Cybersecurity and School-age Young People – Challenges and Threats

ANDRZEJ PIECZYWOK

Abstract Cybersecurity is currently a major priority for states. The Internet is providing growing opportunities for development, but it can also lead to risky situations. As the Web continues to expand, people are more likely to be exposed to threats due to inadequate security or the inappropriate use of resources online. State-of-the-art digital media and interactive information and communications technology – all of which constitute cyberspace and the virtual world – pose many threats for school-age young people. They are dynamic and widespread, and have a global dimension. It is common practice for both teachers and students to use the rich educational resources available online. Against this backdrop, it is important to investigate what causes online threats to emerge and what consequences they have, as well as to develop popular awareness towards a safe use of cyberspace.

Keywords: • cyberspace • cybersecurity • school-age young people • challenges • threats • cybereducation

CORRESPONDENCE ADDRESS: Andrzej Pieczywok, Ph.D., Dr. Habil., University Professor, Kazimierz Wielki University, Faculty of Political Sciences and Administration, Department of Security Policy, ks. J. Poniatowskiego (Street) 12, 85-671 Bydgoszcz, Poland, e-mail: a.pieczywok@wp.pl, ORCID: 0000-0002-4531-0630.

https://doi.org/10.4335/2022.1.14 ISBN 978-961-7124-10-1 (PDF)
Available online at http://www.lex-localis.press.

1 Introduction

The bulk of human activity nowadays – whether educational, social, professional or leisure – takes place in cyberspace. Professional and school lives, and most social contacts, have largely gone online. On the one hand, this creates enormous opportunities, but on the other, we need to realise that many threats are also involved. In recent years, the information-related dimension of threats has become particularly significant. The Internet, networks, information, data and cyberspace have all become critical for citizen and organisational security and knowledge, and even for the authority of states. Virtual space is very often more attractive than other environments. It allows people to meet many of their needs. Interpersonal attractiveness can grow substantially online (financial and social benefits, improved self-esteem, developing a certain identity, etc.). What counts online is closeness, the law of attraction, humour, civility and mutual sympathy. Indeed, virtual communication clearly has many advantages: anonymity, wide reach, imagination, etc. School-age young people are fairly active on social media. It is worth noting that the main idea behind these sites is to allow users to stay in contact with their friends and relatives, or to make new acquaintances, as well as to share certain information with large groups of people. Sometimes it is difficult to maintain privacy. Social media sites are a real world for many young people. Moreover, they are an ever-changing space in which young people can express their identity and establish relations with others, often from different countries (Kowalczuk, 2009: 25). Social media foster their need for being part of a group, for belonging, being active, establishing their presence and promoting themselves. Young people, in particular, adolescents, tend to have a strong desire to express their views. Through social media sites, they can engage in dialogue and share interesting information – i.e. communication that satisfies their sense of agency and fosters their creative achievements and cause-and-effect thinking.

It is worth noting that cybersecurity means the resilience of information systems against actions which compromise the confidentiality, integrity, availability and authenticity of processed data, or the related services provided by those information systems. The use of social media sites involves many emerging threats associated with, among others, providing sensitive information to other users (burglars, paedophiles), phishing (access to passwords and logins), identity theft, cyberstalking, talking to strangers, etc. Information technology carries with it many threats whose consequences are hidden and distant in time. It is important to be aware of the threats and to have the knowledge and skills to navigate cyberspace. School-age young people tend to believe that they know more about the Internet than adults, overestimating their online skills and ability to protect against these threats.

Cyberspace addiction is a common problem nowadays. Some compare it to alcoholism and drug addiction. Many young people struggle with computer, TV or mobile phone addictions. They lie to themselves, which makes them oblivious that they have a problem. School-age young people do not realise the underlying threats. The uncontrolled use of media often causes changes in how their body and personality function.

