EDUCATION IN THE FIELD OF CYBERSECURITY AT UNIVERSITIES IN POLAND

Wojciech Mincewicz
Faculty of Political Science and International Studies, University of Warsaw
Correspondence: w.mincewicz@uw.edu.pl

Abstract

The article characterizes the current state of development of cybersecurity education in higher education institutions in Poland. The purpose of the study is to characterize the models of cyber security education, to verify the development trends and to attempt to estimate further directions in higher education for cyber security professionals. The compiled material, obtained from publicly available databases and curricula, allowed us to formulate conclusions related to the education process itself, as well as to the confirmation of skills. A quantitative as well as qualitative analysis of the data was carried out, focused on the content of study programs. The profile of a cybersecurity graduate varies by the leading institution, as well as by the discipline under which the education is provided. Recent years show a significant increase in new majors with a social-humanities profile, which, in addition to technological issues, pay attention to the broad context of human functioning in cyberspace. An important addition to cybersecurity education, apart from formal confirmation of skills during higher education, is the certification process. This is an example of informal education, but as global experience shows, it is equally important, both from the perspective of improving specialized skills and as a formal requirement in the recruitment and employment search process.

Keywords: cyber security, Internet, education, higher education, education

1. Introduction

In the reality of the 21st century, the digitization of the economy and the rapid development of almost every sphere of social life, the functioning of the entire society, economy and the state keep changing. Kai-Fu Lee, one of the world leaders of research and implementation in the field of artificial intelligence, in his works formulates the thesis that all areas of human life and work, as well as the functioning of socio-political structures, are at an absolutely unique moment

DOI: 10.5604/01.3001.0053.7149
Received: 20.03.2023 Revised: 10.05.2023 Accepted: 10.05.2023
This is an open access article under the CC BY license (http://creativecommons.org/licenses/by/4.0/).

(2019). This is due to the growing spread of the Internet, which has enabled the emergence and growth of the electronic market. The Internet, especially at the time of the coronavirus pandemic, has become an indispensable tool to facilitate human communication and information exchange. At the threshold of 2023, 63.5 percent of the world's population had access to the Internet (Global Digital Report, 2022). The growth rate indicates that the reach of this medium will continue to grow, for there are about 400 million more people using the Internet each year. The steady growth indicates that the Internet is a vehicle for civilizational change in the modern world (Castells, 2001). Probably not even the industrial revolution had such an impact on people's daily life, the evolution of the social structure, as the modern technological and IT progress. The development of the Internet has been attributed a negative or positive, but invariably an important role in shaping various aspects of social reality in the realities of the third decade of the 21st century (e.g., Christopherson, 2007; Pujazon-Zazik, Park, 2010; Filipek, 2013).

Functioning online – in addition to its many benefits – invariably generates new risks. Computerization itself introduces fundamental changes that entail new security risks. One of the most important ones is the significant increase in various types of cyber threats, that is, threats associated with activity in cyberspace, which are taxonomized into three categories: cyberwarfare, cybercrime, and cyberterrorism (e.g., Brenner, 2006; Mider, 2013; Mehan, 2014). Acts that fulfil the hallmarks of violent acts in cyberspace are the domain of both individual actors (hackers acting individually), informal but organized actors (the activities of the *Internet Research Agency)* and, increasingly, state actors. An example of the latter ones, probably the least obvious, may be the actions of the Russian Federation, both historical in 2007 in Estonia and also contemporary during the full-scale February 2022 aggression against Ukraine, Belarus, or North Korea. Cyber threats cause significant disruptions to society and undermine the sense of security. They also have a significant impact on the functioning of public and private institutions. As history shows, cyber threats disrupt the production processes, the provision of public services, and as an effect adversely affect economic growth and public security. Hence, in recent years, cybersecurity has become one of the most frequently discussed topics concerning security in the broadest sense. Cybersecurity is the subject of research by subsequent representatives of the world of science, who focus on the mechanisms of threats, the analysis of their impact on socio-political processes and their perception (e.g., Lobato, Kenkel, 2015; Kumar et. al., 2016; Stępień, 2017; Hussain, Mohamed, Razali, 2020; Rydlewski, 2021). The stability of functioning and development of the information society depend on an open, reliable, and, above all, secure cyberspace.

