Telecommunications Policy 46 (2022) 102282

Contents lists available at ScienceDirect

Telecommunications Policy

journal homepage: www.elsevier.com/locate/telpol

Analysis of cybersecurity competencies: Recommendations for telecommunications policy

Edyta Karolina Szczepaniuk [a], Hubert Szczepaniuk [b,*]

[a] *Military University of Aviation – Lotnicza Akademia Wojskowa, Dywizjonu 303 No. 35 ST., 08-521, Dęblin, Poland*
[b] *Warsaw University of Life Sciences – SGGW, Nowoursynowska 166 ST., 02-787, Warsaw, Poland*

ARTICLE INFO

Keywords:
Cybersecurity
Competencies
Cyber hygiene
Survey research
Sustainability development
Human factors

ABSTRACT

The paper aims to analyse and assess cybersecurity competencies and define the recommended solutions to improve the human factor in cybersecurity. The article presents the results of theoretical and empirical research that were carried out in 2019–2021. The research subject constitutes one of the priorities of many countries and international organisations. Cybersecurity is one of the essential foundations for implementing the idea of sustainable development. A cybersecurity analysis using a layered structure was proposed in the theoretical part. Empirical research was conducted using a diagnostic poll method based on a survey. The presentation of the research results includes an analysis of statistical dependencies. The paper presents the research results on cybersecurity competencies in the field of threats to state cyberspace and methods of securing and protecting data. An important element of the research was to identify forms of education that can be used to achieve greater efficiency in increasing cybersecurity competencies. The result of the implementation of the research objectives was the development of recommended solutions facilitating the improvement of the human factor in the field of cybersecurity.

1. Introduction

Over the last few years, there has been a continuous development of information and communication technologies that determine the nature of changes in the modern world. Progressive computerisation and the transfer of activities to cyberspace are inherent aspects of the functioning of individuals, organisations, states and the international community. These elements have become the target of developing countries and a distinguishing feature of countries highly developed (e.g.,Appiah-Otoo & Song, 2021; Vu, Hanafizadeh, & Bohlin, 2020). Many strategic documents of global political actors recognise the need for further development of the information society, cyberspace, and new technologies (e.g., Mitomo, Fuke, & Bohlin, 2015).

The effectiveness of implementing the above assumptions, including the idea of sustainable development, depends on many factors, one of which is the need to ensure cybersecurity (e.g. Vasiu & Vasiu, 2018). The achievement of goals related to further technological progress requires ensuring the security of data and services implemented in cyberspace. According to the studies of European Union agencies, national reports and publications of commercial companies concerned with cybersecurity, the scale of incidents in cyberspace has a growing tendency (e.g., ENISA, 2019a; Europol, 2019; WEF, 2020a). Cyberspace threats are becoming more sophisticated and encompass a wide variety of attack methods and techniques. Cyberspace is, therefore, an environment of positive and negative cooperation because it not only creates conditions for broadly understood progress but is also a source or target of threats. Ensuring

* Corresponding author.
E-mail addresses: e.szczepaniuk@law.mil.pl (E.K. Szczepaniuk), hubert_szczepaniuk@sggw.edu.pl (H. Szczepaniuk).

https://doi.org/10.1016/j.telpol.2021.102282
Received 17 April 2021; Received in revised form 2 November 2021; Accepted 5 November 2021
Available online 11 November 2021
0308-5961/© 2021 The Authors. Published by Elsevier Ltd. This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/).

technological development with the simultaneous need to ensure cybersecurity is a significant challenge. This issue is reflected in the strategies and legal acts of many countries and international organisations (e.g., O.J. EU L 191/1, 19.7.2016, July 6, 2016).

Cybersecurity is an interdisciplinary issue because it requires coordinated actions in the technological, legal, organisational, procedural and social areas. At the same time, many studies recognise that the human factor is the weakest link in a cybersecurity system. The European Union Agency for Cybersecurity (ENISA) emphasises that increasing the level of skills and knowledge is an indispensable element in building society's resilience to cyberspace threats (e.g., ENISA, 2017). The need to improve competencies in the discussed area is one of the targets of many countries and international organisations. In recent years, there has been a growing interest in the issue of cyber hygiene, which allows avoiding a large number of security incidents. The analysed subject area also covers strategic research and development priorities of the European Union in the field of cybersecurity (e.g., ENISA, 2018).

The outlined context shows the need for research on cyberspace security in the social aspect. This article presents the results of theoretical and empirical research that allowed for the evaluation of competencies in the field of cybersecurity. The conducted research made it possible to identify problem areas and indicate recommended solutions to improve cybersecurity competencies in a systemic approach.

2. Methodological foundations of theoretical and empirical research on cybersecurity competencies

The research subject is competencies in the aspect of cybersecurity. In this context, it is essential to diagnose the actual condition as well as to identify the relationships and dependencies between the subject of research and cyberspace security. Due to the above, it is reasonable to detail the subject of research with the following elements (Sienkiewicz, 2013):

- identification of the **phenomenon**, i.e. the distinguished fragment of reality that constitutes the object-subject of cognition,
- definition of the **system**, i.e. a complex object in which the phenomenon is realised, or is a driving force affecting how phenomena appear;
- determination of the **process** realised in the system, i.e. an ordered set of states and/or events which constitute the cause or effect of the phenomenon;
- evaluation of the risk of **value** loss as a result of the occurrence of a threat (as an element of safety management).

The research subject described by the phenomenon, system, process and value was concretised in the research as indicated in Table 1.

The main aim of the research is to assess cybersecurity competencies and to define recommended solutions for the policy that will help to minimise the risk of threats caused by the vulnerability of the human factor.

The following objectives were defined in the research:

- explaining the essence of cybersecurity,
- determining the impact of competencies on cybersecurity,
- identifying policy challenges for cybersecurity competencies,
- analysis of the results of empirical research on cybersecurity competencies,
- developing solutions that will facilitate the raising of cybersecurity competencies.

The implementation of theoretical considerations results from the need to adopt scientifically justified criteria for assessing competencies in the field of cybersecurity. Moreover, a review of the literature in the context of the research's main aim allows for the specification of dependent and independent variables necessary to implement empirical research. It was assumed that empirical research would contribute to the identification of problem areas relating to the researched issues. As a result of the realisation of the research objectives, it is possible to develop recommended solutions to increase cybersecurity competencies.

The main research problem was formulated as the following question: What is the importance of cybersecurity competencies, and what recommendations can be made for telecommunications policy to minimise the risk of threats from human factor vulnerabilities? Based on the main research problem, areas of theoretical and empirical research as well as specific research problems have been distinguished. Table 2 shows the methods and expected effects that led to the formulation of policy recommendations.

Table 1
Specification of the research subject.

Element	Characteristics in the context of research issues
Phenomenon	- Cybersecurity competencies; - Cyberspace threats, which may arise, among others, from the vulnerability of the human factor.
System	- Cybersecurity system, one of the elements of which is the cyberspace user.
Process	- Cybersecurity management, which includes human resource management.
Value	- Security of information and services in cyberspace; - National security; - Individual security.

Source: Own work.

The specified research subject and formulated research objectives cover issues in many areas of knowledge, including technical sciences, social sciences, law, and management sciences. Therefore, a research process model appropriate for systemic analysis was adopted, which enables to perform the analysis of the phenomena holistically. In theoretical research, the literature analysis and synthesis on the subject, legal acts, and reports were used.

Empirical research was carried out using the diagnostic poll method based on a survey. The survey was conducted among 1520 respondents. The research covered respondents from the enterprise sector. The selection of the research sample was random, which was carried out based on the available database of companies. The research tool was a questionnaire in printed and electronic form. The survey questionnaire contained questions about socio-demographic characteristics and competencies in the field of cybersecurity, which covered such areas as: threats and methods of cyber-attacks, security and data protection in cyberspace, improvement of competencies in the area of cybersecurity. For the purposes of the research, it was assumed that it is justified to examine the statistical relationships between the answers provided and the socio-demographic characteristics. Random selection of the research sample made it possible to apply selected methods of statistical analysis (e.g., Singh, 2006). The presentation of the research results includes an analysis of statistical dependencies. The research used the r-Pearson correlation coefficient, the Chi-2 test of independence and the C Pearson's contingency coefficient.

Table 2
Organisation of theoretical and empirical research.

Research area	Research problems	Methods and effects
The theoretical basis of cybersecurity in the social aspect	- What is the essence of cybersecurity, and what are the elements of cybersecurity? - What is the importance of competencies and cyber hygiene in ensuring cybersecurity? - What are the policy challenges in the field of cyber hygiene?	- Analysis and synthesis of the literature on the subject. - The formulation of scientifically justified criteria for assessing cybersecurity competencies. - Determination of dependent and independent variables for empirical research. - The formulation of policy recommendations to explain the essence and definition of cybersecurity.
Threats to the state cyberspace and methods of conducting cyber attacks	- What is the respondents' knowledge of the threats to the state cyberspace? - What is the respondents' level of knowledge about methods of cyber attacks? - Is there a relationship between knowledge about threats and socio-demographic characteristics (education, age)? - Is there a relationship between knowledge of cyberattack methods and education and training?	- A diagnostic poll method based on a survey. - Analysis of statistical dependencies. - Identification of problem areas in terms of respondents' knowledge of cyber threats. - Identification of factors influencing the knowledge of respondents, which made it possible to determine the recommended solutions for the policy.
Security and data protection in cyberspace	- What data protection methods do the respondents use? - What principles of security and good practices in cyberspace are applied by the respondents? - Do the respondents show risky behaviour in cyberspace? - Do the respondents care about the protection of personal data and privacy in cyberspace? - Is there a relationship between the use of data protection methods and the level of knowledge about the risks? - Is there a relationship between attitudes and behaviour in cyberspace and training?	- A diagnostic poll method based on a survey. - Analysis of statistical dependencies. - Identification of problem areas in the field of cyber hygiene. - Identification of factors influencing cyber hygiene that enabled the definition of recommended policy solutions.
Improving cybersecurity competencies	- Do the respondents see the need to improve their cybersecurity competencies? - What content of education in the area of cybersecurity is important in the assessment of the respondents? - What are the preferred forms of education and information sources on cybersecurity? - Is there a relationship between the preferred forms of education and age?	- A diagnostic poll method based on a survey. - Analysis of statistical dependencies. - Evaluation of methods of improving competencies in the field of cyber hygiene. - Identification of factors influencing the effectiveness of improving competencies in the field of cybersecurity, which made it possible to define recommended solutions for the policy.