The Internet is the main channel for communication and source of knowledge for young people. Hence, it is critically important for them to develop critical thinking and source verification skills. With the spread of fake news and unverified information, these skills are instrumental in protecting young people against being misled or even manipulated. Knowledge acquired online is currently replacing academic knowledge gained by reading books, encyclopaedia and scientific journals. Whereas these traditional sources are highly reliable and can be trusted, the Internet is a mosaic of information, the control over and verification of which is limited. Therefore, it is critically important for them to develop critical thinking and source verification skills.

2 Main threats associated with the inappropriate use of cyberspace

Cyberspace not only opens up qualitatively new opportunities that can make life easier for people, but also involves a range of qualitatively new threats in the personal, national and even international dimensions. It can be a source of addictions, a vehicle for socially unacceptable behaviours and values, a tool of qualitatively new forms of crime, a space for terrorist activities, and an arena for cyberwarfare if seen through the lens of military threats (Pieczywok, 2017: 113).

Threats associated with the broadly defined human contact with the world of technology, and, in particular, cyberspace, have been engendered by the euphoria surrounding the new opportunities afforded by the world of media. This euphoria has caused people to become less cautious, to underappreciate, and even to consciously ignore threats. As shown by the history of human civilisation, threats are an inseparable part of the encounter with new techniques and technologies. This creates – in quantitative and qualitative terms – new needs, or generates them artificially, indirectly making survival dependent on adaptation – in terms of both broadly defined technology and at the psychological level. These technologically forced shifts may lead to outcomes that are difficult to predict – both globally and individually. As rightly noted by S. Bębas, "technological advancements have changed not only human habits, but also the way in which pathologies can manifest" (Bębas, 2013: 22).

According to M. Szydłowska, information threats are "all destructive (intentional and unintentional) acts in the form of the undesirable disclosure, distortion, modification, damage, destruction, or the disabling of the processing of, information produced, processed, stored, and sent in a specific information flow system, potentially causing a loss (Szydłowska, 2019: 22).

P. Bączek claims that, when analysing information security, the following threats should be addressed: 1) random (natural disasters, catastrophes, accidents, fires, floodings); 2) conventional (espionage, subversion, sabotage, disinformation); 3) technological (cybercrime, cyberterrorism, information warfare); 4) civil rights-related (unauthorised disclosure, information selling, breach of privacy, unlawful interference by special forces,

thwarting public transparency); 5) organisational and structural shortcomings (mishandled operations, mismanagement and poor decision-making, poor information flow, corruption) (Bączek, 2005: 71-73).

Adverse phenomena associated with the development of information technology and, by extension, cyberspace, include: 1) the decline of humanistic values – technocratic outlook on the world; 2) opportunities to manipulate people freely – to steer their consciousness; 3) difficulties adapting to an information society and addiction to technology; and 4) the spread of pathological processes associated with the use of technology, such as violence, aggression, erotica and pornography, piracy and hacking, computer addiction (Siemieniecki, 2001: 31).

Cyberspace threats are multidimensional. These do not just pertain to access to inappropriate content, but also to the risk of eye and musculoskeletal diseases, and mental diseases. Of particular concern are addictions and, increasingly, specific behaviours associated with different types of violence and aggression (in both the virtual and real world), social changes and ethical threats, as well as the decline of independent thinking and deep reflection.

Threats may come from unverified software downloaded by students and teachers, fake websites, links to malicious codes and malicious codes contained in attachments to emails offering discounts for teachers, or fake emails from IT departments. Sensitive information about students, teachers and graduates are of great value to hackers – they can demand money to decipher such information or sell it on a black market. The research results and intellectual property of educational institutions are targeted as well.

As far as education is concerned, particular dangers relate to the cognitive and intellectual sphere involving cognition and school learning, which include: cognitive threats (uniformity and/or reduction of experience), limited perception of issues, the primacy of visual over verbal, inundation with ready-to-use hypermedia information, preventing their creative shaping and use, and the inability to take rational decisions and actions (Pieczywok, 2017: 114).