The global cost of cybercrime in 2022 was estimated at $8.4 billion. By 2023, the cost of incidents caused by illegal online activity is envisaged to exceed $11 billion. By 2026, the annual cost of cybercrime worldwide could exceed 20 billion dollars, an increase of nearly 150 percent as compared to 2022 (Statista, 2022). Therefore, the exponentially growing impact of cybercrime on the functioning of the society makes ensuring cyber security a necessity. Investment in cyber security is experiencing growth at the three levels mentioned: citizens, businesses and states (e.g., Gordon et al., 2015; Almeida, Santos, Monteiro, 2020). The effective countering of cyber threats requires interaction and participation of various industries, governments, public participation and the academia. A significant problem in the global Internet Communication Technology (ICT) market, including cyber security, is posed by the shortage of professionals. This is one of the most significant challenges for ICT leaders, with 50% currently facing significant problems in this area. Only 7 percent of ICT decision makers globally state that hiring new specialists is easy (Salary Report, 2020). With the growing demand for specialists, it is therefore necessary to focus educational efforts on the training professionals. At a basic level, education and raising awareness of threats and security solutions is a way of protecting against cyber criminals. But the focus should be on educating specialized personnel capable of effectively countering threats. Globally, most cybersecurity curricula are based on the guidelines of the National Initiative for Cybersecurity Education (NICE), a partnership between government, academia and the private sector that aims to support the state ability to meet current and future cybersecurity education and workforce challenges through standards and best practices.

2. Methodology

In view of the diagnosed problem of employing well-qualified professionals, it seems reasonable to undertake work aimed at analyzing past trends. The objectives of this study are twofold. The first one is an attempt to characterize the adopted models of cyber security education at the higher education level that we are dealing with in Poland. The second is to check development trends and attempt to estimate further directions in higher education for cyber security professionals. The material of the analysis consists of the data collected in the RAD-on system, which is a part of the Integrated Information Network on Science and Higher Education, the largest public system in Poland in terms of the scope of data compiled. The RAD-on system is an open source for obtaining updated and structured data on scientific institutions, educational activities, as well as ongoing research. The data was subjected to quantitative as well as qualitative analysis focused on the content of study programs.

The scope of the analysis conducted for the research effort undertaken included fields of study for the keyword cyber security and all cursory ones, such as: “information security and cyber security”; “cyber democracy and development studies”; “cyberspace and social communication”; “man in cyberspace”; “computer science and cyber security”; “cyber engineering”; “IT cyber security”; “cryptology and cyber security.” The restriction to majors only, and not to specialties within a major, is related to the limitation in the collection of data on specialties, as well as the adopted framework for analysis and the possibility of achieving the set goals. Data of the system were taken in February 2023. To meet the defined objectives of the study, analyses were carried out of the study programs offered by each entity.

3. Results

Table 1. Directions of cyber security education in higher education institutions in Poland

No.	Name of the field of study	Leading institution	Level	Disciplines	Launch date
1.	Information security and cyber security	War Arts Academy	First degree studies	Security sciences (100%)	02.02.2021
			Second-degree studies		02.02.2021
2.	Cybersecurity	Wroclaw University of Science and Technology	First degree studies	Technical IT and telecommunications (100%)	23.03.2017
			Second-degree studies		05.11.2020
3.	Cybersecurity	Warsaw University of Technology	First degree studies	Technical IT and telecommunications (100%)	20.02.2019
			Second-degree studies		20.02.2023
4.	Cybersecurity	University of Economics and Humanities in Warsaw	First degree studies	Technical IT and telecommunications (22%)	30.09.2022
				Security sciences (24%)	
				Political science (54%)	
5.	Cybersecurity	AGH Stanisław Staszic University of Science and Technology in Krakow	First degree studies	Technical IT and telecommunications (100%)	12.06.2019
6.	Cyberdemocracy and development studies	Kazimierz Wielki University in Bydgoszcz	First degree studies	Economics and finance (2%)	22.06.2021
				Sociological sciences (2%)	
				Technical IT and telecommunications (8%)	
				Philosophy (3%)	
				Political science (84%)	
				Social communication and media sciences (1%)	
7.	Cyberspace and social communication	University of Finance and Law in Bielsko-Biała	First degree studies	Social communication and media sciences (100%)	19.07.2019
8.	Man in cyberspace	Cardinal Stefan Wyszyński University in Warsaw	First degree studies	Sociological sciences (21%)	28.01.2016
				Technical IT and telecommunications (15%)	
				Legal sciences (64%)	
9.	Information Technology and Cybersecurity **(studies closed)**	University of Engineering and Economics in Rzeszów	First degree studies	Technical IT and telecommunications (100%)	13.01.2016 (study major closed down in 30.09.2020)
10.	Cyberspace engineering	Pomeranian University in Słupsk	First degree studies	Technical IT and telecommunications (31%)	03.07.2018
				Security sciences (62%)	
				Social communication and media sciences (7%)	