Source: Own study.

3. The theoretical basis of cybersecurity in the social aspect

3.1. The essence and elements of cybersecurity

There are many definitions of cyberspace security in the literature on the subject and in legal acts. Depending on the field of science and the analysed cybersecurity context, the emphasis is on the technical, legal, organisational and many other aspects. An overview of selected definitions of cybersecurity is presented in Table 3.

The interpretations presented in Table 3 take into account essential aspects related to cybersecurity and emphasise the mechanisms associated with ensuring cyberspace protection against potential threats. In technical sciences, many formal models relating to ICT security have also been developed, e.g., the Bell-LaPadula model (e.g., Bell & LaPadula, 1973), the Biba model (e.g., Biba, 1975), the Graham-Denning model (e.g., Graham & Denning, 1972), the Harrison-Ruzzo-Ullman model (e.g., Harrison, Ruzzo, & Ullman, 1976).

From the point of view of research issues, it is legitimate to analyse cybersecurity considering the social aspect of cyberspace. In this context, on a highly generalised level, the cybersecurity layers presented in Fig. 1 can be distinguished.

The strategic layer presented in Fig. 1 covers issues related to legislation, standardisation and shaping cybersecurity strategies at the international, national and individual public and private levels. Therefore, this layer has a significant impact on the organisation of a cybersecurity system, defining the principles of its functioning, and it constitutes a regulator of the rights and obligations of cyberspace users (e.g., Kosseff, 2019). The essential elements of this layer include EU institutions and bodies, EU member states institutions and bodies, standardisation organisations. Examples of achievements that have had a significant impact on cybersecurity include the Regulation on the protection of personal data (GDPR regulation) (O.J. EU L 119/1, 4.5.2016, April 27, 2016) and the Directive on measures for a high common level of security of network and information systems across the Union (NIS Directive) (O.J. EU L 191/1, 19.7.2016, July 6, 2016). The aforementioned legal acts established the principles of cybersecurity protection and obligated EU member states to develop adequate national strategies and cooperation at the EU level (e.g., Markopoulou, Papakonstantinou, & de Her, 2019). The implementation of EU solutions to the national legal order has significantly contributed to increasing cybersecurity and privacy protection (Szczepaniuk, Szczepaniuk, Rokicki, & Klepacki, 2020). The rules set out in the strategic layer affect the organisation of a cybersecurity system in public and private institutions, which includes defining the principles of human resource management and shaping education in the field of cybersecurity.

The technical layer includes a wide range of hardware and software security measures as well as physical protection measures. Currently, top-rated are, for example, antivirus programs, Firewall, IDS/IPS systems. It should be emphasised that cyberspace is an evolving and complex system because several paradigms of its development can be distinguished, related to the popularisation of next generations of the Internet and new technologies (e.g., Liu et al., 2019; Robison & Crenshaw, 2002). The popularisation of a specific technology brings about positive changes in users' quality of life or affects the optimisation of information processes in organisations. On the other hand, the development of new technologies also determines the emergence of new vulnerabilities; thus, research on the design, implementation and improvement of technical security measures is of great importance (e.g., ENISA, 2018). Relating the above considerations to the research subject, the skills of cyberspace users in the scope of the possibility of using technical security measures are of fundamental importance. An important issue is conducting scientific research on cybersecurity, a cooperation of the public and the private sector in the discussed field, and the development of departments and specialities focused on educating future cybersecurity experts.

The social layer covers cyberspace users, including their rights, duties, knowledge and skills in the field of cybersecurity. It should be emphasised that the social layer of cybersecurity can be analysed on many levels. In the literature on the subject, there are studies on various aspects of privacy protection in cyberspace (e.g., Geber, Geber, & Volkamer, 2018; Henriksen-Bulmer, Faily, & Jeary, 2019; Kim & Kim, 2018). An important point is the assessment of threats to information security that occur as a result of human error or intentional human activity. These phenomena may also apply to internal employees of an organisation (e.g., Probst, Hunkel, Dieter, & Bishop, 2010). Another area of analysis is cyberspace threats that expose cyberspace users to personal and material damage, e.g., ransomware, phishing, identity theft (e.g., Connolly & Wall, 2019; Frauenstein & Flowerday, 2020). Therefore, the main challenge is education for security and increasing users' knowledge about cybersecurity rules (e.g., Franke & Brynielsson, 2014; Person et al.,

Table 3
Selected definitions of cybersecurity.

Definition	References
The state of being protected against the criminal or unauthorised use of electronic data or the measures taken to achieve this.	Oxford Online Dictionary
Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.	NSPD-54 / HSPD-23, 2008
The protection of privacy, integrity and accessibility of data information in the cyberspace.	ISO/IEC 27032, 2012
Cybersecurity is the organisation and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights.	Craigen, Diakun-Thibault, and Purse (2014)
Cybersecurity is the protection of cyber systems against cyber threats.	Refsdal, Soulhug, & Stolen (2015)
The process of protecting information by preventing, detecting, and responding to attacks.	Stouffer et al. (2017)
Cybersecurity means the activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats;	O.J. EU L 151, 7.6.2019, April 17 (2019)

Source: Own work.

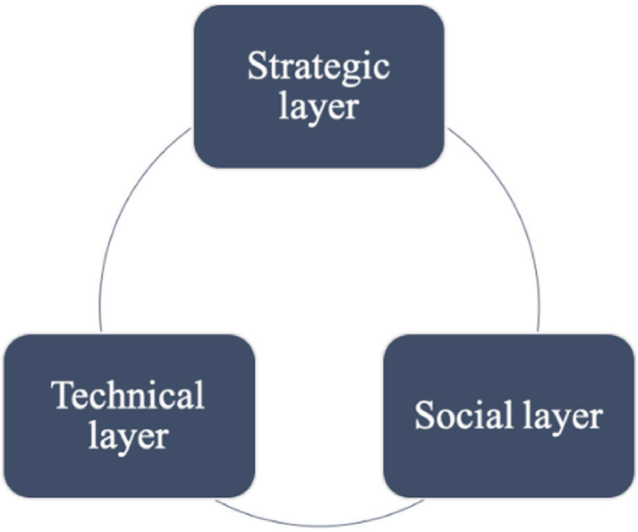

Fig. 1. Cyberspace security layers.
Source: Own work.

2017).

The strategic, technical and social layers are interrelated and interdependent. The essence of cybersecurity can be seen as a state and a process in which the elements that constitute cyberspace are characterised by "the ability to protect against current and future disruptions (threats) to the functioning or loss of certain values - the system is resistant toward threats (internal, external, accidental, intentional)" (Szczepaniuk, Szczepaniuk, Rokicki, & Klepacki, 2020).

From the point of view of research issues, it is reasonable to detail the social aspect of cybersecurity with the following requirements:

- legal documents create conditions for the organisation of a cybersecurity system, which takes into account the improvement of the human factor (including departments and specialities related to cybersecurity, shaping social awareness, standards in the field of employee training);
- the legislation provides legal protection of cyberspace users, including the protection of privacy;
- an appropriate cybersecurity organisation ensures the security of information and services at the assumed level of confidentiality, integrity, and availability;
- research and education in the field of cybersecurity is in development;
- an appropriate cybersecurity organisation minimises the risk of security incidents caused by deliberate activities of the organisation's employees;
- cyberspace users are aware of threats and are not susceptible to them,
- cyberspace users have skills in the aspect of the use of technical security measures that ensure at least the minimum-security requirements;
- the perpetrators of incidents have limited possibilities of using cyberspace to generate threats by utilising the vulnerability of the human factor.

According to the systemic approach, the improvement of a cybersecurity system is equivalent to the desired shaping of all the considered elements (e.g., Sienkiewicz, 1989). The vulnerabilities that create conditions for the appearance of a threat or a security incident may occur in the strategic, technical or social layer.

3.2. *The importance of competencies and cyber hygiene in ensuring cybersecurity*

The growing number of cyberattacks that exploit the vulnerability of the human factor determines the need to raise competencies in the area of cybersecurity. Moreover, digital competence is an essential element of implementing the idea of sustainable development (s.g, Sharma et al., 2016). ENISA underlines that raising knowledge and competencies is essential to the improvement of cybersecurity in the European Union (ENISA, 2020a). A similar position can be observed in NATO's activities, which created the Cybersecurity Collaboration Hub, to exchange experiences and training.

Competency is defined differently depending on the discipline. Moreover, within one discipline, one can also find different interpretations of a discussed category (e.g., Schoon, 2009). In the literature on the subject, some definitions link competency with the effectiveness of action in a given field. In other approaches, competencies are related to collecting many different abilities, skills, and traits (e.g., Raven & Stephenson, 2001; Szczepaniuk, 2019). The article assumes that cybersecurity competencies relate to a combination of knowledge, skills, and attitudes to ensure cybersecurity. Having competencies in the discussed area determines the effectiveness of the unit's actions in decision-making situations related to ensuring cybersecurity and minimising the risk of security incidents.

The National Institute for Standards and Technology (NIST) established the National Initiative for Cybersecurity Education (NICE), which is a forum for collaboration between government, academia and the private sector. NICE has developed the Cybersecurity Competency Model, which is an attempt to define, classify and normalise knowledge, skills and attitudes related to cybersecurity (Whitman, 2018). The model is presented as a pyramid consisting of several levels (Fig. 2).

The model presented in Fig. 2 consists of levels covering basic competencies (levels 1–3), industry competencies (levels 4–5) and higher-level competencies representing a specialisation in a given occupation. In the document specifying the model, measures and indicators for assessing specific competencies groups are distinguished additionally (Cybersecurity Competency Model, 2019). The elements included in the model may constitute a reference point for the analysis and assessment of competencies in the field of cybersecurity.

