Erasmus+ KA2 - KA220-HED - Cooperation partnerships in higher education
2021-1-TR01-KA220-HED-000031993

R1/A1

ANALYTICAL REPORT ON THE NATIONAL DESKTOP ANALYSIS IN PARTNER COUNTRIES

Cyber IN Practice R1/A1 Combined Report

INDEX

ANALYTICAL REPORT ON THE NATIONAL DESKTOP ANALYSIS IN TURKEY

Introduction

The purpose of this report is to describe the situation Turkey is facing due to digital transformation. Parts of the report are divided into four main categories. A brief description of the general situation of the country is given in the first section, followed by an examination of the state of secondary education, and thereafter the state of higher education. The fourth chapter summarizes the digital and cyber awareness of the target audience and related literature studies.

Bibliographical Research

National Policy Documents

Although Turkey seems to lag behind Europe in terms of digital competition, it aims to become one of the ambitious countries in the medium-term future with its investments and future plans. According to the World Digital Competitiveness Ranking 2022, some of the countries in the list and their rankings are presented in the table below:

Table 1. World Digital Competitiveness Ranking 2022

RANK	NAME OF THE COUNTRY
1	Denmark
2	Usa
3	Sweden
4	Singapore
5	Switzerland
…..	…..
39	Italy
…..	…..
46	Poland
…..	…..
48	Bulgaria
…..	…..

54	Turkey
…..	…..
62	Mongolia
63	Venezuela

The rise of cybersecurity-related laws in 2021 and beyond, and diversification is expected. Especially, with the enactment of new laws in order to comply with the regulation rules of many countries, new data management departments are established and it becomes important to monitor who uses the data and where it is kept in all institutions and organizations.

It is very important for businesses to adapt to the digitalization process in order to increase digital literacy in the country, to develop the digital economy and to reflect this development on education budgets.

Latest data provided by TUİK (Turkish Statistical Institute) indicates that, according to the results of the Information Technologies Usage Survey in enterprises in Turkey; Internet access rate of enterprises with 10 or more employees in 2021 was 95.3%. When the rate of access to the Internet is analyzed according to the number of employees and size groups; this rate was 94.7% in enterprises with 10-49 employees, 98.0% in enterprises with 50-249 employees, and 99.9% in enterprises with 250 or more employees.

93.0% of startups used fixed broadband connection to access the Internet in 2021. Considering the highest Internet connection speeds these enterprises subscribe to; It was determined that 9.7% of the enterprises use the Internet at a speed of less than 10 Mbit/s, 62.2% of them in the range of 10-99 Mbit/s, and 28.1% of them using the Internet at a speed of 100 Mbit/s and above. While the rate of Internet users at 100 Mbit/s and above was 37.6% in 2020 in enterprises with 250 or more employees, this rate increased to 47.7% in2021.

Without a doubt, this situation causes the issue of information security to come to the fore, emphasizing the subject of the project. On the other hand, according to the results of the research carried out by Deloitte (2021) with the participation of many experts and senior managers from different sectors to understand the current situation of Turkey on the path to digitalization, it is seen that the most invested subject in the current situation is cyber security.

TEKNOFEST, which has been organized throughout the country since 2018, is one of the most comprehensive digital events organized in Europe in its field.

As part of Turkey's development and strengthening its independence in every field, studies are being conducted to develop national and unique technological products and systems. It is crucial for these studies to motivate all layers of society in line with these goals. In addition, it is crucial for these studies to train and support human resources that can develop advanced technologies. One of the prerequisites for success in these processes, which can be defined as a "National Technology Move", is to be able to make progress in the fields of aviation and space, which are accepted as the locomotive of high technology projects all over the world.

In the festival, where many ministries and presidency as well as universities and companies are stakeholders, the stakeholder institutions vary according to the years, but the latest status of the list is as follows.

Stakeholder Ministries & Presidencies	Stakeholder Corporations
Turkish Technology Team Foundation	AFAD
Republic of Turkey Ministry of Industry and Technology	ASELSAN
Republic of Turkey Ministry of Youth and Sports	BAYKAR
Ministry of Interior of the Republic of Türkiye	Informatics Valley
Republic of Türkiye Ministry of Culture and Tourism	Can Sağlığı Foundation
Ministry of Health of the Republic of Turkey	Cezeri
Republic of Turkey Ministry of National Education	General Directorate Of State Airports Authority of Turkey
Republic of Türkiye Ministry of National Defence	HAVELSAN
Ministry of Transport and Infrastructure of the Republic of Turkey	İGA
Presidency of the Republic of Türkiye Defence Industries	ROKETSAN
Republic of Turkey Ministry of National Defence General Staff	Samsun Metropolitan Municipality
Digital Transformation Office of the Presidency of Republic of Türkiye	Governorship of Samsun
Presidency of the Republic of Turkey Investment Office	SANKO
	Directorate General of Civil Aviation of Turkey
Academic Stakeholders	STM
Afyon Kocatepe Üniversitesi	TEI
Afyonkarahisar Health Sciences University	TÜBİTAK
Altınbas University	TÜBİTAK BİLGEM
Ankara University	TÜBİTAK MAM
Ankara Yıldırım Beyazıt University	TÜBİTAK RUTE
Antalya Bilim University	TÜBİTAK SAGE

