and problems with a clear definition of the concept of cyberterrorism, it is difficult to unequivocally classify specific examples of attacks as the effect of terrorist activities in cyberspace. Many incidents attributed to terrorists may be a form of vandalism, covertly sponsored or secretly accepted by the state, which is difficult to prove.

Emerging new grounds of cyberterrorism are primarily the result of the evolution of conflicts from traditional and industrial ones to the conflicts of the post-industrial era, in which the trigger is not so much frustration arising out of the lack of access to material goods, but rather the issues of participation in the increasingly more important pool of social goods- the new participants, primarily groups of professionals are their feature.

Terrorist attacks on the internet, hacker attempts to intercept data or block websites, and other constantly evolving ICT activities aiming at depriving control of or taking over the information seem to be potentially real. Does this mean that in the near future the e-mail bomb will be a greater threat than conventional weapons, and cyberwar will become the greatest danger to the global village? In the face of globalization, cyberspace protection has become one of the basic strategic goals in the field of each country's security. In the age of free flow of people, goods, information and capital – the security of a democratic state depends on the development of mechanisms to effectively prevent and combat threats to the security of cyberspace. It is necessary to develop national solutions in a coordinated way to prevent and combat emerging threats, in particular to respond quickly and efficiently to attacks directed against systems, ICT networks and services offered on the web or services which use it.

The need for qualified staff that can effectively fight the ever-changing forms of activities in cyberspace deserves to be emphasized. Over the next few years, the importance of the information environment and security in this area will definitely grow and become one of the priorities in adjusting mechanisms ensuring national security.

Challenges of security education in the area of cyberspace

In connection to contemporary threats, there appears a tendency outlined by T. Borowska, which refers to the needs of the educational preparation of the human individual to deal with various threats, mainly through the development of his ability to create his own existence. The author claims that moral, cognitive and emotional resources can have creative power, which, thanks to education, may be acquired by "homo construens – a building man"[8]. The core of these resources are values, especially freedom and responsibility, allowing the "building man" to go beyond the boundaries of his own life in the conditions of threats arising from both the real world (stress) as well as the world of illusion created by the technical media. The illusory world of techno culture is according to T. Borowska one of the main sources of threats and stress, causing negative human reactions and having a destructive effect on all areas of his psychosocial functioning. This especially concerns anxiety, stress and various emotional disorders[9].

Education for safety in cyberspace should consist in: defense training for managerial staff, departmental training and general defense training for the entire society. Due to the objective occasional occurrence of emergencies, modern countries establish universal rescue systems. Such systems are common for the times of peace and war. The base of the systems are functioning rescue services. Concepts are prepared for managing the state and individual regions in a situation of crisis.

In individual areas of security in cyberspace, it is necessary to appoint leaders and institutions specializing in the accumulation of knowledge (theoretical and practical) in a given scope and coordination of activities of all the elements of the defense and protection subsystem. This applies in particular to: 1) combating terrorism, including monitoring international terrorism, general and specific prevention on the country's territory, protection of critical infrastructure, training of units intended to actively combat terrorist

8 T. Borowska, *„Homo construens" – człowiek budujący. Edukacyjne przygotowanie do radzenia sobie z różnymi zagrożeniami* [w:] J. Gnitecki, J. Rutkowiak (red.), *Pedagogika i edukacja wobec nadziei i zagrożeń współczesności. Materiały z III Ogólnopolskiego Zjazdu Pedagogicznego*, Warszawa–Poznań 1999, s. 351.

9 Zob. T. Borowska, *Następstwa zagrożeń występujących w życiu człowieka. Zamówienia składane edukacji wynikające z eksploracji współczesnej psychiatrii oraz psychologii* [w:] A. Siemak-Tylikowska, H. Kwiatkowska, S.M. Kwiatkowski (red.), *Edukacja nauczycielska w perspektywie wymagań zmieniającego się świata*, Warszawa 1998.

acts, as well as methods and procedures for preparing the population in the event of an act of terrorism. This requires establishment of a new act on combating terrorism; 2) combating organized crime, with a precise definition of the leading role of the National Security Bureau in the execution of this task. Today, there exist areas of crime in which almost all entities are interested.

It is necessary to establish a public-private cooperation platform for combating cybercrime, as well as to develop (change) the legal regulations specifying the obligations and powers of its members, to indicate sources of financing, to determine the rules for the national and international cooperation (interinstitutional and cross-border approach), including assessment of the amount of data processed and an indication of technical solutions for this platform.