Evaluation of competencies in the context of the research issues is an essential element of ensuring cybersecurity. Many modern cyberattacks exploit the vulnerability of the human factor to cyber threats. Vulnerability analysis and threat identification are critical elements of risk management, which is the starting point for assessing and improving a cybersecurity system. Regardless of the adopted method of risk management, vulnerabilities are defects or gaps in a security system that facilitate the occurrence of a threat (e.g., Antonucci, 2017). Risk is expressed in the relationship between the threat and vulnerability and the amount of the effects caused by the occurrence of threats. The risk analysis results determine the protection requirements adopted in the form of security measures that minimise the risk (Szczepaniuk, Szczepaniuk, Rokicki, & Klepacki, 2020). Therefore, the purpose of vulnerability analysis and threat identification is to organise a system that will respond to cybersecurity challenges.

It should be emphasised that the vulnerabilities and the resulting threats may occur in all elements of cyberspace or a cybersecurity system. Therefore, the vulnerabilities that may be indicated are, among others, software, physical, infrastructural, organisational, procedural or personal vulnerabilities. Considering the elements presented in Figs. 1 and 2, Table 4 shows examples of vulnerabilities and threats in relation to the human factor.

The impact of the human factor on vulnerabilities and threats can be analysed, among others, in terms of the organisation's security or the personal security of a cyberspace user. Kraemer and Carayon proposed the Human Factor Vulnerability Analysis (HFVA) methodology, which enables the study of employees' vulnerability, including technical vulnerabilities (Kraemer & Carayon, 2003). The methodology is limited to two vulnerability categories, but it can be used to identify security vulnerabilities and analyse security breaches.

Hadlington investigated the relationship between Internet addiction, impulsiveness and human vulnerability to risky behaviour in the aspect of cybersecurity. One of the study's important findings was to show that employees' personality traits and attitudes can affect the effectiveness of involvement in cybersecurity (Hadlington, 2017).

Wang conducted a study assessing users' knowledge and behaviour in the area of cybersecurity on the example of the threat of phishing. The obtained results indicated that there is a relationship between the knowledge and the behaviour of end-users in the aspect of utilising anti-phishing solutions (Wang, 2013). Phishing also often depends on the knowledge of human attitudes and the use of human vulnerabilities (Dodge, Carver, & Ferguson, 2007).

ENISA emphasises that in the last several years, activities facilitating cybersecurity consisted mainly in the technical security of

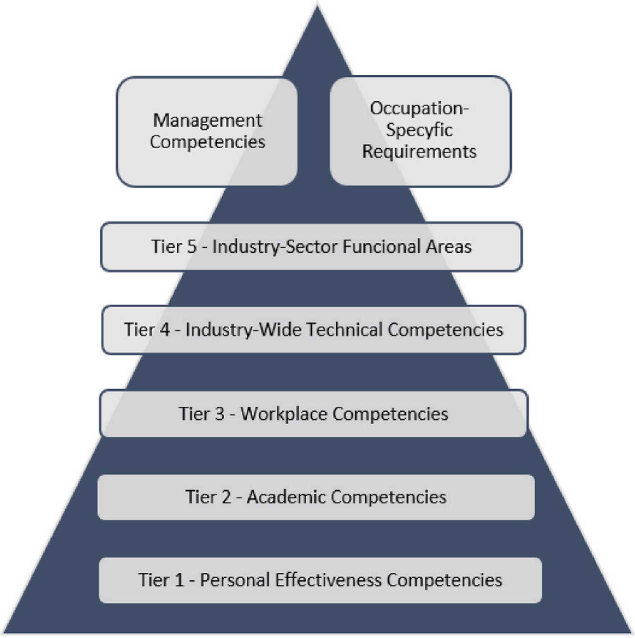
Management Competencies
Occupation-Specyfic Requirements
Tier 5 - Industry-Sector Funcional Areas
Tier 4 - Industry-Wide Technical Competencies
Tier 3 - Workplace Competencies
Tier 2 - Academic Competencies
Tier 1 - Personal Effectiveness Competencies

Fig. 2. Cybersecurity competency model.
Source: Own work based on (Whitman, 2018).

Table 4
Example of vulnerabilities and threats in relation to the human factor.

Layer	Vulnerability example	Threat example
strategic	- lack of personnel training - lack of cybersecurity education	- human error
technical	- inability to use security or data protection mechanisms in cyberspace	- infecting a computer with malware
social	- lack of awareness of the possibility of malware spreading or conscious risky actions	- phishing - ransomware

Source: Own work.

systems and devices. The importance of the human factor in the cybersecurity system was limited primarily by procedures and sanctions (ENISA, 2019b). It may have contributed to the low competencies in cyberattack prevention.

The scientific literature and initiatives of many countries and international organisations began to notice the need to improve cybersecurity competencies. In this context, the concept of “cyber hygiene” has emerged, which means knowledge and behaviour aimed at reducing risky behaviours in cyberspace (Neigal, Claypoole, Waldfoogle, Acharya, & Hancook, 2020). A proper level of cyber hygiene reduces the system’s vulnerability to threats and includes the ability to prevent a potential attack (e.g., Kalhoro, Rehman, Ponnusamy & Shaikh, 2021). Cyber hygiene refers to a set of rules and behaviours that, if followed, increase the safety of individual users and have a positive impact on an organisation.

Competencies are essential in ensuring cybersecurity. Both the lack of knowledge or the lack of appropriate skills can contribute to the occurrence of cyber threats. Cyberspace is a subject of further evolution; therefore, it is important to improve competencies to minimise the risk of threats. Promoting cyber hygiene principles can help to avoid a large number of security incidents.

3.3. Policy challenges - cybersecurity competencies

Many strategy documents and policies emphasise the importance of digital technologies for socio-economic development while respecting the Sustainable Development Goals. The World Economic Forum report indicated that the computerisation of the public and private sectors determines changes in the employment structure. Nowadays, there is a demand for an increase in digital competencies among employees (WEF, 2020b).

The effective implementation of modern technologies requires the implementation of many projects, including ensuring cybersecurity. According to some forecasts, it is estimated that the cost of cybercrime is growing by 15% annually, and by 2025 it could reach over $ 10 trillion annually (Morgan, 2021). Therefore, the issue of cybersecurity is a significant global challenge. The United

Table 5
Cybersecurity competencies - selected EU regulations.

Initiative	Characteristic
The Directive on security of network and information systems (the NIS Directive)	- The Directive sets out the obligations of the Member States to increase the overall level of cybersecurity in the EU. - The tasks of the cooperation group include the exchange of information and best practices on awareness-raising and training. - The document indicates that the national strategy for the security of network and information systems should contain guidelines relating to education, information and training programs (O.J. EU L 191/1, 19.7.2016, July 6, 2016)
The Cybersecurity Act	- The Regulation indicates that additional efforts are needed to raise citizens’ awareness of cybersecurity. - The recommended solution is to promote cyber hygiene in the Member States. - ENISA supports the Member States in raising awareness of cybersecurity. - ENISA contributes to the promotion of best practices and solutions, including in the field of cyber hygiene and digital skills, at the level of citizens, organisations and enterprises. - Public information campaigns should spread knowledge about threats such as phishing attacks, botnets, financial and banking fraud, data fraud incidents. In addition, security methods should be promoted, including multi-level authentication, encryption, anonymisation and data protection (O.J. EU L 151, 7.6.2019, April 17, 2019)
Digital Education Action Plan 2021–2027	- The document concluded that all Member States lack digital experts, including cybersecurity analysts. - The demand for e-skills will grow, and it will be necessary, among other things, competencies in the field of cybersecurity (COM/2020/0624).
The EU’s Cybersecurity Strategy for the Digital Decade	- The strategy emphasises that cybersecurity competencies are low. In addition, there is a significant shortage of cybersecurity skills among employees. - Cybersecurity competence and hygiene should underpin the digital transformation (JOIN, 2020)

Source: Own work.

Nations recommends building digital capabilities, including cybersecurity competencies (UN, 2017). At the European Union level, there is also a need to improve solutions in this area. Table 5 presents selected regulations and initiatives of the European Union concerning, among other things, cybersecurity competence.

The table above presents selected initiatives of the European Union, which emphasise that achieving an acceptable level of cybersecurity requires actions in the legal, technical, physical, and social areas. The documents indicate that the cybersecurity competencies are too low. Consequently, a significant policy challenge is the dissemination of knowledge and skills for building cybersecurity defence capabilities.

The European Union regulations have a significant impact on the legal system of the Member States. As a result of the initiatives taken, there is an improvement in the level of security of network and information systems in the Member States. Significant importance in this regard was played, among others, by detective NIS (Szczepaniuk, Szczepaniuk, Rokicki, & Klepacki, 2020). It can be assumed that the analysis of cybersecurity competencies may contribute to the identification of problem areas that will determine policy challenges in the studied area.

4. Empirical research results

Theoretical considerations lead to the conclusion that insufficient competencies in the field of cybersecurity may generate significant vulnerabilities in a security system. For empirical research, it was assumed that vulnerabilities might occur in each layer presented in Fig. 1 or Fig. 2. The relationships between the human factor and other cybersecurity system elements were examined in this context.

4.1. Threats to the state cyberspace and methods of conducting cyber attacks

The survey questionnaire formulated questions about the respondents' knowledge of threats and selected cyberattacks methods. Table 6 presents quantitative data illustrating the respondents' knowledge of threats to the state cyberspace.

According to the table above, the respondents' knowledge of threats may be insufficiently assessed. Most of the respondents are not aware of the scale of security incidents caused by the activities of the organisation's employees or social engineering. The research results also showed that many respondents do not know the specifics of such threats as cyberwar or cyber spying. Most of the respondents are aware of the threat of cyberterrorism and cybercrime and can assess the scale of the potential effects of such activities.