Generally, cyberspace threats to school-aged young people can be divided into a number of primary areas. These include: 1) cyberspace threats: a) mental and physical health threats: eye ailments, hearing disorders, musculoskeletal ailments, wrist ailments, thumb ailments (texting), diseases of other body organs, self-destruction, self-harm, cyberspace suicide; b) moral threats: cyberpornography, online prostitution; cyberpaedophilia, cybersex, sexting, human trafficking, including for organ trade; c) socio-educational threats: cyberbullying, online violence and aggression, gambling, second life, cybersectarianism, human trafficking, including for organ trade, impaired interpersonal relationships, human functioning in the world of humanoid robots; d) chemical hazards: bigorexia, drugs online, energy drinks, new psychoactive substances; and e) infoholism and computer-game threats; as well as 2) crime and ICT security threats: a) ICT crime in

the EU; b) ICT security policy, including: - violating the integrity and confidentiality of, and disabling access to, data and computer systems; - computer crime; - crime specific to the nature of targeted information; - intellectual property crime; c) ICT crime in Poland, including: - crime against information protection, - computer hacking, - electronic eavesdropping; - unlawful destruction of information; - computer sabotage; - copyright violation, - crimes against the credibility of documents; and d) virtual financial crime. Among school-age young people, these threats can take the form of an addiction, necessitating measures to prevent, diagnose and treat threats and pathologies.

3 The cybereducational dimension of shaping attitudes in school-age young people

It can be assumed that education is a unique socio-cultural process through which humans gradually develop, mature and shape their personality. The educational system allows young people to establish social relationships and gain socio-cultural experience (Tkacz, 2008: 315).

For a long time, the aim of education was to facilitate the acquisition of certain information, skills and attitudes. Nowadays, however, its main priority is not to pass encyclopaedic information, but to shape attitudes. Accordingly, the qualities that are now fostered by education include being active, having imagination, being intellectually autonomous, and engaging in continuous education.

It is clear, then, that school education related to identifying and counteracting cyberthreats improves the effectiveness of help and support to school-age young people experiencing virtual-world problems. Thorough knowledge about the psychological mechanisms underlying addiction and co-addiction, and the ability to apply it in everyday work with students, are very important.

As human civilisation continues to develop, the educational system has no choice but to follow. Digitisation, digital teaching, mixed learning styles, cyberspace learning and mobility have all become a part of the educational routine. Nevertheless, there exist some deeply ingrained and persisting habits causing teachers to be viewed through the lens of the system as compliant cogs, deprived of any tools – a part of a mindless testing machine. Embracing these new developments while overcoming the deep-seated mindset is a challenge for teachers. Usually, however, change is not entirely possible even if there is willingness to make it.

The constantly evolving digital technology and very easy access to diverse information engender the misconception that, for instance, the Internet and e-learning are fully sufficient to teach more in less time. There is no denying, however, that the ongoing ICT revolution will force profound changes across formal and informal education, mainly in the choice of educational contents, the teaching-learning methodology, and in evaluating school performance. Media pedagogy is facing the serious challenge of actively shaping

indispensable human skills. This mainly involves improving the ability to actively and creatively participate in developing the culture of network society. School and broadly defined education will certainly come under criticism. There is no doubt, however, that teachers will manage to mould information acquired by young people from a wide range of sources into the sound knowledge they will especially need in the future (Pieczywok, 2017: 120).

Today's schools provide students with inadequate – or, to be more exact, very little – preparation to handle the emerging challenges associated with ICT threats, addiction to new technology, and cyberspace pathologies. It should be kept in mind, however, that nobody prepared teachers (educators) and parents for these new tasks. Schools lack experts and teachers capable of diagnosing issues among students exposed to cyberspace threats. For these reasons, online security and safety in the context of the threats and social pathologies is emerging as the latest and highly important educational problem and challenge for teachers. Hence, as rightly noted by J. Kopański – "preparation for the teacher profession and the continuing professional development among teachers must change to take account of the ongoing evolution in the use of media" (Kopański, 2010: 83).

It is not common for teachers and students to have adequate knowledge about the functioning of social media sites, about using the potential of the Internet, and about online safety. As online crime, addiction to the Internet, and the adverse impacts of the Internet on behaviour become a growing phenomenon, the role of media education at school is coming to the fore (Goban-Klas, 1999: 49).

