STUDIA WARMIŃSKIE 59 (2022)
ISSN 0137-6624
DOI: 10.31648/sw.8331

Serhii Terepyshchyi[1]
Department of Social Philosophy, Philosophy of Education and Education Policy
National Pedagogical Dragomanov University

Anastasia Kostenko[2]
Department of Theoretical and Applied Economics
State University of Infrastructure and Technology

Mapping the Landscapes of Cybersecurity Education during the War in Ukraine 2022

[Mapowanie krajobrazów edukacji w zakresie cyberbezpieczeństwa podczas wojny na Ukrainie 2022]

Streszczenie: Media są potężną siłą w nowoczesnym społeczeństwie. Uczniowie i nauczyciele muszą rozwijać umiejętności korzystania z mediów, aby być zainteresowanymi i krytycznymi ich konsumentami. Podczas wojny na Ukrainie rozwój szkolnictwa wyższego wymaga dostosowania zasad zarządzania, metod i praktyk organizowania i prowadzenia procesów wyborczych w celu zminimalizowania problemów bezpieczeństwa w edukacji. Cyberprzestrzeń jest zarówno szansą, jak i wyzwaniem dla bezpieczeństwa i prywatności danych osobowych, a także procesu badań i uczenia się. Informacje takie, jak: dane akademickie, dane badawcze, wiedza osobista, złożone projekty urządzeń czy rysunki nieopatentowanych produktów stały się niezwykle podatne na ataki cybernetyczne. Według ekspertów i polityków należy spodziewać się, że częstotliwość i dotkliwość cyberataków będzie nadal rosła i pogrążała obszary, które w przeszłości nie były głównymi celami – chodzi tu m.in. o dane akademickie. Niniejszy artykuł wpisuje się w prace dotyczące metodologii minimalizacji problemów bezpieczeństwa w edukacji w kontekście wojny na Ukrainie w 2022 r.

Summary: The media is a powerful force in modern society. Students and teachers need to develop media literacy skills to be interested and critical consumers of the media. During the war in Ukraine, the development of higher education requires the adjustment of management principles, methods, and practices for organizing and conducting electoral processes to minimize security problems in education. Cyberspace is both an opportunity and a challenge for the security and privacy of personal data, as

[1] Serhii Terepyshchyi, Department of Social Philosophy, Philosophy of Education and Education Policy, National Pedagogical Dragomanov University, 9 Pyrogowa Str., 01601 Kyiv, Ukraine, s.o.terepyshchyi@npu.edu.ua, https://orcid.org/0000-0001-5506-0914.

[2] Anastasiia Kostenko, Department of Theoretical and Applied Economics, State University of Infrastructure and Technology , 19 Ivana Ogienko Street, Kyiv, Ukraine, kostenko84@ukr.net, https://orcid.org/0000-0001-7112-9643.

well as the research and learning process. Moreover, information such as academic data, research data, personal data, personal knowledge, complex equipment designs, and drawings for unpatented products has become extremely vulnerable to cybersecurity attacks. According to experts and politicians, the frequency and severity of cyberattacks are expected to continue to rise and plunge into areas that have not been the main targets in the past, such as academic data. This paper is a continuation of the authors work and an attempt to add the following element to the puzzle of the methodology for minimizing security issues in education in the context of the war in Ukraine in 2022.

Słowa kluczowe: cyberbezpieczeństwo; media; edukacja; wojna na Ukrainie.
Keywords: cybersecurity; media; education; war in Ukraine.

Introduction

The media is a powerful force in modern society. Internet, television, video games, magazines, and other media have a strong influence on how we see the world, and this influence often begins in childhood. To be interested and critical media consumers, students must develop media literacy skills and habits. These skills include the ability to access the media at a basic level, critically analyze them based on certain key concepts, evaluate them based on this analysis, and finally create your own media. This process of learning media literacy skills is media education, through which people become media literate – able to critically understand the nature, techniques, and impact of media messages and products. Media education recognizes and relies on the positive, creative dimensions of mass culture. It includes creating media texts and critical thinking about the media to help us navigate the increasingly complex media landscape. This landscape includes not only traditional and digital media but also popular culture texts such as toys, comics, fashion, shopping malls, theme parks, and more.