Atatürk University	TURKCELL
Boğaziçi University	Turkish Aerospace Industries
Bolu Abant İzzet Baysal Üniversitesi	TURKISH AIRLINES
Bursa Technical University	Turkish Patent
Bursa Uludağ University	Turkey Beyaz Ay Association
Dokuz Eylül University	Turkish Academy of Sciences
Ege University	Turkish Maarif Foundation
Eskişehir Technical University	TÜSEB
Fatih Sultan Mehmet Foundation University	Turkish Space Agency
Fırat University	TÜRKSAT
Gazi University	YONGATEK
Gaziantep University	Yunus Emre Institute
Gebze Technical University	YTB
Giresun University	
Hasan Kalyoncu University	**Media-Digital Media Stakeholders**
Isparta Uygulamalı Bilimler Üniversitesi	Anadolu Agency
İnönü University	TRT
İstanbul Aydın University	A HABER | SABAH
İstanbul Medeniyet University	Albayrak Medya
İstanbul University Cerrahpaşa	Demirören Medya
İstanbul Technical University	Doğuş Yayın Grubu
Karadeniz Technical University	HaberTürk
Konya Technical University	Kanal 7 Medya Grubu
Kütahya Dumlupınar Üniversitesi	TGRT Haber
Manisa Celal Bayar University	Türk Medya
Marmara University	GZT
Necmettin Erbakan University	
Ondokuz Mayıs University	
ODTU METU	
Pamukkale Üniversitesi	
Recep Tayyip Erdoğan University	
Samsun University	
Sanko University	
Selçuk University	
Trabzon Üniversitesi	

Yıldız Technical University	

The "Digital Turkey: Roadmap" report, published annually by the Ministry of Science, Industry and Technology, examines the current state and future prospects of the country's digitalization process. The report emphasizes that education infrastructure and qualified workers are two of the most important components of digital transformation. Manufacturing will become increasingly digital as a result of the need for a workforce with a variety of skills and qualifications. As a result of the digital transformation process, the way businesses are conducted is being remodeled, and the need for qualified employees is becoming increasingly evident. In order for the workforce with the qualifications required by digital transformation to acquire these qualifications, it has become necessary to redesign the necessary trainings and the environments where these trainings will take place. From the primary education level, training and programs will be provided for the development of digital skills at all levels of basic, vocational, higher education, as well as in business life, so that the workforce is prepared to meet the needs of enterprises. The manufacturing industry is predicted to lose many jobs based on muscle power with the advent of digitalization, while more qualified workers will be needed for higher-level jobs. Since the workforce is expected to work in areas that require qualifications such as the development, design, programming and optimization of production processes and the technologies used in these processes and where brain power will come to the forefront, it is important to increase the qualifications of the existing workforce and to have the qualifications to work in these areas. offers. In this regard, the quality of technical and vocational education will be increased. New programs for digital technologies will be developed and implemented in universities, and the workforce will be trained in a way that will meet the requirements of the digital age.

State of the Art in the Secondary Education

It is one of the issues that is considered very important to place the perception of cyber security in students in secondary schools and to carry out studies in this field. Turkey is among the countries that have started to accelerate their efforts in this sense.

With the new regulations, Technology and Design courses in the 7th and 8th grades, and Information Technologies and Software courses in the 5th and 6th grades are included in the curriculum as compulsory courses. With these courses, it is aimed to bring digital awareness to students at an early age. This situation can be considered as a serious step in the formation of the perception and awareness of cyber security.