The analysis of the socio-demographic characteristics of the respondents and the answers provided allows us to assume that there is a relationship between education, age and knowledge of the threats to the state cyberspace. Comparing the quantitative data in individual groups of the education structure, 85% of people with an academic degree or title know the threats to the state cyberspace. Among people with higher education, 68% of respondents showed knowledge in the researched field. According to the level of knowledge, the following groups of respondents are as follows in the education structure: secondary - 22%, vocational - 13%, primary - 11%. Relating the data to the age structure of the respondents, younger people are more aware of the threats to the state cyberspace compared to older adults. The percentage distribution in individual age groups in relation to the possessed knowledge is as follows: 78% (people under 26 years of age), 75% (26–35 years), 66% (36–45 years), 37% (46–55 years), 21% (56–65 years) and 17% (people over 65). The tables below present quantitative data and percentage data in terms of knowledge about threats to the state cyberspace, taking into account the level of education (Table 7) and the age of the respondents (Table 8).

The relationship between education, age and knowledge about the risks was investigated using the r-Pearson correlation coefficient. The value of the correlation coefficient for the studied variables is presented in Table 9, while the scatter diagrams showing the correlation between the variable X and the variable Y are illustrated in Fig. 3 and Fig. 4.

The r-Pearson correlation coefficient showed a strong statistical relationship between the examined variables. In the case of the influence of education on the respondents' knowledge, the direction of the relationship is positive, which means that the higher level of one variable determines the higher level of the other one. There is a negative correlation between age and the answers given by the respondents.

The next group of questions in the survey questionnaire concerned cyberattacks and malware. Table 10 presents the respondents' knowledge in the discussed area.

The quantitative data in Table 10 shows that the respondents do not have detailed knowledge about cyberattacks in most cases. The survey questionnaires did not include a definition of individual attack methods because one of the research objectives was to evaluate

Table 6
Knowledge of respondents on threats regarding state cyberspace.

Threat	Has knowledge	Has no knowledge	Σ
actions of the organisation's employees	329	1191	1520
social engineering	281	1239	1520
cybercrime	822	698	1520
cyber spying	619	901	1520
cyberterrorism	1115	405	1520
cyberwar	597	923	1520
Σ	3763	5357	

Source: Own work.

Table 7
Knowledge regarding threats to the state cyberspace depending on the education structure of the respondents.

Variable Y: education	No. of persons	Variable X: knowledge					
		Has knowledge		Has no knowledge		Σ	
		quantity	%	quantity	%	quantity	%
primary	89	58	11	476	89	534	100
vocational	232	175	13	1217	87	1392	100
secondary	517	677	22	2425	78	3102	100
higher	613	2501	68	1777	32	3678	100
academic degree/title	69	352	85	62	15	414	100

Source: Own work.

Table 8
Knowledge about threats to the state cyberspace depending on the age structure of the respondents.

Variable Y: education	No. of persons	Variable X: knowledge					
		Has knowledge		Has no knowledge		Σ	
		quantity	%	quantity	%	quantity	%
<26	109	513	78	141	22	654	100
26–35	212	949	75	323	25	1272	100
36–45	266	1054	66	542	34	1596	100
46–55	171	379	37	647	63	1026	100
56–65	386	491	21	1825	79	2316	100
>65	376	377	17	1879	83	2256	100

Source: Own work.

Table 9
The impact of education and age on knowledge of threats – hypothesis testing.

Variable Y	Pearson's r correlation coefficient					
	Variable X: education			Variable X: age		
	Value	Strength of dependency	Direction of dependency	Value	Strength of dependency	Direction of dependency
Knowledge of threats to the state cyberspace	0,76	Strong dependency	Positive dependency	−0,77	Strong dependency	Negative dependency

Source: Own work.

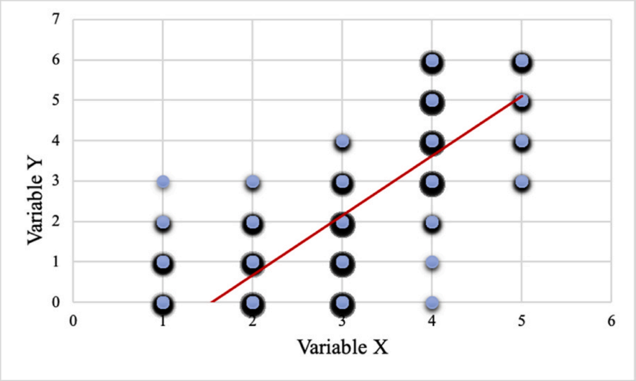

Fig. 3. Scatter diagram of variable X (education) and variable Y (knowledge about cyberspace threats in the state).
Source: Own work.

the respondents' level of knowledge. It should be emphasised that understanding the specifics of individual attacks and malware requires specialist knowledge. The analysis of the answers provided showed that most of the respondents were aware of such threats as a computer virus or a Trojan horse. The collected material indicates that most of the respondents are not aware of the remaining threats. Spoofing, SQL Injection, Redirects, Spyware, and Cryptojacking are among the least known threats.

Detailed analysis of the collected material made it possible to adopt a hypothesis that there is a relationship between knowledge of

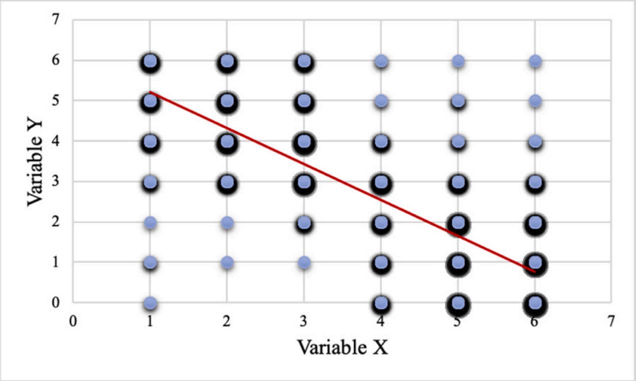

Fig. 4. Scatter diagram of variable X (age) and variable Y (knowledge about threats to state cyberspace).
Source: Own work.

Table 10
The respondents' knowledge of cyberattacks and malware.

Cyberattack	Has knowledge	Has no knowledge	Σ
Trojan horse	1009	511	1520
Computer virus	994	526	1520
Phishing	728	792	1520
DDoS attack	422	1098	1520
Botnet	398	1122	1520
Ransomware	349	1171	1520
Man in the middle	252	1268	1520
Keylogger	231	1289	1520
Cryptojacking	203	1317	1520
Spyware	191	1329	1520
Redirects	186	1334	1520
SQL Injection	174	1346	1520
Spoofing	165	1355	1520
Σ	5302	14,458	
	19,760		

Source: Own work.

cyberattacks and malware and the type of education (IT and non-IT) and the participation of the respondents in training in the field of information security (including, among others, courses or participation in classes on the discussed issues). The research results on the issues mentioned above are presented in Table 11.

Table 11
Knowledge about cyberattacks, including education and training of the respondents.

Variable Y: knowledge about threats	Variable X: education				Variable X: training, courses			
	IT		other		realised		not realised	
	has knowledge	has no knowledge	has knowledge	has no knowledge	has knowledge	has no knowledge	has knowledge	has no knowledge
Trojan horse	174	0	835	511	320	37	689	474
Virus	174	0	820	526	319	38	675	488
Phishing	174	0	554	792	321	36	407	756
DDoS attack	173	1	249	1097	287	70	135	1028
Botnet	174	0	224	1122	301	56	97	1066
Ransomware	165	9	184	1162	320	37	29	1134
Man in the middle	165	9	87	1259	205	152	47	1116
Keylogger	167	7	64	1282	178	179	53	1110
Cryptojacking	159	15	44	1302	165	192	38	1125
Spyware	169	5	22	1324	189	168	2	1161
Redirects	170	4	16	1330	172	185	14	1149
SQL Injection	171	3	3	1343	171	186	3	1160
Spoofing	162	12	3	1342	164	193	1	1162
Σ	2197	65	3105	14,393	3112	1529	2190	12,929
	19,760				19,760			

Source: Own work.

Based on the data contained in the table above, a hypothesis can be assumed that there is a relationship between knowledge about cyberattacks and malware and the acquired education. It can also be assumed that respondents' participation in courses and training in information security influences their knowledge. The adopted hypothesis was verified with the Chi-2 test. However, the dependency's strength was determined using the C Pearson's coefficient. The described dependencies are presented in Table 12.

The results of the Ch-2 test, presented in Table 12, allowed for positive verification of the formulated hypothesis. Pearson's C coefficient indicates a very strong relationship between the studied variables. Both respondents with IT education and persons participating in training in the field of information security showed greater knowledge of cyberattacks and malware.

4.2. Security and data protection in cyberspace

An important issue is the analysis of data protection methods used in cyberspace by the respondents. The survey questionnaire formulated questions about technical security and actions taken for data protection in cyberspace. The study results regarding the applied technical protections are presented in Table 13.

Referring to the above results, it can be stated that the majority of the respondents use such security measures as antivirus (86%), firewall (77%) or IDS/IPS systems (62%). A smaller proportion of the respondents use such solutions as VPN (35%), disk encryption (33%), e-mail encryption (31%), end-to-end encrypted instant messaging (24%). A small number of respondents use Tor Browser (13%), configure the Wi-Fi router to hide the SSID network (11%) and filter allowed clients by MAC address (8%).

The applied analysis of the answers provided on the security measures showed that the knowledge of the respondents about the threats to the state cyberspace influences the decision on the choice of security and data protection methods. This relationship was investigated using the r-Pearson correlation coefficient (Table 14), and it is depicted in a scatter diagram (Fig. 5).

The r-Pearson correlation coefficient's value showed a strong statistical relationship between the studied variables. In the case of the studied variables, there is a positive correlation, i.e. an increase in knowledge about threats to the cyberspace of the state affects the increase in the data protection security measures and methods used.

The empirical research also included the respondents' attitudes towards good practices or risky behaviour in cyberspace. This is because ensuring data protection is determined mainly by compliance with cyberspace security rules. Moreover, user behaviour may generate vulnerabilities that expose data and services to the loss of information security attributes. In this context, the survey questionnaire formulated questions about the attitudes and behaviour of the respondents in the area of compliance with security rules and good practices, risky behaviour in cyberspace, as well as personal data protection and privacy. The survey results regarding the issues mentioned above are presented in Table 15.