During the war in Ukraine, the development of higher education requires the adjustment of management principles, methods, and practices for organizing and conducting electoral processes in order to minimize security problems in education. In particular, Ukrainian higher education is characterized by the emergence and development of disputes and contradictions over certain aspects of the organization of education, which leads to external information flows, in particular, in the form of media attacks by the Russian Federation.

In Ukraine, there is a certain background of research on this issue. Thus, T. Belskaya, O. Kryukov considered the features of information wars and information security in the context of threats and challenges to

democracy (Belskaya T., 2019, pp. 3–11). R. Bondarenko, V. Mikhalchuk considered aspects of information security of the state and international cooperation in the development of media and information literacy and intercultural dialogue (R. Bondarenko, V. Mikhalchuk, 2021). N. Fedorova, V. Smesova studied aspects of challenges to information security of the country, issues of information wars, information security and ways to ensure it at the stage of information technology revolution (Fedorova N., Smesova V., 2020). K. Fokina-Mezentseva draws attention to the problems of information security in the global society (Fokina-Mezentseva K., 2021, pp. 61–71). The authors of this article also touched upon the problems of media literacy and information security in information warfare (Svyrydenko D., Terepyshchyi S., 2020; Terepyshchyi S., Kostenko A., 2021; Terepyshchyi S., 2021; Oleksiyenko A., Terepyshchyi S ., Gomilko O., & Svyrydenko D., 2021).

However, since February 24, 2022, when Russia's criminal, uncorrected, large-scale war against Ukraine began, the issue of security and media literacy in the educational environment has ceased to be purely academic and has become existential.

This paper is a continuation of the authors' work and an attempt to add the next element to the puzzle of the method of minimizing security problems in the field of education in the context of the war in Ukraine.

The "dark side" of digital civilization

We live in a virtual world, where not only the real way of life is reproduced, but also simulations are generated, not inferior to reality. Growing dependence on the use of social networks around the world has led to great concerns about information security. One of the drivers of social media platforms is how they bring people together around the world to interact, share content, and engage in interactions of common interest that cross geographic boundaries. Behind all these incredible achievements is the equivalence of digital crime, which threatens physical socialization. Criminals and hackers exploit the availability of a social media platform for many evil actions to harm others. "Easy access to equipment, software, and platforms to create, distribute, and provide access to fake news stories has exacerbated the problem of fake news, making for a large number of highly biased sources that are reaching the mainstream through social networks. The economics of emotion theory proposes that fake news headlines are created to evoke emotional responses in readers that will cause them to interact with the article in a way that allows the creator to make a profit

(by clicking on the link to the full article, by sharing the article, etc.)" (Horner C. et. all., 2021, p. 1039).

The field of cyber threats is constantly evolving. As new and more developed risks emerge with astonishing frequency, it is becoming clear that without proper safety oversight and labor training initiatives, educational institutions are at risk of potentially catastrophic security incidents, as "the peculiarities of higher education as a target for cyberthreats are often overlooked due to the dominance of high-profile cyber incidents as opposed to mundane, everyday threats in policymaking and academic discourses on cybersecurity" (Fouad N., 2021, p. 137).

Cyberspace is both an opportunity and a challenge for the security and privacy of personal data, as well as the research and learning process. Moreover, information such as academic data, research data, personal data, personal knowledge, complex equipment designs and drawings for not yet patented products has become extremely vulnerable to cybersecurity attacks. "The continuous and increasing cyber incidents against universities proves that the mundane, everyday threats in cybersecurity can evoke urgency without existentiality . In addition to their direct disruptive implications in the form of breaching students' and staff's privacy, interrupting learning processes, causing financial losses and intellectual property rights theft, cyber incidents against education can also ultimately lead to reputational damages, affect the potential of grants and foreign investments and erode trust in the sector at large. The likelihood of such disruptive consequences has been rising exponentially given the complex digital footprint of educational institutions, their culture of openness and their relatively limited preparedness for cybersecurity as compared with other sectors" (Fouad N., 2021, p. 154).