It seems reasonable to specify the methodology and clear criteria for the selection of topics in scientific and research work in the field of security in cyberspace. A database of experts and research centers should be created which have the potential and resources to support the activities of entities responsible for security in cyberspace with their knowledge.

Education for security in cyberspace consists in numerous cognitive and empirical areas subject to many analyses. These are didactic and educational processes covering education and upbringing as well as broadly understood education, aiming at proper preparation of young people and adults for threat situations from cyberspace. Challenges and threats are listed as the main problem (research) areas, as well as subjective and objective security structure. New areas are also emerging in research in the area of education for security – including: determining the nature and legitimacy of respecting the human tolerance to risk and uncertainty; shaping and developing the human ability to work on anxiety and fear; building skills in dealing with one's own and other people's emotions; broadening the perspective of a person involved and exposed to threats.

The structural arrangement and organisation of institutions which directly affect education for security also require changes. These changes should mainly concern normative and organisational issues in the field of cooperation and removal of the effects of threats. It seems appropriate to start from constitutional foundations and security strategies concerning social needs.

The media should systematically participate in raising public awareness in the field of security, existing threats and methods to prevent them. Due to the widespread and common access of recipients to public television, it

is necessary to conduct educational and preventive programs utilising to promotie knowledge about security.

Education for safety should be a continuous process aiming at the most comprehensive development of personality and general mental fitness. An individual, improving his personality by deepening knowledge, fulfills himself as a human person. Knowledge, skills as well as his moral and spiritual values are values in themselves related to the realisation of his potential.

Many educators, including educators in the area of safety, give consideration to a model of the 21st century man. They draw attention to the need to develop the characteristics of the individual and to realize their ambitions in a way that does not harm the society. Hence, individual and social development is needed – it is a modern education model that should have many features, including: 1) people (youth, adults) being educated in a modern way, that are being educated for the future; 2) that are able to solve problematic tasks; 3) that can counteract all threats; 4) that can direct the development of their personality; 5) that would be able to use their knowledge in the near and distant future.

Education for the safety of modern man must be based on universal, national, social and personal values. From this arises the need to defend peace, to protect the natural environment, and to strive to adhere to certain principles in one's life. It should be noted that the hierarchy of values has been shaken recently and the life goals and priorities of many citizens have changed. The current customary and even legal norms are questioned and new forms of social dysfunctionalities are developing. It is worth to pay attention to the praxeology of education for security.

Greater emphasis should be placed on developing young people's ability to recognize the wide-ranging threats and dangers of cyberspace around them.

School education should include time and space for shaping young people's awareness of the possibility of cyber-terrorist threats. Educational institutions should focus on providing reliable knowledge about threats in cyberspace, shaping the attitude of civic vigilance, showing a broad context of security considerations.

The perspective of multilateral education for safety is clearly being developed, and its main subject is the complex process of human development that occurs under the influence of education, and not only school teaching and learning. Reflections on human development concern both the development of the individuals subjected to education and the development of the entire – young and old – generation, in a specific way affecting the development and progress in the society's life.

While analyzing the discussed threats, it is easy to see that information resources and elements of Poland's ICT infrastructure are subject to the same trends as cyberspace at the global level. Along with the progressing computerization of the state, it is necessary to create effective preventive, technical, organisational and legal solutions to protect its citizens.

To achieve these goals, it is necessary to take multi-level actions requiring the cooperation of all interested parties. First of all, appropriate legal norms should be ensured, allowing the effective operation of the state and its institutions in the field of cyberspace security.

Technical issues are another area that requires action. Ensuring cyberspace security will not be possible without developing early warning systems for attacks, implementing additional preventive solutions and special protection for key ICT systems, combined with exercises to assess the resistance of this infrastructure to cyber attacks.

Ensuring the security of cyberspace will not be possible without the involvement of the widest possible group of global network users who, aware of the dangers, will be able to contribute to the protection of this environment. It is necessary to train ICT security specialists and clerical staff consistently.

Bibliography

Arguilla J., Ronfeldt D., *The Aduent of Netwar* [w:] J. Arguilla, D. Ronfeldt (red.), *Networks and Netwars. The Future of Terror, Crime and Militancy*, Santa Monica 2001.

Bolechów B., *Sieci przeciwko hierarchiom – wyzwania dla suwerenności państw* [w:] Z. Leszczyński, S. Sadowski (red.), *Suwerenność państwa we współczesnych stosunkach międzynarodowych*, Warszawa 2005.

Borowska T., *„Homo construens" – człowiek budujący. Edukacyjne przygotowanie do radzenia sobie z różnymi zagrożeniami* [w:] J. Gnitecki, J. Rutkowiak (red.), *Pedagogika i edukacja wobec nadziei i zagrożeń współczesności. Materiały z III Ogólnopolskiego Zjazdu Pedagogicznego*, Warszawa–Poznań 1999.