According to the above table, the questions in the questionnaire regarding the attitudes and behaviour of the respondents were formulated using the Likert scale. In the area of safety rules and best practices, the answer "sometimes" was dominant in the overwhelming majority of cases. The figures lead to the conclusion that the majority of respondents do not follow the recommended solutions that contribute to ensuring cyberspace security. After summing up the answers "always" and "often", the attitudes and behaviour of the respondents for individual safety rules and good practices are as follows: software updating (including the operating system) - 44%, viruses' database updating in an antivirus program - 42%, using websites that have the HTTPS protocol - 39%, regular password changing and applying passwords of adequate complexity - 27%, scanning external storage media - 25%, two-factor authentication - 19%, scanning e-mail attachments - 16%, regular scanning computer for malware - 16%. The largest number of respondents "never" scan external storage media, do not use two-factor authentication and do not scan attachments in received e-mails.

Another area presented in Table 15 is risky behaviour in cyberspace. Analysing the study results, most of the respondents confirmed the performance of activities in cyberspace that are potentially dangerous and may generate vulnerability. The sum of the answers "always", "often" and "sometimes" for each of the examined elements was as follows: downloading illegal software - 84%, using potentially dangerous websites - 71%, using public Wi-Fi - 67%, opening attachments and links from an unknown source - 59%, viewing spam and other messages from an unknown source - 53%. It should be emphasised that the behaviours of the respondents, which may be considered risky in cyberspace, do not occur regularly because the most common answer was "sometimes". Nevertheless, it can be assumed that respondents' awareness is insufficient in terms of the risk resulting from the analysed behaviour in cyberspace.

The last group listed in Table 15 is personal data protection and maintaining privacy in cyberspace. It should be emphasised that marginalising the discussed issues is facilitating the occurrence of various types of threats that may relate to the personal safety of users (e.g., Newman, 2006). The cited data shows that 50% of respondents "always" or "often" adjust the default privacy settings on social networks to their own needs. About 41% of respondents "always" or "often" consent to data profiling, with the most frequently chosen

Table 12
The impact of education and training on knowledge of cyber-attacks – hypothesis testing.

Variable X	Chi-2 test			Pearson's C coefficient	
	Empirical value	Critical value	Hypothesis verification	Empirical value	Dependency strength
	Variable Y: knowledge of cyberattacks and malware				
Education	6429,23	3,84	positive	0,89	Strong dependency
Training, courses	4998,51		positive	0,87	Strong dependency

Source: Own work.

Table 13
Security measures and methods for data protection used by respondents.

Security measures	Yes	No	Σ
Antivirus software	1302	218	1520
Firewall	1174	346	1520
IDS/IPS systems	939	581	1520
Virtual Private Network (VPN)	525	995	1520
Disc encryption (e.g., BitLocker, VeraCrypt)	501	1019	1520
E-mail encryption	472	1048	1520
End-to-end encryption instant messengers	363	1157	1520
Backup copies	321	1199	1520
Tor Browser	167	1353	1520
Hiding SSID network	162	1358	1520
Utilising MAC addresses filtering	124	1396	1520

Source: Own work.

Table 14
The impact of knowledge about threats on the applied data protection methods and security measures – hypothesis testing.

Variable Y	Variable X: Knowledge about threats to the state cyberspace		
	Value	Dependency strength	Dependency direction
Data protection security measures and methods	0,89	Strong dependency	Positive dependency

Source: Own work.

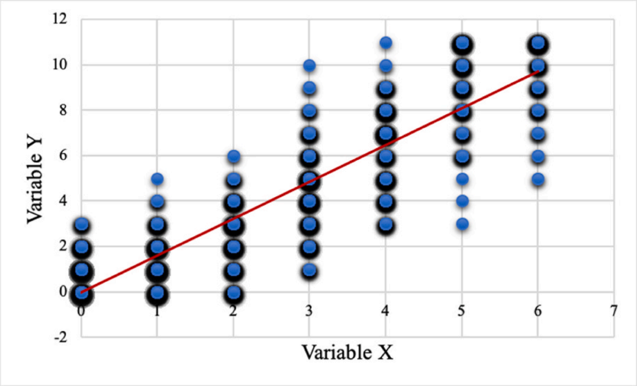

Fig. 5. Scatter diagram of variable X (knowledge of threats to the state cyberspace) and variable Y (security and data protection methods).
Source: Own work.

answer being "sometimes". The exclusion of geolocation services in an operating system is as follows: "always" - 12%, "often" - 17%, "sometimes" - 38%, "rarely" - 26%, "never" - 7%. The analysis of the collected material shows that only 36% of the respondents "always" or "often" read privacy policies and terms of use of websites. The largest number of respondents indicated that they do not or rarely use browsers that do not record their search history. 27% of respondents admitted that "always" or "often" consent to allowing third parties to access and use their data. Network traffic anonymisation is the solution used by the smallest number of respondents. The percentage distribution in this range is as follows: "always" - 4%, "often" - 10%, "sometimes" - 22%, "rarely" - 24%, "never" - 40%.

Summarising the above considerations, it can be stated that the attitudes and behaviour of the respondents in the area of cybersecurity are insufficient. Compliance with the rules and good practices functions to a limited extent. Most of the respondents perform activities that may be considered dangerous and risky with varying frequency. The protection of personal data and the preservation of privacy in cyberspace occurs at a slightly better level than other areas of the study. It can be assumed that this is a consequence of implementing the provisions of the GDPR in the EU member states.

The analysis of the respondents' answers made it possible to adopt the hypothesis that there is a relationship between the attitudes and behaviour of respondents in cyberspace and participation in training or courses in the field of information security. This relationship was tested using the Chi-2 test and the Persona C correlation coefficient (Table 16).

The results of the Chi-2 test and the values of the C Pearson's coefficient allowed for positive verification of the hypothesis about the existence of a relationship between the attitudes and behaviour of respondents and participation in training or courses. Compliance with the principles of security and good practices in cyberspace occurred in an overwhelming number of cases regarding people who acquired appropriate knowledge in this area. The research results show a moderate correlation between the risky behaviour of users in cyberspace and participation in training or courses. Despite their knowledge of the threats, respondents relatively often download

Table 15
Attitudes and behaviour of respondents in cyberspace.

	always	often	sometimes	rarely	never	Σ
Security rules and good practices in cyberspace						
Software updating (including operating system)	252	410	584	239	35	1520
Updating viruses' database in antivirus software	247	391	590	240	52	1520
Using websites with HTTPS protocol	161	430	522	321	86	1520
Password (complexity and password changing)	135	274	652	386	73	1520
Scanning external storage media	112	275	635	180	318	1520
Scanning e-mail attachments with antivirus software	89	152	425	573	281	1520
Two-factor authentication	75	215	421	510	299	1520
Scanning computers for malware	54	188	672	545	61	1520
Risky behaviour in cyberspace						
Downloading illegal software	152	523	599	172	74	1520
Opening attachments and links from unknown sources	75	328	492	371	254	1520
Viewing spam and other messages from unknown sources	58	215	529	447	271	1520
Using potentially unsecure websites	43	421	619	346	91	1520
Using public Wi-Fi	28	418	574	324	176	1520
Personal data protection and maintaining privacy in cyberspace						
Adjusting default privacy settings on social networks to individual needs	305	462	411	246	96	1520
Consent to data profiling	254	371	473	252	170	1520
Disabling geolocation services in an operating system	183	251	584	402	100	1520
Reading privacy policies and website's terms of use	178	250	521	421	150	1520
Using web browsers that do not store the history of searches	76	189	365	272	618	1520
Allowing third parties to access and use personal data	111	302	382	454	271	1520
Web traffic anonymisation	57	149	341	364	609	1520

Source: Own work.

Table 16
The impact of training on attitudes and behaviour in cyberspace – hypothesis testing.

Variable Y	Chi-2 test			Pearson's C coefficient	
	Empirical value	Critical value	Hypothesis verification	Empirical value	Strength of dependency
	Variable X: training, courses				
Safety rules and good practices in cyberspace	2772,099	9,4877	positive	0,80	Strong dependency
Risky user behaviour in cyberspace	584,437		positive	0,53	Moderate dependency
Personal data protection and maintaining privacy in cyberspace	1916,404		positive	0,75	Strong dependency

Source: Own work.

illegal software, use potentially dangerous websites or use public Wi-Fi. Nevertheless, many other publications also emphasise that the elements mentioned above constitute a significant problem in cybersecurity (e.g., Jaishankar, 2011). The attitudes and behaviour of respondents facilitating data protection and maintaining privacy in cyberspace are determined by the knowledge that the respondents acquired during training or courses. As already mentioned, it can be assumed that the results of research in this area could also be influenced by the implementation of the GDPR provisions into the legal order of European Union member states.

The above considerations lead to the conclusion that raising knowledge in the area of cyberspace, including shaping the right attitudes and behaviour, can be achieved through education for cybersecurity.

Table 17
Assessment of the need to improve competencies in the area of cybersecurity at specific levels and types of education.

Level and type of education	yes	no	no opinion	Σ
Education in primary schools	905	314	301	1520
Education in secondary schools	921	279	320	1520
University education	962	235	323	1520
Training at workplaces	1114	157	249	1520
Additional courses and training	803	91	626	1520
Public information campaigns	1006	194	320	1520

Source: Own work.

4.3. Improving competencies in the field of cybersecurity

In 2020, ENISA published a report on cybersecurity skills development. The report focuses on the education system and the problems related to the shortage of cybersecurity specialists and inadequate professional skills to meet modern labour market requirements (ENISA, 2020b). In this context, the improvement of competencies is an essential issue regarding ensuring cybersecurity.

The survey questionnaire included questions about education, courses and training, the content of education, the form of education and sources of information on cybersecurity. Table 17 presents the study results on the respondents' opinions on the validity of shaping competencies at various levels of education, workplace, and public space.