Some of the main objectives of Technology and Desing course is listed below;

- To gain basic information about the technology development process,

- To gain basic information about the concept of design, its types and process,
- To take responsibility for the solution of the problems they encounter in daily life and to solve these problems.
- To enable them to use technology development processes and design skills in their solution,
- To help designers understand the processes of identifying the problem and developing the most appropriate solution proposal according to the conditions,Technology and design knowledge; sustainable development of society, economy and natural resources
- To realize the interaction between the individual, environment, society and technology,
- To raise awareness about their capacities and to raise awareness among students,
- Helping to develop problem identification, solving and application skills,
- To gain career awareness about technology and design, To realize the importance of occupational safety measures in technology and design processes,
  To raise awareness that it can be producted through Information on the origin and future of advances in different technological fields (energy, transportation, informatics, etc.).
- To provide information on concepts such as invention, invention, discovery, science, technique, industry,

After the 8th grade, when it comes to high school, it is seen that only computer science course is included in the curriculum. Computer Science is a course that focuses entirely on problem solving and programming. As an elective, it is preferred that the course approach be consistent with the desired course. Within the scope of the course, computers, tablets, and robot kits can be used. It is possible for individuals and institutions with different technological infrastructures to diversify their practices by selecting different titles from the curriculum. As part of this course, which consists of two courses in total, students are expected to devote two hours per week to discussing the basic subjects of Level 1 and learning text-based programming. This level allows students to select the programming language they wish to learn (Phyton, C, Java, etc.). A variety of approaches suitable for teaching programming are available at Level 2.

It is very important that the emphasis on digital subjects is increased and that they can be integrated with all other courses. In this sense, it is considered very important to ensure the adaptation of students to digital transformation, awareness and a wide range of knowledge in the pre-university education processes.

However, with the “Cyber Security School”, which was established in 2020 and is the first in Turkey, it has been officially announced that the focus is on the development of the domestic cyber security ecosystem and closing the qualified manpower gap in this field. It is a testament to the high level of interest in the field.

Number of new studies and projects are also ongoing by the Turkish Government. Fatih Project aims to provide equal opportunities in education and improving the technology in schools using information technology to engage more senses in the educational process, which was created with 5 main principles for success;

- Accessibility: Offering service any where regardless of time and tools;
- Productivity: Providing target-oriented and more productive environments and subjects for development;
- Equality (Equal Opportunities) : Enabling all users to access the best service;
- Measurability: Providing accurate measurements of the process and results and providing feedback accordingly for a better assessment of the development;
- Quality: Enhancing the quality of education in a measurable way.

FATİH Project in Education involves much more than hardware and education. An important role is played by it in energizing the domestic economy as a multi-faceted service.

1. Within the scope of the project, the following will be achieved: Increasing domestic production and added-value, and producing goods which haven’t been produced domestically; Conducting research and development activities for new technologies and products; Creating an opportunity for accessing information technology hardware, software, network infrastructure and Internet to be provided to all schools and classrooms, and e-content; Providing e-books to students and teachers, and developing young entrepreneurship spirit.

2. 21st century citizenship skills such as Technology use, Effective communication, Analytical thinking, Problem solving, Cooperation and Collaboration will be developed within FATİH Project in Education.

3. In order to enable easier access to information, the Project aims to establish 'information technology classrooms' with necessary hardware in all schools where teachers and students will be provided with the opportunity to access technology.

The project has different innovations and aims for different levels and environments which are shown below:

For every school	For every classroom	For every teacher	For every student

VPN- Broadband Internet Access	Interactive Board	EBA Applications	EBA Market
Infrastructure	Wired/Wireless Internet Access	Eba Market	Eba Market
High Speed Access		Cloud Account	Cloud Account
		Sharing Course Notes	Digital Identity
			Sharing Homework
			Individual Learning Materials

Another study conducted by the Turkey Strategic Technology Transformation Research Center (TÜSİDAM) entitled with “81 İlde 81 Siber Kahraman” (81 Cyber Heroes in 81 Cities) aims to prepare talented young people for the future of the country with the activities organized in the field of cyber security throughout Turkey.

As a result of awareness seminars and applied training programs held in 20 cities within the scope of the project, thousands of students' cyber security awareness has been increased.

In the organized training camps, trainings are given to the participants under the following main headings. Trainings are also turned into practice with competitions.

- Introduction to Information Security
- Introduction to Cyber Security
- Introduction to Basic Information Technologies
- Vulnerability Analysis
- Network Security
- System Security
- Web Security
- Security Technologies
- Attack Techniques and Applied Hacking Simulations

State of the Art in the Higher Education

As in the industry, many studies and projects are carried out in the field of education in terms of digitalization throughout Turkey. Higher Education Council (YÖK) is at the center of studies related to higher education.

Within the scope of the cooperation between YÖK and CISCO in the field of digital education initiated in 2020, the project, which started with 8 pilot universities in Anatolia within the scope of the "Digital Transformation in Higher Education Project", offers a high level of expertise in subjects that are very critical in today's world such as cyber security and network management. It aims to increase the awareness of students and academicians in educational institutions and to increase the supply of qualified personnel.