No.	Name of the field of study	Leading institution	Level	Disciplines	Launch date
11.	It cyber security	Maria Curie-Skłodowska University in Lublin	Second-degree studies	Political science (55%)	01.10.2020
				Technical IT and telecommunications (45%)	
12.	Cryptology and cybersecurity	Military Technical Academy	First degree studies	Technical IT and telecommunications (100%)	27.02.2014
			Second-degree studies		27.02.2014
			Uniform Master studies		29.05.2019

Source: own compilation based on data from RAD-on (as on February 20, 2023).

According to data presented in Table 1, to date, cyber security education and majors are (or have been) offered at 12 universities in Poland. It is noteworthy that a significant number of majors have been launched in recent years, which demonstrates the growing need to educate cyber security specialists. Historically, the first educational facility to offer training opportunities was the Jaroslaw Dabrowski Military University of Technology, which launched its studies in 2014, both at the first and second-degree levels. From the viewpoint of assigning them to a concrete discipline, all of them have been assigned to computer science and telecommunications, thus educating specialists with a strict profile. While the science education profile remains, the following years have seen the development of majors with significant contributions from social science disciplines, mainly security science. This is due to the fact that cyber security is slowly becoming not only a technical problem, but also a social one. The observed trend indicates the interdisciplinary nature of cyber security issues and problems.

It should be noted that in 2016, a first-degree program in computer science and cyber security was offered at the School of Engineering and Economics in Rzeszow. After four years of operation as a separate field of study, it was closed. The study of cyber security became a specialization discipline offered in the computer science major. One university offers classes in English at the second-degree level (Maria Curie-Sklodowska University in Lublin), and the other ones in Polish. Four universities in Poland - the Academy of Military Art, the Wroclaw University of Technology, the Wroclaw University of Technology and the Military University of Technology offer studies at the first- and second-degree level. In the remaining cases, education is provided at the first study (bachelor or engineering) level.

An analysis of the study programs indicates that the educational models vary based on the disciplines under which education is provided. Universities that deliver teaching in the area of sciences, where graduates receive an engineering diploma (the Warsaw University of Technology, the Wroclaw University of Technology, and the Military University of Technology) focus strictly on technical issues. The curricula include subjects that allow educating professionals in data security, ICT networks and cybersecurity of critical infrastructure facilities. The subjects taught include the use of modern ICT tools in practice, the practical application of security tools and technologies and the audit of ICT networks to protect business entities and public institutions. Another aspect of education is the operation of electronic applications and services in the Internet and local networks and ICT network security solutions. The curricula also include subjects that allow students to acquire knowledge in the design of intelligent ICT systems to protect against attacks and the principles of operation of basic cryptographic tools. The issues that require students to have significant knowledge of the Internet are supplemented by the necessary and indispensable knowledge of the humanities owing to the fact that the educational programs include subjects focusing on information management systems, legal regulations related to data protection, and the functioning of national and international cybersecurity systems.

The studies, which are conducted within the disciplines of social sciences, focus on the interdisciplinary nature of the issues addressed. Cybersecurity, similarly as cyberspace itself, is an inherently complex social phenomenon; hence, the need for an expanded, holistic approach. On the basic level, in the education process students acquire knowledge and skills in the field of information, but also the necessary knowledge of law, management, politics and administration, or security science. In this case, the curricula include subjects that enable students to acquire knowledge of information and communication systems security. The expansion of the curricula and an equal emphasis on knowledge of a social nature will allow a prospective professional to effectively counter soft threats in the future, such as disinformation, propaganda, and fake news. It is equally important to understand the processes taking place in the public and legal spheres. Consequently, the studies are aimed at acquiring comprehensive knowledge in the field of security, as well as those focusing on specific aspects of cyber security or combining cyber security with other issues, e.g., cyber security management, computer networks and cyber security. Accordingly, the profile of a graduate indicates that he or she is expected to have IT competence in the analysis and design of information systems and at the same time understand the social and sociological mechanisms related to specialized knowledge and the formation of the information society and statistical data processing. In fact, the subject of study includes issues in the formation of the information society, but also administrative, criminal, and civil law.