Based on the above data, it can be concluded that the majority of respondents see the need to improve competencies in the area of cybersecurity at all levels and types of education studied. The largest number of respondents assessed that it is necessary to conduct training at a workplace (73%) and to conduct public information campaigns (66%), which will contribute to the improvement of competencies in the field of cybersecurity. The percentage distribution for the remaining levels and types of education according to the affirmative responses of the respondents was as follows: university education - 63%, education in secondary schools - 61%, education in primary schools - 59%, additional courses and training - 52%.

The questionnaire also formulated questions related to the content of education in which the respondents perceive the need to improve competencies. The questions included, among others, knowledge and skills in the context of formal and legal aspects of cybersecurity, principles of safe use of cyberspace, threats and methods of protection against threats, as well as personal data protection and maintaining privacy. The research results on the issues mentioned above are presented in Table 18.

The figures in Table 18 show that most respondents see the need to raise knowledge and skills of the areas mentioned above. The sum of the answers “definitely yes” and “rather yes” for individual educational content was formed in the following order: rules of safe use of e-services - 96%, characteristics and use of security measures - 95%, procedures in the event of a security incident - 87%, characteristics, effects and detection of cyber threats - 86%, rights and obligations of cyberspace users - 85%, legal basis for cybersecurity - 83%, personal data protection and maintaining privacy - 78%. It is worth noting that the respondents are aware of the need for education in the field of cybersecurity and positively assess the proposed educational content.

The last area studied within the scope of improvement and competencies was the preferred form of education and obtaining information on cybersecurity. Data on these issues are presented in Table 19.

The table above presents the results of a study in the field of courses, training, and sources of information on cybersecurity. The study's goal in this area was to identify the forms by which it is possible to achieve effectiveness in raising competencies and awareness. Most respondents prefer to participate in stationary training in a traditional form (63%) and raise knowledge during information campaigns in the public media (53%). The respondents showed less interest in education and obtaining information using modern technologies. The percentage distribution in this respect is as follows: e-learning courses and training - 51%, mixed courses and training - 48%, information campaigns on social networks - 43%. The smallest number of respondents declared press articles (41%) and information brochures and newsletters (28%) as the preferred source of obtaining information on cybersecurity. It is worth emphasising that the forms of education and sources of information selected by the respondents are significantly differentiated in terms of age structure (Table 20).

Table 20 show that younger people prefer forms of communication based on new technologies, such as e-learning and social networks. On the other hand, older people declared traditional forms of education and information sources, i.e. stationary courses and training, information campaigns in public media. Therefore, it can be assumed that there is a correlation between the answers given by the respondents and their age. The adopted hypothesis was verified using the Chi-2 independence test and the Pearson C coefficient (Table 21).

The above data lead to a positive verification of the hypothesis that there is a relationship between the preferred forms of education and sources of information about cybersecurity and the age of the respondents. The value of the C Pearson's coefficient indicates a strong correlation between the studied variables in the scope of e-learning courses and training and information campaigns on social networks. A moderate dependence occurred in traditional courses and training, information campaigns in public media, articles in the press, and information brochures and newsletters. The study of the relationship between the age of the respondents and the courses and training carried out in a mixed form indicates a weak relationship between the studied variables. Summing up, it can be assumed that the effectiveness in raising knowledge may be achieved in different channels and forms of communication according to potential recipients.

5. Conclusions and recommendations

The technological revolution and the emergence of the information society generate many possibilities and areas of functioning in cyberspace. The further evolution of cyberspace, on the one hand, creates further development possibilities, and on the other hand, there is a need to ensure the security of the carried-out processes. One of the conditions for the effective functioning of society in cyberspace is having appropriate knowledge and skills in the discussed field. With regard to the subject and objectives of the research and research problems, the following conclusions were formulated:

– A review of the literature on the subject indicated that many of the analysed definitions of cybersecurity take into account the cyberspace user. The key issue in this respect is to raise the level of skills and knowledge to build society's resilience to threats in cyberspace. Furthermore, for many countries and international organisations, the discussed issue is one of the priorities in cybersecurity.

Table 18
Assessment of the need to improve competencies in the area of cybersecurity in relation to the content of education.

Content of education	Definitely yes	Rather yes	No opinion	Rather no	Definitely no	Σ
Legal basis for cybersecurity (including those applicable in the workplace)	643	621	237	10	9	1520
Rights and obligations of cyberspace users	716	579	186	33	6	1520
Rules for safe use of e-services	1018	439	56	5	2	1520
Procedure in the event of a security incident (including rights arising from damage dealt)	949	373	198	0	0	1520
Characteristics, effects and detection of cyber threats	947	365	142	47	19	1520
Characteristics and use of security measures	1161	282	71	5	1	1520
Personal data protection and maintaining the privacy	627	565	242	52	34	1520

Source: Own work.

Table 19
Preferred forms of education and sources of information on cybersecurity.

Forms of education and sources of information	yes	no	Σ
Courses and training in traditional form	950	570	1520
E-learning courses and training	771	749	1520
Courses and training in a mixed form	734	786	1520
Information campaigns in public media	804	716	1520
Information campaigns on social networks	648	872	1520
Brochures and newsletters	421	1099	1520
Articles in the press	621	899	1520

Source: Own work.

Table 20
Preferred forms of education and information sources on cybersecurity considering the age structure of respondents.

Variable Y	Variable X: age											
	<26	26–35	36–45	46–55	56–65	>65	<26	26–35	36–45	46–55	56–65	>65
	yes						no					
Courses and training in traditional form	39	72	151	125	267	296	95	160	167	35	72	41
E-learning courses and training	132	226	261	65	50	37	2	6	57	95	289	300
Courses and training in a mixed form	76	152	185	82	144	95	58	80	133	78	195	242
Information campaigns in public media	5	23	131	113	253	279	129	209	187	47	86	58
Information campaigns on social networks	132	226	197	40	31	22	2	6	121	120	308	315
Brochures and newsletters	0	4	41	75	135	166	134	228	277	85	204	171
Articles in the press	2	5	59	115	198	242	132	227	259	45	141	95

Source: Own work.

Table 21
The impact of age on the choice of the form of education and the source of information on cybersecurity – hypothesis testing.

Variable Y	Chi-2 test			Pearson's C coefficient	
	Empirical value	Critical value	Hypothesis verification	Empirical value	Strength of dependency
	Variable X: age				
Courses and training in traditional form	307,731	11,0705	positive	0,41	Moderate dependency
E-learning courses and training	844,839		positive	0,60	Strong dependency
Courses and training in a mixed form	103,502		positive	0,25	Weak dependency
Information campaigns in public media	524,815		positive	0,51	Moderate dependency
Information campaigns on social networks	859,646		positive	0,60	Strong dependency
Brochures and newsletters	296,791		positive	0,40	Moderate dependency
Articles in the press	547,743		positive	0,51	Moderate dependency

Source: Own work.

– Cyberspace security in the context of the human factor can be analysed by applying a layered structure. The article proposes to distinguish a strategic layer, a technical layer and a social layer. The areas mentioned above are interrelated and may affect the effectiveness of cybersecurity management. The proposed interpretation of cyberspace security may contribute to the study of relationships between individual layers and the identification of problem areas. In this context, the article details the social dimension of cybersecurity with the following types of requirements: legal, organisational, procedural, educational and technical.

Table 22
Policy recommendations - cybersecurity competencies.

Field	Recommendations
The essence and definition of cybersecurity	- In defining cybersecurity, it is justified to consider the human factor. The social dimension of cybersecurity should take into account the following requirements: o Policies, strategic documents and legal acts define the areas of education and training that will include cybersecurity competencies. o Legal acts provide legal protection of cyberspace users. o The organisation of the cybersecurity system ensures the attributes of information security and minimises the risk of threats caused by the vulnerability of the human factor. o Cyberspace users have and improve their competencies in the field of cybersecurity.
Research on cybersecurity competencies	- One of the measures for assessing the effectiveness of the implementation of the sustainable development goals may be the empirical research results on cybersecurity competencies. - Research should take into account knowledge, skills and attitudes in the field of cybersecurity. - Competency analysis should take into account user interactions with individual layers of cyberspace security (Fig. 1). - The Cybersecurity Competency Model can be the basis for assessing competencies in the field of cybersecurity (Fig. 2). - It is legitimate for research to include the analysis of statistical relationships between dependent and independent variables. Recognition of the relationship between the studied variables will enable the development of educational programs that will be dedicated to specific groups of recipients.
Threats to cyberspace of the state and methods of cyber attacks	- Research results have shown that there is a need to increase knowledge about the threats and methods of cyberattacks. - Courses and training have a significant impact on the level of knowledge about threats. It is important to disseminate general and specialist knowledge about the threats and methods of cyberattacks. - The analysis of statistical dependencies showed that there is a relationship between the knowledge of cyberspace threats and the socio-demographic characteristics of the respondents. The content of information campaigns and training courses should be developed taking into account the characteristics of the recipients, i.e. age, education.
Security and data protection in cyberspace	- It is necessary to promote knowledge and skills about specialised solutions that minimise the risk of security incidents. - The findings of empirical research have shown that awareness of threats influences the choice of security measures and methods of data protection. There is a strong correlation between the use of specialised security measures and knowledge about the threats to the state cyberspace. Educational programs should include knowledge of identifying threats in cyberspace and the types of adequate protection methods. - It is reasonable to promote principles and good practices, such as two-factor authentication, scanning (computers, storage media, e-mail attachments), updating (software, virus databases in an antivirus program). - Training programs should present the potential effects of risky activities in cyberspace, such as, e.g. downloading illegal software, opening attachments and links from an unknown source, using public Wi-Fi and using potentially dangerous sites. - The protection of personal data and the preservation of privacy in cyberspace is on a better level compared to other areas of the study. Nevertheless, it is justified to improve competencies in the discussed area. - The analysis of statistical dependencies showed that there is a relationship between attitudes and behaviour in cyberspace and participation in training and courses. Therefore, it can be assumed that increasing the frequency of training and disseminating knowledge may contribute to increasing competencies in the field of security and data protection in cyberspace.
Improving cybersecurity competencies	- Most of the respondents see the need to improve their cybersecurity competencies. There is great interest in on-the-job training and public information campaigns. Appropriate information campaigns and training can be positively accepted by the public. In addition, it is reasonable to include cybersecurity issues at all levels of education (primary schools, secondary schools, university education). - The recommended content of education in the field of cybersecurity includes, among others: legal bases, rights and obligations of users, rules of safe use of e-services, conduct in the event of a security incident, detection of cyber threats, use of security, data and personal protection and preservation of privacy. - The choice of the preferred forms and sources of information depends on the age structure. Research findings have shown that younger people prefer new technologies, while older people prefer traditional forms of training. Therefore, it is reasonable to implement training courses taking into account various forms and sources of information, e.g. e-learning, social media, public media, press articles.