In addition, within the scope of the "Training Powerful Generations for the Next Decade" project, YÖK Doctoral Scholarships are given in 100 thematic fields in domestic state universities in order to meet the need for human resources with doctorate degrees in priority areas determined by the Council of Higher Education. Some of these areas are listed as follows:

- Network Technologies
- Cyber security, cryptology
- Data Science and Cloud Computing (including Big Data Technologies)
- Artificial Intelligence, Machine Learning, Augmented and Virtual Reality (including Artificial Neural Networks)
- Software and Systems Engineering
- Distance Education Applications (including Measurement and Evaluation Techniques, Virtual Laboratory Applications, Digital Game Technologies in Education)
- Digital Platforms and Social Media (including Social Media Management)
- IT-Law

Another relevance study relating to higher education is “YÖK Virtual Laboratory Project” As part of this project, general chemistry and general physics laboratory courses are being offered online in a wide range of university programs, especially in science and engineering faculties. Initially, the project was offered to 15 thousand students in 24 universities involved in the Digital Transformation Project.

In addition to these, many universities are now offering certificate programs in "Digital Transformation Management/Expertise." In addition to artificial intelligence, big data, augmented reality, the internet of things, and design thinking, these programs cover a wide range of topics related to digital transformation. Furthermore, the programs equip participants with information on choosing key technology projects and managing portfolios, as well as advice on creating smart and connected products.

The Higher Education Council and the Digital Transformation Office signed also the 'Protocol on the Opening of Cyber Security Vocational Schools' in the fourth quarter of 2022. In this partnership, the Digital Transformation Office's Vocational Schools will contribute to the employment of graduates with its technical, infrastructure, and expert assistance, and the

Digital Transformation Office is expected to serve as a bridge between the IT sector, the labor market and universities.

Moreover, graduate programs related to cyber security are actively continuing education at Turkish universities. In light of technological transformation, all these indicate that the country responds positively to the demands of the age.

Cyber Awareness of the Target Group

Karacı & Bilgici (2017) examined the cyber security behaviors of university students studying in a department related to information technologies. The study group consists of a total of 170 students studying in Computer Engineering and Computer Education and Instructional Technologies Departments of a state and a foundation university. According to the results of the study, it is seen that students' behaviors towards cyber security are at a level that will provide cyber security. When a more detailed examination was made according to the factors, it was seen that the students were able to protect their personal privacy, avoid untrusted applications and take precautions for security. In addition, they are able to protect payment information such as credit or debit cards, and it has been observed that they do not leave a trace when surfing the Internet. There was no significant difference between the cyber security behaviors of boys and girls.

Yiğit & Seferoğlu (2019) examined the cyber security behaviors of university students according to the five factor personality traits and the variables such as gender, grade level, department, status of receiving information security training and weekly Internet usage. Based on the findings, students exhibited acceptable levels of cyber security behavior. Furthermore, although students considered themselves conscientious, open to experience, and agreeable, they remained neutral about whether they were extroverted or neurotic. Additionally, cyber safety behaviors were significantly correlated with five personality dimensions: openness to experience, conscientiousness, agreeableness, neuroticism, and extroversion. Cyber security behavior levels were found to be more adequate among students from CEIT and computer programming departments, those in third and fourth grades, and those who received information security training.

Another study conducted by Karakaya & Yetgin (2020) aims to measure the personal cyber security perceptions of academic and administrative staff working at Karabuk University. The results show that there are significant differences in employees' perceptions of personal cybersecurity according to the age, location and gender of the individuals. Accordingly, it has become necessary for all employees to have sufficient knowledge about cyber danger and social engineering issues that may come from the outside, to individually apply basic computer, password and internet security.

In the study carried out by Tuğal et al (2021), it is discussed why universities, which have many weak links against cyber threats, are the target of cyber attacks. Establishing and complying with information security policies, providing users with cyber awareness training, strengthening information systems infrastructures are listed as important results of the study.

Avcı & Oruç also examined cyber security behaviors and information security awareness of university students. As a result of this study, it is seen that the awareness of university students about providing personal cyber security and information security, is generally at high levels. However, also the results show that there are students with little or no awareness. This issue varies according to the students' departments or the number of their social media accounts.

The study was conducted by Cengizalp (2021) to determine the level of digital data security and cyber security awareness among university employees in the information technology departments. Based on the findings of the study, it appears that there is a weak positive relationship between awareness of providing digital data security and awareness of providing personal cyber security. In addition, it was observed that employees' awareness of providing digital data security and personal cyber security differed significantly by variables of age, professional experience, educational background and position. Furthermore, it has been found that the awareness of providing digital data security and personal cyber security by employees in university information technology departments is high. These awareness's are shaped by gender, age, professional background, and educational background.