Hence, providing the general public with media education is now an important challenge. Contemporary school is being profoundly influenced by the Internet, perhaps to the point of being under its dictatorship. What is interesting is that not only pupils and students but also teachers succumb to this dictatorship. For many years now – in fact, from the dawn of computers and later the Internet – education has been constantly adapting to the world of technology.

In the face of the technological advancements and increasing digitisation, there is an ever-growing need for raising awareness about cyberthreats and for education in this area among young people.

In the context of these threats, it is particularly important to provide cybereducation understood as the diagnosis, prevention, and therapy at institutions dealing with the education and socialising of school-age young people, including family, schools, media, counselling centres, foundations, organisations, etc.

It is important that school curricula incorporate instruction on cybersecurity, which is becoming one of the primary challenges of the 21st century. Cybereducation should become a permanent part of the school landscape, especially in the form of practical

classes to teach young people how to use the Internet safely. While the user is usually the weakest link in each system, cybereducation among students and teachers is still lacking. Therefore, it is important to show teachers and students what to pay attention to, what information and applications should raise suspicions, and to whom to report incidents. It is not enough to give a 15-minute talk at the beginning of the school year. What is needed is ensuring continuous cyberhygiene care.

The aim of cybereducation is to make sure young people know how to use online resources safely, where to look for help when they fall victim to cybercrime, and how to critically approach information found on the Internet.

The basic skill that young people should learn is to remain aware of how the information they share online, almost on a daily basis, can be used. For instance, pictures of them walking their dog, photos of expensive gadgets, and logging in at specific locations can help criminals determine, for one, their daily routine. Another fundamental task is to teach school-age young people to identity attempts to illegally obtain information.

Education will certainly face the challenge of adapting instruction plans to the dynamically changing landscape of threats and methods used by criminals. Caution should be at the core of students' activities online. Being careful, however, is not enough. It is fundamentally important to instil in them scepticism about sharing their sensitive data online. Everyone should also form the habit of protecting their information, and learn how to create strong passwords. While this might seem obvious, it is still common for students to use weak combinations and log in at various locations using the same identification data.

A growing number of teachers and experts are realising that the issue of cybersecurity is underestimated at schools. Cybersecurity instruction could take place during weekly class meetings, computer science classes, or as part of a dedicated subject. It should be borne in mind that lectures and routine school talks are not enough. One way to mobilise young people to explore the subject deeper would be to organise contests and practical classes for them. In fact, there are a myriad of possibilities to tackle this challenge.

Cybersecurity education should be provided as soon as children and young people gain access to digital services, preferably before they even enter the digital world, i.e. at preschool. There is a need for a wide social campaign on cybereducation and cyberhygiene. To make this happen, a multi-pronged approach should be taken by incorporating cybersecurity into the core curriculum and securing adequate funds to improve teacher competencies, among others. This would involve developing and implementing a continuous teacher development programme on using new technology, and supporting them in meeting core-curriculum requirements related to the safe use of new technology.

The combination of the teacher's professional knowledge and deep experience allied with the digital skills of students and opportunities afforded by digital devices creates a true synergy in shaping modern education and educating a generation that will change the world more consciously and responsibly. Jan Wróbel is right to claim that "in the school of the future, it is the teacher that is, or at least should be, of prime interest" (Wróbel, 2010: 67).

Routine tasks performed by teachers should be increasingly replaced with attractive computer programs, especially given the now fairly common availability of virtual lectures, modern e-learning courses, instructional games, electronic tests, educational portals, as well as digital school registers and systems designed to monitor the learning process. Indeed, for many students, a multimedia lecture is much more interesting than a regular class. Teachers are not, therefore, needed to pass knowledge, test and evaluate. Their new role involves acting as advisers, coaches, counsellors and learning experts, supporting students in difficult moments, guiding and motivating them when in doubt, and teaching them how to learn.