Source: Own work.

- The theoretical analysis indicates that competencies in the context of the research subject are often equated with the proper perception of threats in cyberspace, having adequate knowledge, skills and attitudes to facilitate ensuring cybersecurity. The Cybersecurity Competency Model developed by NICE can provide a reference point for analysing and assessing the human factor in cybersecurity. It is worth emphasising that the lack of knowledge and competencies may generate vulnerabilities in a security system.
- Achieving sustainable development goals requires the implementation of many projects, including increasing cybersecurity competencies. Many strategic documents indicate that the challenges for cybersecurity policy include the need to improve the human factor. An essential task for politics is promoting cyber hygiene, digital skills, providing information on threats and protection methods. The European Union regulations improved the level of security of networks and information systems. Nevertheless, there are still problem areas in the field of cybersecurity. In addition, it can be assumed that the further development of digitisation will increase the demand for competencies in the field of cybersecurity. Therefore, it is justified to improve the existing solutions to minimise the risk of threats caused by the vulnerability of the human factor.
- The paper presents the research results on competencies in the field of threats to the state cyberspace, methods of cyberattacks, and data security measures and protection. The survey questionnaire also contained questions aimed at finding out the respondents' opinions within the range of educational content and the need to improve competencies. The empirical research aimed to identify forms of education and communication sources that can be used to achieve efficiency in raising cybersecurity competencies.
- The research results showed that the respondents' awareness and knowledge of threats to the state cyberspace are insufficient. Most of the respondents are not aware of the specificity and scale of such threats as intentional and unintentional activities of the organisation's employees, social engineering, cyber warfare and cyber spying. The analysis of the socio-demographic characteristics of the respondents and the answers provided indicated the existence of a relationship between knowledge, education, and age. People with higher education and younger people are more aware of the threats to the state cyberspace. In this context, the authors recommend the implementation of information campaigns and training courses that take into account the education and age structures.
- The quantitative data on cyberattacks and malware highlighted significant gaps in specialised knowledge. The research results showed a significant statistical relationship between the answers provided and the type of education and training in information security. The respondents with IT education and the people participating in the training were distinguished by much greater knowledge within the range of the discussed field. Therefore, it is justified to consider the need to introduce a subject considering principles of safe use of cyberspace to the education programs of all fields of study. However, in the field of training, the gradual introduction of courses for public and private sector employees is recommended.
- Based on the results of research on security and data protection methods, it can be stated that the majority of respondents use popular solutions such as antiviruses or firewall software. Other of the tested methods of protection occurs to a rather limited extent. The statistical dependencies analysis showed a positive correlation between knowledge of threats and the applied security measures and data protection methods. People who are more aware of the threats to the cyberspace of the state usually use many types of security simultaneously. Therefore, it can be assumed that improving the knowledge about the scale and effects of cyber threats could contribute to increasing the prevention of cyberattacks among society. Therefore, it is reasonable to include the discussed content both in education programs and courses, as well as in public media.
- The empirical research also covered the attitudes and behaviours of users in cyberspace, which concerned compliance with security principles and good practices, risky behaviour, as well as personal data protection and maintaining privacy. Detailed analysis of the issue proves that most respondents do not comply with the recommended cyberspace security rules and perform activities that may be considered dangerous. Examples include no regular computer scanning for malware, no scanning of external storage media, downloading illegal software, using public Wi-Fi networks or viewing messages from an unknown source. On the other hand, the protection of personal data and the maintenance of privacy are of a higher level. Nevertheless, it can be stated that too high a percentage of respondents, for example, do not read privacy policies and terms of use of websites. The study of statistical relationships showed a relationship between training and the attitudes and behaviour of the respondents in cyberspace. The research results in this area once again confirm the positive impact of education on raising competencies in the area of cybersecurity. Therefore, it is recommended to increase the number of training courses regarding the research issues.
- The questionnaire also included questions regarding the respondents' opinions on education, training, education content and preferred forms of obtaining sources of information on cybersecurity. This part of the research aimed to identify social needs in the discussed area and to identify forms of communication with the help of which it is possible to achieve greater efficiency in raising competencies. It should be emphasised that the majority of respondents are aware of the need to popularise knowledge and improve competencies in the studied areas. Therefore, it can be assumed that relevant information campaigns could be positively received by the public. Comparing the research results to the preferred forms and sources of information on cybersecurity, it can be noticed that the selection of specific types is determined by the age structure. The statistical dependencies analysis showed that younger people prefer methods that use new technologies, e.g., e-learning, social media. On the other hand, the older adults declare their readiness to raise knowledge using traditional forms of communication, e.g., stationary courses and training, information campaigns in public media. In this context, the authors recommend using the potential of the available forms of education and information sources to improve cybersecurity competencies. It can be assumed that the differentiation of the forms of communication according to the age structure could contribute to the expanse of the range of potential recipients.

The research results made it possible to define the recommended solutions for the policy for the purpose of improving cybersecurity competencies (Table 22).

The article's subject concerned the important issue of improving the human factor in cybersecurity. It should be emphasised that the lack of appropriate competencies in the discussed area may lead to negative consequences for both personal safety and may bring about significant losses to public and private institutions and national security. Moreover, the modern labour market requirement is the demand for cybersecurity specialists.

The implementation of the recommended solutions for the policy requires increasing financial outlays on cybersecurity. In organisations, it is justified to increase expenditure on educating employees and increasing their competencies in the field of cybersecurity. As previously mentioned, many reports show that cybercrime losses are enormous and tend to increase. Compliance with cyber hygiene principles can reduce the significant number of security incidents caused by human factor vulnerabilities. Education expenditure can be a significant economic burden for many organisations. However, the costs of handling security incidents are often much higher. Especially that there is still an unsolved problem area of insufficient competencies in the field of cybersecurity. The overall economic profit and loss account of investments in cybersecurity education requires further analysis.

In addition, it is also worth considering the risks associated with the vulnerability of the human factor to fake software updates. There are many attack vectors that take advantage of fake updates. Cybercriminals can use social engineering techniques and send fake messages about updates. Directional attacks on update servers are also possible, causing end devices to receive updates containing malware.

Therefore, it can be concluded that raising cybersecurity competencies is a significant strategic challenge. In conclusion, the authors perceive a need to continue research regarding competencies in the area of cybersecurity.

References

Antonuci, D. (2017). *The cyber risk Handbook: Creating and Measurning effective cybersecurity capabilities*. USA: Wiley. Hoboken.

Appiah-Otoo, I., & Song, N. (2021). The impact of ICT on economic growth-Comparing rich and poor countries. Telecommunications Policy. *Elsevier, 45*(Issue 2). https://doi.org/10.1016/j.telpol.2020.102082. March 2021, Article 10208.

Bell, E., & LaPadula, L. J. (1973). MITRE Technical Report 2547. *Secure computer systems: Mathematical foundations, ume I*. Bedford, MA: MITRE Corporation. Retrieved from http://www-personal.umich.edu/~cja/LPS12b/refs/belllapadula1.pdf.

Biba, K. (1975). *Integrity considerations for secure computer systems*. MITRE *Technical Report MTR-3153*. Bedford,. MA: MITRE Corporation. Retrieved from http://seclab.cs.ucdavis.edu/projects/history/papers/biba75.pdf.

Com/2020/0624. (2020). *Communication from the Commission to the European Parliament, the Council, the European economic and social Committee and the Committee of the Regions digital education action plan 2021-2027* (Vol. 30). Brussels: Resetting education and training for the digital age, 9.

Connolly, L., & Wall, D. (2019). The rise of crypto-ransomware in a changing cybercrime landscape: Taxonomising countermeasures. In *Computers & security* (Vol. 87). Elsevier. https://doi.org/10.1016/j.cose.2019.101568. November 2019, Article 101568.

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. *Technol. Innov. Manag. Rev.', 4*(Number 10), 13–21. https://doi.org/10.22215/timreview/835

Cybersecurity Competency Model. (2019). *Employment and training Administration*. United States Department of Labor Accessed 7 January 2021 https://www.careeronestop.org/CompetencyModel/competency-models/pyramid-download.aspx?industry=cybersecurity.

Dodge, R. C., Carver, C., & Ferguson, A. J. (2007). Phishing for user security awareness. Computers & Security. *Elsevier, 26*(1), 73–80. https://doi.org/10.1016/j.cose.2006.10.009

ENISA. (2017). *Stock taking of information security training needs in critical sectors* Accessed 14 January 2021 https://www.enisa.europa.eu/publications/stock-taking-of-information-security-training-needs-in-critical-sectors.

ENISA. (2018). *Analysis of the European R&D priorities in cybersecurity Strategic priorities in cybersecurity for a safer Europe* Accessed 14 January 2021 https://www.enisa.europa.eu/publications/analysis-of-the-european-r-d-priorities-in-cybersecurity.

ENISA. (2019a). *Threat Landscape report 2018* Accessed 13 January 2021 https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018.

ENISA. (2019b). *Cybersecurity Culture Guidelines: Behavioural aspects of cybersecurity* Accessed 08 February 2021 https://www.enisa.europa.eu/publications/cybersecurity-culture-guidelines-behavioural-aspects-of-cybersecurity.

ENISA. (2020a). *ECSM ECSM Deployment report 2019* Accessed 12 January 2021 https://www.enisa.europa.eu/publications/ecsm-deployment-report-2019.