In order for young people to fight against cyberbullying/victimization, they should be familiar with the concept of cyberbullying and develop coping skills. The aim of the study carried out by Şener et al. (2022) is to determine the cyber bullying and cyber victimization levels and cyber security awareness of university students during the COVID-19 pandemic.While the frequency of cyberbullying and the scale score were very low among the students, it was found that three out of every 10 students experienced cyber victimization and the scale score was not very high.

In their research, Talan and Aktürk (2021) investigated the levels of digital literacy and information security awareness of secondary school students in Gaziantep and Kilis provinces in TRC1. Information security awareness is significantly higher among students who use the internet for more than 7 hours per day. Despite this, it was observed that students' information security awareness levels did not differ significantly depending on the amount of time they spent on social media. Moreover, males are more aware of information security than females, according to the study

Hızmalı & Tosun (2022) also examined the digital data security awareness levels of university students and the relationship of this concept with various variables in their research, in which

2.500 associate, undergraduate and graduate students were used. Students are highly aware of digital data security, according to the results. It has been determined that there are differences among students in terms of their awareness of digital data security depending on their gender, household income level, educational level, and amount of time spent on the internet. In terms of awareness scores, male students tend to score higher than female students, undergraduate students tend to score higher than associate degree students, and people who spend less than 1 hour a day are more aware than people who spend more than 8 hours a day. Additionally, the average digital data security awareness score increases as family income increases. It has been determined that students expect the university administration to open courses and inform them through seminars or conferences on digital data security in order to increase awareness and knowledge.

References

TALAN, T., & AKTÜRK, C. (2021). Orta öğretim öğrencilerinin dijital okuryazarlık ve bilgi güvenliği farkındalığı seviyelerinin incelenmesi. *Kahramanmaraş Sütçü İmam Üniversitesi Sosyal Bilimler Dergisi*, *18*(1), 158-180.

Avcı, Ü., & Oruç, O. (2020). Investigation of the Students' Personal Cyber Security Behaviour and Information Security Awareness.

Gündüzalp, C. (2021). Üniversite çalışanlarının dijital veri ve kişisel siber güvenlik farkındalıkları (bilgi işlem daire başkanlıkları örneği). Journal of Computer and Education Research, 9(18), 598-625.

Hızmalı, A. M., & Tosun, N. (2022, August). Üniversite Öğrencilerinin Dijital Veri Güvenliği Farkındalıklarının Çeşitli Değişkenler Açısından İncelenmesi. In The 14th International Scientific Research Congress (p. 137).

KARACI, A., AKYÜZ, H. İ., & BİLGİCİ, G. (2017). Üniversite öğrencilerinin siber güvenlik davranışlarının incelenmesi. Kastamonu Eğitim Dergisi, 25(6), 2079-2094.

KARAKAYA, A., & YETGİN, M. A. (2020). KARABÜK ÜNİVERSİTESİ ÇALIŞANLARINA YÖNELİK KİŞİSEL SİBER GÜVENLİK ÜZERİNE ARAŞTIRMA. Kahramanmaraş Sütçü İmam Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi, 10(2), 157-172.

Şener, H., Arıkan, İ., & Gülekçi, Y. (2022). COVID-19 Pandemisinde Üniversite Öğrencilerinin Siber Güvenlik Farkındalıkları ile Siber Zorbalık ve Siber Mağduriyet Düzeylerinin Değerlendirilmesi.

TUĞAL, İ., ALMAZ, C., & Mehmet, S. E. V. İ. (2021). Üniversitelerdeki Siber Güvenlik Sorunları ve Farkındalık Eğitimleri. *Bilişim Teknolojileri Dergisi*, *14*(3), 229-238.

YİĞİT, M. F., & SEFEROĞLU, S. S. (2019). Öğrencilerin siber güvenlik davranışlarının beş faktör kişilik özellikleri ve çeşitli diğer değişkenlere göre incelenmesi. *Mersin Üniversitesi Eğitim Fakültesi Dergisi*, *15*(1), 186-215.

www.yök.gov.tr (Official web page of Council of Higher Education)

www.meb.gov.tr (Official web page of Ministry of National Education)

www.tuik.gov.tr (Official web page of Turkish Statistical Institute)

www.teknofest.org

ANALYTICAL REPORT ON THE NATIONAL DESKTOP ANALYSIS IN ITALY

Introduction

The desktop analysis (R1A1) is carried out in order to shed light on the focus group study (R1A2) and to prepare an infrastructure for it. As a result of the A1, it is aimed to have an idea about the target group, to create the questions that should be used in the focus group study and to ensure the integrity of the subject by combining the current literature directly or indirectly related to the subject of the project in the partner countries.