As new information and communication technologies and cyberspace continue to evolve, the role of teachers is changing. As well as being able to use cyberspace tools, teachers should know the threats posed by cyberspace to respond appropriately when seeing adverse cyberspace-related effects in their students. Also, in addition to passing on the latest knowledge, their role is to protect children against negative phenomena in cyberspace. In order to provide such protection, however, they need to become familiar with the origin, scale, causes and effects of these phenomena.

When providing education with the use of latest information technologies, to shape desirable attitudes in school-age young people, teachers should not only provide them with the right conditions to acquire knowledge and the practical skills to apply it, but also shape their moral qualities, such as honesty, reliability, responsibility, etc.

It is worth stressing that digital space, the virtual world and the Internet are changing the lifestyles and culture of learning of both teachers and students, as well as the way they communicate. Hence, the following should be at the core of educating the young generation as a conscious information society: 1) promoting critical attitudes towards content found in cyberspace and the ability to cull through the content; 2) forming an active attitude to cyberspace resources to make it a tool for actively influencing audiences; 3) stimulating and strengthening sensitivity to providing objective information and promoting attitudes against its distortion; and 4) passing on knowledge of cyberspace specifications and its underlying mechanisms (Trzcińska, 2006: 269).

4 Conclusion

The potential of technology and online resources, teenager habits shaped by their contact with technology and the power of teachers' expert knowledge should create a new space for learning and a new model of working. Parents and teachers will, thus, together face the challenge of implementing innovative project methods and preparing students for work.

In addition to a range of advantages, the use of cyberspace by students has a fair share of negative aspects. The threats that await us online, including, in particular, that faced by children and young people, are increasingly serious, and it is impossible to protect young users against them only by using software to block undesirable websites.

Today, the key factor in school-age young people's development is having the ability to use, analyse, creatively process and appraise information. Media digitisation has made it possible to create virtual reality, leading to a life in the so-called "simulacrum culture". This is why reflective thinking, nurturing imagination, and developing the ability to distinguish facts from fiction are important.

References:

Bączek, P. (2005) *Zagrożenia informacyjne a bezpieczeństwo państwa polskiego* (Toruń: Wydawnictwo Adam Marszałek).

Bębas, S. (2013) *Patologie społeczne w sieci* (Toruń: Wydawnictwo Edukacyjne „AKAPIT").

Goban-Klas, T. (1999) *Społeczeństwo informacyjne. Szanse, zagrożenia, wyzwania* (Warszawa: Wydawnictwo Fundacji Postępu Telekomunikacji).

Kopański, J. (2010) Kompetencje nauczyciela a cyberbezpieczeństwo ucznia, *Meritum*, 4, pp. 82-87.

Kowalczuk, P. (2009) Posługuje się myszą i klawiaturą, *Wychowawca*, 9, pp. 25-26.

Pieczywok, A. (2017) Edukacyjne wyzwania w kształtowaniu pozytywnych postaw młodzieży w cyberprzestrzeni, In: Trubalska, J. & Wojciechowski, Ł. (eds.) *Bezpieczeństwo osób w cyberprzestrzeni* (Lublin: Wydawnictwo Wyższej Szkoły Innowacji i Ekonomii), pp. 107-126.

Siemieniecki, B. (2001) *Technologia informacyjna w polskiej szkole. Stan i zadania* (Toruń: Wydawnictwo Adam Marszałek).

Szyłkowska, M. (2019) *Bezpieczeństwo informacyjne państwa. Wybrane problemy* (Toruń: \Wydawnictwo Adam Marszałek).

Tkacz, T. (2008) Formalne i prywatne funkcje przestrzeni edukacyjnej, *Nierówności Społeczne a Wzrost Gospodarczy. Uwarunkowania Instytucjonalne*, 12, pp. 315-320.

Trzcińska, M. (2006) W stronę pedagogiki mass mediów, In: Muchacka, B. (ed.) *Szkoła w nauce i praktyce edukacyjnej* (Kraków: Oficyna Wydawnicza „Impuls"), pp. 265-273.

Wróbel, J. (2010) *Nauczyciele, supermani i poczciwe niezguły* (Gdańsk: Wydawnictwo Aeropag).