ENISA. (2020b). *Cybersecurity skills development in the EU* Accessed 27 January 2021 https://www.enisa.europa.eu/publications/the-status-of-cyber-security-education-in-the-european-union.

Europol. (2019). *Internet organised Crime Thread assessment (IOCTA). Europol. European cybercrime Centre. The Hauge* Accessed 5 January 2021 https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment.

Franke, U., & Brynielsson, J. (2014). Cyber situational awareness - a systematic review of the literature. Computers & Security. *Elsevier, 46*(October), 18–31. https://doi.org/10.1016/j.cose.2014.06.008, 2014.

Frauenstein, E., & Flowerday, S. (2020). Susceptibility to phishing on social network sites: A personality information processing model. In *Computers & security* (Vol. 94). Elsevier. https://doi.org/10.1016/j.cose.2020.101862. July 2020, Article 101862.

Geber, N., Geber, J., & Volkamer, M. (2018). Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. Computers & security. *Elsevier, 77*(August), 226–261. https://doi.org/10.1016/j.cose.2018.04.002, 2018.

Graham, G. S., & Denning, P. J. (1972). Protection: Principles and practice. In *Proceedings of the may 16-18, 1972, Spring Joint computer conference* (pp. 417–429). New York, NY, USA: Association for Computing Machinery. https://doi.org/10.1145/1478873.1478928.

Hadlington, L. (2017). Human factors in cybersecurity; examining the link between Internetaddiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon, 3*(7). https://doi.org/10.1016/j.heliyon.2017.e00346. Article E00346.

Harrison, M. A., Ruzzo, W. A., & Ullman, J. D. (1976). Protection in operating systems. *Communications of the ACM, 19*, 461–471. Number 8.

Henriksen-Bulmer, J., Faily, S., & Jeary, S. (2019). Privacy risk assessment in context: A meta-model based on contextual integrity. In *Computers & security* (Vol. 82, pp. 270–288). Elsevier. https://doi.org/10.1016/j.cose.2019.01.003. May 2019.

ISO/IEC 27032. (2012). *Information technology – security techniques – Guides for cybersecurity*. Retrieved from Accessed 17 January 2021 https://www.iso27001security.com/html/27032.html.

Jaishankar, K. (Ed.). (2011). *Cyber Criminology: Exploring Internet Crimes and Criminal behavior*. Boca Raton, FL: CRC Press.

JOIN. (2020). *18. Joint Communication to the European Parliament and the Council the EU'S. Cybersecurity Strategy for the Digital Decade. Brussels*, 16.12.2020.

Kalhoro, S., Rehman, M., Ponnusamy, V., & Shaikh, F. B. (2021). Extracting key factors of cyber hygiene behaviour among software engineers: A systematic literature review. *IEEE Access, 9*, 99339–99363. https://doi.org/10.1109/ACCESS.2021.3097144

Kim, M. S., & Kim, S. (2018). Factors influencing willingness to provide personal information for personalised recommendations. In *Computers in human behavior* (Vol. 88, pp. 143–152). Elsevier. https://doi.org/10.1016/j.chb.2018.06.031. November 2018.

Kosseff, J. (2019). *Cybersecurity law* (2nd ed.). USA: Wiley. Hoboken.

Kraemer, S., & Pascale, C. (2003). A human factors vulnerability evaluation method for computer and information security. Human Factors and Ergonomics Society Annual Meeting Proceedings. *Sage, 47*(12), 1389–1393. https://doi.org/10.1177/154193120304701202

Liu, H., Ning, H., Mu, Q., Zheng, Y., Zeng, J., Yang, L., et al. (July 2019). (2019). A review of the smart world. In *Future generation computer systems* (Vol. 96, pp. 678–691). Elsevier. https://doi.org/10.1016/j.future.2017.09.010

Markopoulou, D., Papakonstantinou, V., & de Her, P. (2019). The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation, 6. In *Computer law & security review* (Vol. 35). Elsevier. https://doi.org/10.1016/j.clsr.2019.06.007. November 2019, Article 105336.

Mitomo, H., Fuke, H., & Bohlin, E. (Eds.). (2015). *The Smart revolution towards the sustainable digital society: Beyond the Era of Convergence*. Cheltenham, UK: Edward Elgar Publishing. https://doi.org/10.4337/9781784710040.

Morgan, S. (2021). *Report: Cyberwarfare in the C-suite*. Cybersecurity Ventures https://1c7fab3im83f5gqiow2qqs2k-wpengine.netdna-ssl.com/wp-content/uploads/2021/01/Cyberwarfare-2021-Report.pdf.

Neigal, A. R., Claypoole, V. L., Waldfoogle, G. E., Acharya, S., & Hancook, G. M. (2020). Holistic cyber hygiene education: Accounting for the human factors. In *Computers & security* (Vol. 92). Elsevier. https://doi.org/10.1016/j.cose.2020.101731. May 2020, Article 101731.

Newman, R. (2006). Cybercrime, identity theft, and fraud: Practicing safe internet - network security threats and vulnerabilities. In *Proceedings of the 3rd annual conference on Information security curriculum development (InfoSecCD '06)* (pp. 68–78). New York, NY, USA: Association for Computing Machinery. https://doi.org/10.1145/1231047.1231064.

NSPD-54/HSPD-23. (2008). *National security Presidential directive/NSPD-54. National security Presidential directive/NSPD-23*. Washington: The White House.

Oxford Online Dictionary. https://www.lexico.com/definition/security Accessed 7 December 2020.

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6. July 2016 concerning measures for a high common level of security of network and information systems across the Union (O.J. EU L 191/1, 19.7.2016).

Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance) (O.J. EU L 151, 7.6.2019).

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of the personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (O.J.EU L 119/1, 4.5.2016).

Person, K., Calic, D., Pattison, M., Butavisius, M., McComac, A., & Zwaans, T. (2017). The human aspects of information security questionnaire (HAIS-Q): Two further validation studies. In *Computers & security* (Vol. 66, pp. 40–51). Elsevier. https://doi.org/10.1016/j.cose.2017.01.004. May 2017.

Probst, C., Hunkel, J., Dieter, G., & Bishop, M. (2010). *Insider threats in cyber security*. Boston: Springer. https://doi.org/10.1007/978-1-4419-7133-3. Systems.

Raven, J., & Stephenson, J. (Eds.). (2001). *Competence in the learning society*. New York: Peter Lang.

Refsdal, A., Soulhug, B., & Stolen, K. (2015). *Cybersecurity. Cyber-risk management. SpringerBriefs in computer science*. Cham: Springer. https://doi.org/10.1007/978-3-319-23570-7_4

Robison, K., & Crenshaw, E. (2002). Post-industrial transformations and cyber-space: A cross-national analysis of internet development. Social science research. *Elsevier, 21*(3), 334–363. https://doi.org/10.1016/S0049-089X(02)00004-2

Schoon, I. (2009). *Measuring social competencies. (RatSWD Working Paper Series, 58). Berlin: Rat für Sozial - und Wirtschaftsdaten (RatSWD)*. Retrieved from https://nbn-resolving.org/urn:nbn:de:0168-ssoar-409526.

Sharma, R., Fantin, A., Prabhu, N., Guan, C., & Dattakumar, A. (2016). Digital literacy and knowledge societies: A grounded theory investigation of sustainable development. Telecommunications policy. *Elsevier, 40*(7), 628–643. https://doi.org/10.1016/j.telpol.2016.05.003

Sienkiewicz, P. (1989). *Systemy kierowania*. Warsaw: Wiedza Powszechna. Poland.

Sienkiewicz, P. (2013). *25 wykładów*. Warsaw: AON. Poland.

Singh, Y. K. (2006). *Fundamental of research methodology and Statistics*. New Delhi: New Age International.

Stouffer, K., Zimmerman, T., Tang, C., Lubell, J., Cichonski, J., & McCarthy, J. (2017). *Cybersecurity Framework Manufacturing profile*. National Institute of Standards and Technology. Report 8183 (NISTIR 8183). Retrieved from https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8183.pdf.

Szczepaniuk, H. (2019). *Efektywność kształcenie e-learningowego w Polsce*. Warsaw: Wydawnictwo SGGW. Poland.

Szczepaniuk, E., Szczepaniuk, H., Rokicki, T., & Klepacki, B. (2020). *Information security assessment in public administration. Computers & Security* (Vol. 90). Elsevier. https://doi.org/10.1016/j.cose.2019.101709. March 2020, Article 101709.

UN. (2017). *Report of the Committee on the future Economy. Pioneers of the next generation*. https://sustainabledevelopment.un.org/content/documents/16265Committee_on_the_Future_Economy_Report.pdf.

Vasiu, I., & Vasiu, L. (2018). Cybersecurity as an essential sustainable economic development factor. *European Journal of Sustainable Development, 7*(Number 4), 171–178. https://doi.org/10.14207/ejsd.2018.v7n4p171

Vu, K., Hanafizadeh, P., & Bohlin, E. (2020). ICT as a driver of economic growth: A survey of the literature and directions for future research. Telecommunications policy. *Elsevier, 44*(Issue 2). https://doi.org/10.1016/j.telpol.2020.101922. Article 101922.

Wang, P. A. (2013). *Assessment of cybersecurity knowledge and Behavior:an anti -phishingScenario .ICIMP 2013 :the Eighth international Conference on Internet Monitoring and protection*. Rome ,Italy: IARIA. Retrieved from https://www.thinkmind.org/index.php?view=article&articleid=icimp_2013_1_10_30003.

WEF. (2020a). *The global risks report 2020* (15th ed.). Geneva: World Economic Forum. Retrieved from https://www.weforum.org/reports/the-global-risks-report-2020.

WEF. (2020b). *The future of Jobs report 2020*. World Economic Forum. http://www3.weforum.org/docs/WEF_Future_of_Jobs_2020.pdf.

Whitman, M. E. (2018). Industry priorities for cybersecurity competencies. *J. Colloq. Inform. Syst. Secur. Edu. Edition 6*, (1). Retrieved from https://cisse.info/journal/index.php/cisse/article/view/91/CISSE_v06_i01_p06.pdf.