After an informative and guiding introduction part, the report should include national bibliographic reviews in five different countries. After a general introduction to the subject, the report should include national bibliographic reviews in five different countries. Subsequently, the conclusion section will be formed by presenting the current local situations, developing suggestions on the issues that are considered important but with lack of studies on a national basis.

Bibliographical Research

The Italian institutional and legislative framework governing cybersecurity is currently in the making, and is being developed around the ACN (National Cybersecurity Agency), established with the Decree-Law No. 82 of 14 June 2021, transformed with amendments into law No. 109 of 4 August 2021. Such legislative developments demonstrate Italy's growing acknowledgement of the complexity of the cyber threat, starting with the tight connection between the state's cybersecurity and national defence. In order to gain a better understanding of the state of the art, this chapter provides a brief description of the main normative developments which have outlined the legislative and institutional framework for cybersecurity in Italy since 2013, as well as an analysis of the newly-established Agency.
In Italy, cyber defence is set within the broader cybersecurity framework. Following a series of initiatives at the European Union and NATO level, Italy established its first structure for national cybersecurity and critical infrastructures protection through a Decree of the President of the Council of Ministers (Decreto del Presidente del Consiglio dei Ministri – DPCM) of 24 January 2013, also known as Decreto Monti. 6 The Decreto Monti identified the Security Intelligence Department (Dipartimento delle Informazioni per la Sicurezza – DIS) as the entity tasked with the protection of Italy's cybersecurity, notwithstanding that the tasks identified by Decree are actually different from the duties historically carried out by the DIS as an intelligence agency. The Decree also established the National Cybersecurity Management Board (Nucleo per la Sicurezza Cibernetica – NSC), aimed at providing operative support in the event of cyber crises of national relevance, and an inter-ministerial board responsible for the prevention and management of such crises. Moreover, according to the Decree, the Interministerial Committee for the Security of the Republic (Comitato Interministeriale per la Sicurezza della Repubblica – CISR) was in charge of advising the President of the Council of Ministers concerning the national strategic framework for cyberspace and cybersecurity strategic

objectives, through the National Plan for Cyberspace Protection and ICT Security (Piano nazionale per la sicurezza dello spazio cibernetico). In addition, the CISR had to elaborate guidelines for possible cooperation between public and private entities, disseminate best practices for cyberspace protection, and advocate activities aimed to ensure an Italian presence in international cooperative frameworks, including NATO and the EU.

The Italian cybersecurity institutional and normative framework evolved according to the DPCM of 17 February 2017 (Decreto Gentiloni),7 then followed by the National Plan for Cyberspace Protection and ICT Security (Piano nazionale per la protezione cibernetica e la sicurezza informativa).8 The need to rationalise and simplify a complex institutional landscape, in an attempt to create synergies and economies of scale in a coordinated fight against the cyber threat, led to the evolution of the national cyber architecture.

Following the implementation of the Decreto Gentiloni, the DIS gained further duties and became both an operative actor of the cybersecurity structure and an entity responsible for defining guidelines in order to safeguard this domain and respond in the event of crises. A further and relevant change introduced by the decree consists in the establishment of a National Centre for Evaluation and Certification (Centro di valutazione e certificazione nazionale – CVCN).9 The CVCN is tasked with verifying security standards of technological products that will be employed within national critical infrastructures.10 The relevance of private entities for the determination of national cybersecurity levels was already acknowledged in the Decreto Monti.

Such awareness led to the drafting of the Decree-Law No. 105 of 21 September 2019, defining the National Cybersecurity Perimeter according to the procedures later defined by the DPCM No. 131 of 30 July 2020. The aim of the Cybersecurity Law Decree is to establish the national cybernetic security perimeter and to introduce suitable measures to guarantee safety standards for networks and information systems as well as IT services for public administrations, private and public national entities and operators, which perform essential functions of the State or provide essential services in the civil, social and economic fields and whose malfunction may cause a national security risk.