Modern society is largely dependent on technology in most aspects. ICT-based devices are often interdependent, and although one party is reliable and active in data protection, the inability of others to maintain confidentiality negatively affects the rest (Lee Y., 2010, p. 1928).

Researchers are concerned about the process of empowering the government to protect data through legislation and, ultimately, institutions . This means that non-breathing governments can gain illegal access to their citizens' private data, but through mining, any entity can collect people's private data for surveillance and benefit. "There has been a lot of interest recently on using data mining for counter-terrorism applications. For example, data mining can be used to detect unusual patterns, terrorist activities and fraudulent behavior. While all of these applications of data mining can benefit humans and save lives, there is also a negative side to this technology, as it could be a threat to the privacy of individuals. This is

because data mining tools are available on the web or otherwise and even naïve users can apply these tools to extract information from data stored in various databases and files and consequently violate the privacy of individuals" (Thuraisingham B., 2002, p. 3).

Media products are created by people who consciously and unconsciously choose what to include, what to exclude and how to present what is included. These decisions are based on the creators' own point of view, which will be shaped by their thoughts, assumptions and prejudices, as well as the media they have encountered. As a result, media products are never a complete picture of the real world – even the most objective documentary filmmaker has to decide which shots to use, what to cut, and where to place the camera – but we instinctively view many media products as direct representations of that. that is real.

Most media production is a business and therefore has to make a profit. In addition, the media industry belongs to a strong network of corporations that influence content and distribution. Issues of ownership and control are central – relatively few people control what we watch, read and hear in the media. Even when the media content is not for benefit – for example, videos on YouTube and are always published for benefit. "YouTube's technical affordance structure allows for the distribution of video, advertising, communication between commentators and subscribers, subscriber recruitment and retention, and community participation. It also allows for the effective collection of data that along with the advertising system can be translated into revenue. The social affordances frame practices such as community dynamics, subscriber exchange and valuation systems, competition, participatory culture, and so on. There exists a tension between those social – technical affordances and structures that serve the accumulation of social capital and those that serve the accumulation of revenue… Should a partner lose subscribers, they will go to someone else who will then be offered a partnership. Should a channel shrink or a genre go out of fashion, another will take its place and YouTube's architecture will accommodate it and get its share of cash" (Postigo H., 2016, pp. 248–149).

In addition to business and money, the media broadcast propaganda, ideological messages, glorify power, and so on. In media literacy, what or who is missing may be more important than what or who is included. These messages may be the result of conscious decisions, but more often they are the result of unconscious prejudices and unquestionable assumptions – and they can have a significant impact on what we think and believe. In particular, the StopFake initiative is worth noting: counter-propaganda weapon (Haigh M., Haigh T., & Kozak N., 2018, p. 2062).

Social media has become a major platform for business and communications, and each industry now faces a unique set of risks on social media, many of which have put organizations in the press or at the center of controversy. Whether it's blocking targeted phishing attacks, protecting corporate accounts from compromise, fighting fraud, or protecting against fraud and issuing accounts, social media security is critical to the success of today's business. Social media security is the process of analyzing dynamic social media data to protect against cybersecurity and business threats. Social media is an evolving vector of attack that many traditional media outlets do not pay attention to. "Social media are now firmly embedded in professional newsrooms, and policies and guidance within these newsrooms have evolved to include social media activities" (Duffy A., & Knight M., 2019, p. 932).