4. Conclusions

In the information age, all key sectors of human activity such as politics, economy, business, finance, transport, infrastructure, postal service, telecommunications, medicine and science are closely dependent on information technology. Due to its global nature, governments have virtually no influence over the content appearing in cyberspace, and the censorship imposed is severely limited to a specific country, except, of course, for a total ban on access to the network. In practice, the Internet provides almost unlimited opportunities for the distribution of various ideologies and views. The advancement of information technology and with it the dependence of daily life on the Internet are leading to many new challenges and threats in cyberspace.

In the above study, the author's goal was to characterize the models of cybersecurity education at the higher education level available in Poland, and then to illustrate the development trends and attempt to estimate further directions of development. Based on the compiled material, it should be noted that among the 12 majors established in Poland, in one case after four years there was a change in the concept of conducting studies and the launch of cyber security as a specialization path within the field of study. In recent years, there has been a significant increase - at both the first and the second degree levels - of studies in cyber security at more universities in Poland. An important distinction is observed at the level of assignment of studies to the discipline that is leading within the field of study. In sciences, the focus is predominantly on the practice of operations and skills in information security and related sciences that deal with systemic solutions to information security and ICT systems. In social sciences, there is a significant addition of knowledge regarding the principles of state, society, information security systems and management at various levels of organization.

The formal education process, both in Poland and around the world, is complemented by skill certification. ICT workers (and therefore cyber security professionals) are striving to acquire professional qualifications in line with global trends. Certification in ICT is a widespread phenomenon. 85% of ICT professionals worldwide hold one of the recognized certifications (Global Knowledge, 2020). This ratio is higher in Europe, the Middle East and Africa (EMEA) and is as high as 90 percent. Certificate holders commonly believe that having a certificate enables them to do higher quality work (52 percent of respondents), increases commitment to their work (36%), efficiency speed of work (31%), reduces mistakes (15%), enables them to receive a raise (17%) or promotion (8%) and enables them to change jobs (16%) (Global Knowledge, 2020). In Poland, skills certification can be based on both international and national documents. An important complement, in addition to higher education and skills certification, is the offer of self-study. Such solutions are most often based on courses in the form of asynchronous communication, that is, the listener has access to videos and materials for self-study. Such solutions are offered most frequently by private companies, but they are also increasingly being offered by higher education institutions, which are fulfilling their social impact role in this way. One of the more widespread in Poland is HackerU, prepared by the Faculty of Mathematics and Information at Warsaw University. It is an example of informal education, but one that is widely recognized and honoured by employers.