The national legislative framework on cybersecurity has been further regulated by the Decree-Law 82/2021. Amended by law, the decree introduces several changes to the national cybersecurity architecture, such as the establishment of the ACN. The institution of the Agency is one if the initiatives implemented through the Italian Recovery and Resilience Plan (Piano nazionale di ripresa e resilienza – PNRR),17 which the MoD intends to support through its expertise and the structures at its disposal. The law establishes regulatory, administrative, patrimonial, organisational, accounting and financial independence of the Agency, while the President of the Council of Ministers holds the high management and the general responsibility of national cybersecurity policies (Article 2). Among the major changes introduced by the Decree-Law is the relocation of the national cybersecurity architecture from the DIS to the ACN, still governed by public law, which will report directly to the President of the Council of Ministers. The ACN will work closely with the Intelligence System for the Security of the Republic (Sistema di informazione per la sicurezza della Repubblica) through the Cyber Security Unit (Nucleo per la cybersicurezza), namely the institution established to replace the NSC. The Unit encompasses the ACN Director General and Deputy Director, the Prime Minister's Military Advisor, representatives of the DIS, of the Internal Intelligence and Security Agency (Agenzia Informazioni e Sicurezza Interna – AISI) and of the External Intelligence and Security Agency

(Agenzia Informazioni e Sicurezza Esterna – AISE), all Ministers involved in the CISR,19 and representatives of the Ministry of University and Research, of the Ministry for Technological Innovation and Digital Transition and of the Civil Protection Department. The Unit is responsible for organising and planning the response in the event of cyber crises, as well as coordinating interministerial exercises and the Italian participation in international drills. The Agency is the sole national reference institution in cybersecurity, and it is responsible for the drafting of the national cybersecurity strategy and for ensuring the regular development of common actions meant to reach higher levels of national resilience.

Many times the damage of cyber attacks depends on an identifiable weak link. The weak link in cybersecurity is the human factor; One of the main reasons for the success of cyber attacks in various areas is the lack of an adequately skilled cybersecurity workforce. Italy also suffers from a shortage of professionals in the area of cybersecurity, exacerbated by the flight of young people, trained in our universities, but attracted abroad by more attractive salaries. Given the pervasiveness of cybersecurity in the professional, educational, academic to the broader context, i.e., the social context, aspects related to training on the topic, as highlighted in the National Cybersecurity Laboratory's 2018 white paper, must therefore be addressed along six complementary lines: 1- Advanced training, 2- Basic education, 3- Vocational training, 4- Search for talent, 5- Coaching, 6- training and citizen awareness measures.
At the national level, it is therefore necessary to initiate a systemic action for training on safe use of the Web, as a technological knowledge enhancement and social security initiative for the country, pursuing the following objectives:
- National Framework for Awareness Raising and Continuing Education - To develop a structured path at the national level for the definition of a Framework as a reference model for continuing education on the issues of network security and the conscious use of digital tools, within which to place educational action.
- Minimal citizen controls and cyber-hygiene-(1) Define a set of minimal citizen controls and a set of cyber-hygiene ground rules that must be systematically followed. (2) Identify and activate the most appropriate mechanisms for the maximum dissemination of these minimal controls and basic cyber-hygiene rules.
- Public-private-third sector cooperation-Promote and incentivize a virtuous model of cooperation between the public, private and third sectors for the enhancement and systemization of the initiatives already in place today, in a wide variety of forms, throughout the country.

State of the Art in the Secondary Education

Italy as most EU countries have been left behind in the domain of secondary schools due to the uneven distribution of educational programs in cybersecurity or because cybersecurity content is not included in their high-school programs at all.
According to the report “Teaching cybersecurity in high school—Our way to turn ideas into practice” by the Concordia team and its Survey among EU High-School students, Teachers, and Parents (2021-2022), the answers to the question “Is cybersecurity taught at the survey participant’s high school at all” were not very encouraging as cybersecurity is not really part of

the high school program, and in those schools where it is included, the time dedicated to topics dealing with cybersecurity is scarce (including the Italian respondents). The majority of teachers replied to the question with Yes, but with the comment that cybersecurity content is a part of computer courses with 2–3 h per month. The majority of parents replied with "I don't know" and many of students replied negatively. The results show that even if cybersecurity topics are part of the curriculum and are taught in high schools in other forms, students and parents are unaware of it.

Student answers on the risk related question do not show differences related to students' country of origin. The average values regarding the awareness of high school students is situated between agree and strongly agree. At the same time, when the teachers and parents were asked the same questions regarding the risk awareness of students the average values were neutral to confident respectively. A distinct difference between the perspective regarding risk of the high-school students and the teachers of high-school students was noticed in all countries, in Italy too.
Finally, the findings of the Concordia team survey have shown that one of the most desired delivery methods for teaching Cybersecurity Education for High-School Students selected by all involved audiences were serious or educational games (in Italy as well).