Despite advances in technology, such as the invention of virtual machines that allow all users to log on to a central computer that can be managed by information security experts, violations still occur. The advantage remains that despite any attack, a properly managed central computer can be returned in seconds. Therefore, cybersecurity has shifted its focus beyond mitigating cyber attacks; recognize that they are inevitable, and, accordingly, new policies are created that always ensure the availability of data (Boyd-Barrett O., 2015).

Cloud computing solutions have facilitated the immediate recovery of data as well as the integrity of backups, as they are mostly managed by highly specialized professionals using modern equipment and in most cases anonymous locations. Thus, virtual machines and cloud computing solutions, including isolated architectures, help to reduce the likelihood of cyber attacks more effectively in addition to professional security, continuous monitoring, automatic backup and recovery protocols, particularly in educational institutions (Lim N., Grönlund Å., Andersson A., 2015).

Cybersecurity in conditions of war

Traditionally, cybersecurity is largely associated with the software elements of computer systems. "The need for cybersecurity appeared in the early years of the digital era, when the first mainframe computers were developed. As networked computers and systems have progressively come to dominate computing and communication platforms, the volume and severity of cybercrimeshave has increased to the extent that cybersecurity is now an underpinning area of computer systems. Owing to the huge impact of cybercrime has in the economy and safety of organizations and coun-

tries, the importance of cybersecurityhas grown to such a level that it is now considered an independent discipline" (Cabaj K., Domingos D., Kotulski Z., & Respício A., 2018, p. 24).

However, recent findings have shown otherwise. On-site hardware can be made for illegitimate and secret data transmission to the manufacturer. The transfer of such data leads to the monitoring and violation of data privacy, and governments as well as private institutions must strive to ensure the security and integrity of their data . In this context, an interesting model is proposed by L. Megouache and colleagues: "The need to improve security in a multi-cloud environment has become very urgent in recent years. Although in this topic, many methods using the message authentication code had been realized but, the results of these methods are unsatisfactory and difficult to apply, which, is why the security problem remains unresolved in this environment. This article proposes a new model that provides authentication and data integrity in a distributed and interoperable environment. For that in this paper, the authors first analyze some security models used in a large and distributed environment, and then, we introduce a new model to solve security issues in this environment. Our approach consists of three steps, the first step, was to propose a private virtual network to secure the data in transit. Secondly, we used an authentication method based on data encryption, to protect the identity of the user and his data, and finally, we realize an algorithm to know the integrity of the data distributed on the various clouds of the system. The model achieves both identity authentication and the ability to inter-operate between processes running on different cloud's provider. A data integrity algorithm will be demonstrated. The results of this proposed model can efficiently and safely construct a reliable and stable system in the cross-cloud environment" (Megouache L., Zitouni A., & Djoudi M., 2020, p. 1).

According to experts and politicians, the frequency and severity of cyberattacks is expected to continue to rise and plunge into areas that have not been the main targets in the past, such as academic data. Personal data has always been the target of hackers because of the value they are given by marketing institutions and the field of social engineering (Boyd-Barrett O., 2015, p. 1030).

In conditions of war, these threats become especially relevant. Analysts suggest 5 steps to strengthen cybersecurity defenses in wake of Ukraine-Russia war:

"1. Analysis. Threat intelligence is critical in analyzing potential cyber threats. It enables organizations to evaluate the validity and impact on the organization.

2. Detection. A good cybersecurity defense requires an effective detective mechanism based on the foundational mechanism of Sysmon to allow the detection of a wide range of attacks.

3. Protection. Account control is one of the most important aspects of an organization's security. Whether petty criminals or governments, all entities utilize the strategy of gaining control of valid credentials.

4. Response. In the modern environment, it's crucial to have a centralized overview. This can be achieved by a basic log management solution or more advanced solutions, such as SIEM. A SIEM provides the ability to contextualize, evaluate, validate, and invest across multiple security controls, giving operations and response teams a much-needed health overview of an organization's IT infrastructure resulting in a quicker response to potential threats.