Borowska T., *Następstwa zagrożeń występujących w życiu człowieka. Zamówienia składane edukacji wynikające z eksploracji współczesnej psychiatrii oraz psychologii* [w:] A. Siemak-Tylikowska, H. Kwiatkowska, S.M. Kwiatkowski (red.), *Edukacja nauczycielska w perspektywie wymagań zmieniającego się świata*, Warszawa 1998.

Bożek M., Karpiuk M., Kostrubiec J., *Zasady ustroju politycznego państwa*, Poznań 2012.

Chałubińska-Jentkiewicz K., Karpiuk M., *Informacja i informatyzacja w administracji publicznej*, Warszawa 2015.

Chałubińska-Jentkiewicz K., Karpiuk M., *Prawo nowych technologii. Wybrane zagadnienia*, Warszawa 2015.

Czuryk M., Drabik K., Pieczywok A., *Bezpieczeństwo człowieka w procesie zmian społecznych, kulturowych i edukacyjnych*, Olsztyn 2018.

Czuryk M., Dunaj K., Karpiuk M., Prokop K., *Bezpieczeństwo państwa. Zagadnienia prawne i administracyjne*, Olsztyn 2016.

Karpiuk M., *Konstytucyjna właściwość Sejmu w zakresie bezpieczeństwa państwa*, „Studia Iuridica Lublinensia" 2017, nr 4.

Karpiuk M., *Miejsce samorządu terytorialnego w przestrzeni bezpieczeństwa narodowego*, Warszawa 2014.
Karpiuk M., *Ograniczenie wolności uzewnętrzniania wyznania ze względu na bezpieczeństwo państwa i porządek publiczny*, „Przegląd Prawa Wyznaniowego" 2017, t. 9.
Karpiuk M., *Służba wojskowa żołnierzy zawodowych*, Olsztyn 2019.
Karpiuk M., *Właściwość wojewody w zakresie zapewnienia bezpieczeństwa i porządku publicznego oraz zapobiegania zagrożeniu życia i zdrowia*, „Zeszyty Naukowe KUL" 2018, nr 2.
Karpiuk M., *Zadania i kompetencje zespolonej administracji rządowej w sferze bezpieczeństwa narodowego Rzeczypospolitej Polskiej. Aspekty materialne i formalne*, Warszawa 2013.
Karpiuk M., Chałubińska-Jentkiewicz K., *Prawo bezpieczeństwa informacyjnego*, Warszawa 2015.
Karpiuk M., Prokop K., Sobczyk P., *Ograniczenie korzystania z wolności i praw człowieka i obywatela ze względu na bezpieczeństwo państwa i porządek publiczny*, Siedlce 2017.
Karpiuk M., Szczęch N., *Bezpieczeństwo narodowe i międzynarodowe*, Olsztyn 2017.
Kitler W., Czuryk M., Karpiuk M. (red.), *Aspekty prawne bezpieczeństwa narodowego RP. Część ogólna*, Warszawa 2013.
Okoń W., *Nowy słownik pedagogiczny*, Warszawa 2012.
Suchodolski B., Mazur S., *Edukacja dla bezpieczeństwa. Materiały międzynarodowej konferencji naukowej*, Katowice 2015.

Zagrożenia i wyzwania człowieka w cyberprzestrzeni a jego edukacja

Streszczenie

Współczesny człowiek mocno akcentuje potrzebę bezpieczeństwa we wszystkich aspektach życia społecznego i indywidualnego. Treść artykułu dotyczy zagrożeń i wyzwań człowieka w cyberprzestrzeni. Autor pokazuje w nim związki i zależności pomiędzy bezpieczeństwem a edukacją. Wiele miejsca poświęca charakterystyce zagrożeń w cyberprzestrzeni. Wobec dynamicznie zmieniającej się rzeczywistości, szczególną uwagę autor nakazuje zwrócić na nowoczesne sposoby przeciwdziałania zagrożeniom płynącym z cyberprzestrzeni. Teść artykułu pokazuje jak istotnym aspektem życia człowieka jest szeroko pojęta profilaktyka oraz edukacja we wszystkich możliwych etapach korzystania przez człowieka z cyberprzestrzeni.

Słowa kluczowe: zagrożenia, wyzwania, edukacja dla bezpieczeństwa, poczucie bezpieczeństwa, człowiek, społeczeństwo, profilaktyka, nauczyciel, media, globalizacja