References

1. Almeida, F., Santos, J. D., Monteiro, J.A., (2020). The challenges and opportunities in the digitalization of companies in a post-COVID-19 World. *IEEE Engineering Management Review*, *48*(3), 97–103.
2. Brenner, S.W., (2006). Cybercrime, cyberterrorism and cyberwarfare. *Revue internationale de droit pénal*, *77*(3), 453–471.
3. Castells, M., (2001). *The information age* (Vol. 98). Blackwell Publishers: Oxford.
4. Christopherson, K.M., (2007). The positive and negative implications of anonymity in Internet social interactions:"On the Internet, Nobody Knows You're a Dog". *Computers in Human Behavior*, *23*(6), 3038–3056.
5. Filipek, K., (2013). Mobilizacje społeczne, rewolucje i kontrrewolucje w środowisku Web 3.0. *Konteksty Społeczne*, no. I (1), pp. 51–61.
6. Fu Lee, K., (2018). *Inteligencja sztuczna, rewolucja prawdziwa. Chiny, USA i przyszłość świata*, K. Hejwowski (trans.), Poznań: Media Rodzina.
7. Gordon, L.A., Loeb, M.P., Lucyshyn, W., & Zhou, L., (2015). Increasing cybersecurity investments in private sector firms. *Journal of Cybersecurity*, *1*(1), 3–17.
8. Global Digital Raport. (2022). *Digital in 2022: Global Internet Use Accelerates.* Accessed: https://datareportal.com/reports/digital-2022-global-overview-report [20.02.2023].
9. Global Knowledge. (2020*). IT Skills and Salary Report*, Accessed: https://www.globalknowledge.com/us-en/content/salary-report/it-skills-and-salary-report/#gref [15.02.2023].
10. Hussain, A., Mohamed, A., & Razali, S., (2020). A review on cybersecurity: Challenges & emerging threats. In *Proceedings of the 3rd International Conference on Networking, Information Systems & Security*, pp. 1–7.
11. Kumar, S.R., Jassi, J.S., Yadav, S.A., & Sharma, R., (2016). Data-mining a mechanism against cyber threats: A review. In *2016 International Conference on Innovation and Challenges in Cyber Security (ICICCS-INBUSH)*. IEEE, pp. 45–48.
12. Lobato, L. C., & Kenkel, K. M., (2015). Discourses of cyberspace securitization in Brazil and in the United States. *Revista Brasileira de Política Internacional*, *58*, pp. 23–43.
13. Mehan, J., (2014). *CyberWar, CyberTerror, CyberCrime and CyberActivism: An in-depth guide to the role of standards in the cybersecurity environment*. IT Governance Publishing.
14. Mider, D., (2013). Analiza pojęcia cyberterroryzmu. Próba uporządkowania chaosu. *Annales Universitatis Mariae Curie-Skłodowska, sectio K–Politologia*, 20(2), pp. 81–114.
15. Pujazon-Zazik, M., Park, M.J., (2010). To tweet, or not to tweet: gender differences and potential positive and negative health outcomes of adolescents' social internet use. *American journal of men's health*, *4*(1), 77–85.
16. Rydlewski, G., (2021). *Rządzenie w epoce informacji, cyfryzacji i sztucznej inteligencji.* Warsaw: Dom Wydawniczy i Handlowy Elipsa.
17. Salaryreport. (2020). *2020 IT Skills and Salary Report*, accessed: https://go.globalknowledge.com/2020salaryreport [15.02.2023].

18. Statista. (2022). *Estimated cost of cybercrime globally 2016-2027*, accessed: https://www.statista.com/statistics/1280009/cost-cybercrime-worldwide/ [30.01.2023].
19. Stępień, A., (2017). Bezpieczeństwo w erze cyfryzacji. *Przedsiębiorczość i Zarządzanie*, *18*(5.2), pp. 83–92.

Information

The article was written as part of the conference "The crisis and the organization of internal security in the face of contemporary threats. New challenges of the digital society".

KSZTAŁCENIE W ZAKRESIE CYBERBEZPIECZEŃSTWA NA UCZELNIACH WYŻSZYCH W POLSCE

Abstrakt

W artykule scharakteryzowano aktualny stan rozwoju kształcenia w zakresie cyberbezpieczeństwa na uczelniach wyższych w Polsce. Celem opracowania jest charakterystyka modeli kształcenia w zakresie cyberbezpieczeństwa, weryfikacja trendów rozwojowych oraz próba oszacowania dalszych kierunków rozwoju szkolnictwa wyższego w zakresie cyberbezpieczeństwa. Zebrany materiał, pozyskany z ogólnodostępnych baz danych i programów nauczania, pozwolił na sformułowanie wniosków związanych z samym procesem kształcenia, jak i potwierdzeniem umiejętności w zakresie cyberbezpieczeństwa. Przeprowadzono ilościową i jakościową analizę danych, koncentrując się na treści programów studiów. Profil absolwenta cyberbezpieczeństwa różni się w zależności od wiodącej instytucji, a także dyscypliny, w ramach której prowadzone jest kształcenie. Ostatnie lata pokazują znaczący wzrost liczby nowych kierunków o profilu społeczno-humanistycznym, które oprócz kwestii technologicznych zwracają uwagę na szeroki kontekst funkcjonowania człowieka w cyberprzestrzeni. Ważnym uzupełnieniem edukacji w zakresie cyberbezpieczeństwa, poza formalnym potwierdzeniem umiejętności w trakcie studiów wyższych, jest proces certyfikacji. Jest to przykład edukacji nieformalnej, ale jak pokazuje globalne doświadczenie, jest ona równie ważna, zarówno z perspektywy doskonalenia specjalistycznych umiejętności, jak i formalnego wymogu w procesie rekrutacji i poszukiwania zatrudnienia.

Słowa kluczowe: cyberbezpieczeństwo, Internet, edukacja, szkolnictwo wyższe, edukacja