5. Recovery and Business Continuity. From a resilience perspective, engage, test, and run drills on the business continuity plans. Organizations should expect to be impacted and ensure that staff is trained, systems have restoration capability, and response teams have the necessary tools to recover from the impact on their IT infrastructure" (Vinogradov I., 2022).

In summary, we can say that cybersecurity in wartime is due to three main factors.

– First, it is the language that the army speaks, thinks, plans and works.

– Secondly, the army becomes a real force only when it is trained in new technologies, and it has trained fighters, who are directed not only to perform specific combat missions, but also to comprehend them.

– And, thirdly, cybersecurity covers all spheres of modern society.

Cybersecurity in education is not just one of the political slogans, but a specific field of activity that is considered in terms of military science and has some elements of professional ethics. Currently, cybersecurity covers only military education. Since the main object of cybersecurity is the army, and the technologies used in the field of military cybernetics are military cyber devices, cybersecurity, as previously thought, is a purely military affair. But given the enormous ideological and intellectual importance of education in modern life, "civilian" education should engage in this activity. Political science is the closest to the problems of cybersecurity. However, T. Herr, with colleagues ask questions: "Colleges and universities continue to expand their curricula to include cybersecurity as an explicit course of study in political science. But what is taught in a course on cybersecurity? Are syllabi deep dives into technology, broad romps through contemporary policy debates, or do they reflect a more varied disposition?" (Herr T., Laudrain A., & Smeets M., 2021, p. 503).

Moreover, in today's world of war and peace, many educators need to be taught cybersecurity, if only because of their isolation, they are the most vulnerable to such means. Teachers and scientists of all specialties are required to devote several hours a week to cybersecurity training (Cabaj K., Domingos D., Kotulski Z., & Respício A., 2018).

In the context of Russia's aggression against Ukraine and its citizens in pursuance of Putin's political will, the concept of military cybersecurity has become synonymous with the idea of civilian security. Education, especially history and language, develop citizens' civic consciousness and civil-deontic culture, ensuring effective internal and external control of citizens over the state. Cybersecurity and civic culture are different aspects of the same activity of educating citizens on the principles of medical literacy and information security.

Conclusions

A media attack should be understood as a set of external informational influences on the university community and public opinion about real or fake actions of officials, professors, and students of educational institutions, which can bring image costs for both the educational institution and the education system as a whole. An example is the frequent reports that teachers or students are pro-Russian and are in fact collaborators. Such media attacks are a factor in the emergence of real threats that can lead not only to reputational losses of an individual institution but also to the discrediting of the state.

To minimize security issues in the field of education in the context of Russia's media attacks on Ukraine, it is important to develop media literacy, information transparency, and algorithms for interacting with stakeholders. Educational institutions, due to the amount of valuable data collected and stored on their servers, as well as the ideological role in society, have been a target for hackers of the enemy, who are interested in destabilizing the situation. University leaders must choose the right security strategy, including technological and educational solutions, to protect their infrastructure from war attacks. By linking these preventive measures to the value and goals of education and science, they can attract the support of society and secure support for their long-term awareness-raising initiatives.

These examples point to the vulnerability of the information space in the field of education, especially in times of war. There is a need for security in the field of education in the context of media attacks, in particular:

– conducting media literacy courses for students and staff of educational institutions;

– increasing the level of transparency of management practices and decision-making in the industry;

– conducting periodic communications justifying the factors and reasons for making individual decisions in the industry;

– increasing the quality of communication channels in the industry.

BIBLIOGRAPHY

Belskaya Tatiana, Kryukov Alexander, 2019, *Information Wars and Information Security: Threats and Challenges for Democracy*, Herald National university civil protection Of Ukraine. Series: State management. No. 2. pp. 3–11.

Bondarenko Roman, Mikhalchuk Viktor, 2021, *Information security of the state*, Investments: practice and experience, 5, p. 95–101. [In Ukr.]

Boyd-Barrett Oliver, 2015, *Ukraine, Mainstream Media and Conflict Propagand,* Journalism Studies, 18 (8), p. 1016–1034.

Cabaj Krzysztof, Domingos Dulce, Kotulskic Zbigniew & Ana Respício, 2018, *Cybersecurity education: Evolution of the discipline and analysis of master programs,* Computers & Security , 75 , p. 24–35.

Christy Galletta Horner, Dennis Galletta, Jennifer Crawford, Abhijeet Shirsat, 2021, *Emotions: The Unexplored Fuel of Fake News on Social Media,* Journal of Management Information Systems, 38 (4), p. 1039–1066.

Duffy Andrew, Knight Megan, 2019, *Don't be stupid: The role of social media policies in journalistic boundary-setting,* Journalism Studies, 20 (7), p. 932–951.

Fedorova Natalia, Smesova Valentina, 2020, *Information security and ways to ensure it at the stage of information and technological revolution*, Black Sea Economic Studies, 57, p. 13–16.

Fokina-Mezentseva Katerina, 2021, *Information security in global society,* Bulletin Kyiv national trade and economic university, 5, p. 61–71.

Fouad Noran Shafik, 2021, *Securing higher education against cyberthreats: from an institutional risk to a national policy challenge,* Journal of Cyber Policy, 6 (2), p. 137–154.

Haigh Maria, Thomas Haigh, Nadine Kozak, 2018, *Stopping fake news: The work practices of peer-to-peer counter propaganda,* Journalism studies, 19 (14), p. 2062–2087.

Herr Trey, Arthur Laudrain, Max Smeets, 2021, *Mapping the Known Unknowns of Cybersecurity Education: A Review of Syllabi on Cyber Conflict and Security,* Journal of Political Science Education, 17 (supl), p. 503–519.

Lee Yeung Chung, 2010, *Science – Technology – Society or Technology – Society – Science? Insights from an Ancient Technology,* International Journal of Science Education, 32 (14), p. 1927–1950.

Lim Nena, Åke Grönlund, Annika Andersson, 2015, *Cloud computing: The beliefs and perceptions of Swedish school principals,* Computers & Education, 84, p. 90–100.

Megouache Leila, Abdelhafid Zitouni, Mahieddine Djoudi, 2020, *Ensuring user authentication and data integrity in a multi-cloud environment,* Human-centric Computing and Information Sciences, 10 (1), p. 1–20.

Oleksiyenko Anatoly, Terepyshchyi Serhii, Gomilko Olga, Svyrydenko Denys, 2021, *‚What Do You Mean, You Are a Refugee in Your Own Country?': Displaced Scholars and Identities in Embattled Ukraine*, European Journal of Higher Education, 11 (2), p.101–118.

Postigo Hector, 2016, *The socio-technical architecture of digital labor: Converting play into YouTube money,* New Media & Society, 18 (2), p. 332–349.

Svyrydenko Denys, Terepyshchyi Serhii, 2020, *Media Literacy and Social Responsibility of Educators in the Conditions of Information War: The Problem Statement*, Studia Warmińskie, 57, p. 75–83.

Terepyshchyi Serhii, 2021, *In Search of Peacebuilding Strategies for the Global Civilization: from "Education for War" to "Education for Peace",* Philosophy and Cosmology, 27 (27), p. 153–162.

Terepyshchyi Serhii, Kostenko Anastasiya, 2021, *Media Literacy and Information Security in Education*, Studia Warmińskie, 58, p. 133–141.

Thuraisingham Bhavani, 2002, *Data mining, national security, privacy and civil liberties*, ACM SIGKDD Explorations Newsletter, 4 (2), p. 1–5.

Vinogradov Ivan, 2022, *5 steps to strengthen cybersecurity defenses in wake of Ukraine-Russia crisis*, https://www.securitymagazine.com/articles/97393-5-steps-to-strengthen-cybersecurity-defenses-in-wake-of-ukraine-russia-crisis (22.09.2022).