State of the Art in the Higher Education System

According to recent studies carried out in Europe, education for developing sustainable skills is not sufficiently integrated with European High Educational Level programs (HEI). The active pedagogical activities that help strengthen this vision are not yet included within the majority of HEI cybersecurity programs. Actions for addressing the increased cybersecurity skills shortage have been launched in Europe in the last few years but as reported by the European Cyber Security Organization (ECSO), and by other organizations, they are not sufficiently viewed by the European HEI as an emerging discipline important for developing the sustainability of the digital society. This finding comes from the analysis of the contents of European HEI programs; it was found that these programs focus mainly on traditional cybersecurity topics as part of classical academic courses. Modern learning methodologies with hands-on training and range platforms that help in building skills have been left behind in the European HEI, Italy included.
The building of cybersecurity skills among higher education students and the related topics of cybersecurity within educational programs have not yet been studied at large in Italy as well as in Europe, even though children start using the internet at an early age and more than 90% of young Europeans are online every day.
According to recent surveys, the following are the online activities for which the EU students (including the Italian ones) voted to be discussed during cybersecurity courses, in descending order: On-line social media platforms (e.g., Facebook, Instagram, Twitter) 84%, Recognizing fake accounts/websites/emails 70%, Creating strong password for on-line accounts and devices, 49% Securely downloading applications/software/data, 49% Ensuring that the privacy of students is respected in on-line activities, 45% Using email applications in a secure way (e.g., avoiding spams), 38% Being safe when playing on-line games, 31% Provision of secure on-line

shopping, 29% Sharing files on-line (e.g., Dropbox, OneDrive) and being safe regarding who can access the files.

The following are some of the training and educational opportunities on cybersecurity at HEI level now available in Italy:

- MSc in Cyber Risk Strategy and Governance

University Politecnica di Milano - 2 years
https://www.masterstudies.com/MSc-in-Cyber-Risk-Strategy-and-Governance/Italy/PdM/

- CYBER SECURITY SPECIALIST 2

University of Prato
https://www.pin.unifi.it/cybersecurity

- Advanced Training Courses "Advanced Training Course in Cyber Security Management"

School of Management-LAM University

Cyber Awareness of the Target Group

In Italy Cybersecurity has increasingly become a headline feature in news media in recent years also in Italy, generally prompted by spectacular security breaches in various information systems. The importance of cybersecurity awareness for the sustainable development of society is now recognized widely, but the problem of how to build an educational ecosystem which will include the most relevant target audiences that need to develop cybersecurity skills, is not yet solved. In that context, skills are understood to represent a combination of abilities, knowledge, and experience that enable an individual to successfully complete a task when working in a digital environment and using digital services.
The biggest concerns in the education on cybersecurity are the lack of hands-on experience in students, which results in a skills mismatch between the needs of the emerging digital society in this regard and the skills that the majority population needs to adopt to effectively use digital services.

Conclusion & Recommendations

The answers collected during the focus group session were relevant for the general aim of the project: important comments and observations from teachers, researchers, lecturers and students of non IT HEIs were collected becoming the basis for the future development of Cyber in Practice Nuggets training content. The focus groups, despite the fact that there were different types of targets groups, showed a precise and heterogeneous framework of knowledge, awareness and limits of the participants concerning cyber security issues. This level of competence and knowledge of cyber security issues was quite low and insufficient, taking into consideration the fact that the only information they have are about the most common risks of cyber attacks and the basic methodologies and tools to be applied in case of informatics attack. Malware, Ransomware, Phishing, spam, Data appropriation & person substitution, email and message scams are the problems they know, however not all of the respondents would be able to avoid these threats successfully. The results show a low level of awareness among students and academic staff of non-IT HEIs; even though the interviewees are able to

understand the basic concepts of cyber security, the most common risks of cyber attack and the easier procedure to react in case of cyber attacks, the level of knowledge and awareness is not sufficient yet.

With regard to the security at University using the learning environment, all the respondents agreed on the fact that they feel “safe” when using the university network or accessing websites and platform with personal account for learning reasons, however they are often not conscious enough of risks and not aware of both risks and ways of dealing with them. Their lack of awareness about the risks that could occur if some cyber attacks showed up is an important starting point of our thinking and analysis that will guide us in the development of the training contents.

ANALYTICAL REPORT ON THE NATIONAL DESKTOP ANALYSIS IN BULGARIA

Introduction

According to the Project proposal, the needs analyses on cyber security awareness is planned to be carried out through 2 major steps:

- R1-A1 The National Desktop Analysis to be developed by all participating countries; and
- R1-A2 Analysis of the results from the Focus Group interviews held in each partner country.

Then, based on these national survey-based and focus groups analyses, a Synthesis Report should be developed by the lead partner.

The present document refers to the first task R1-A1 Analytical Report on the National Desktop Analysis in Bulgaria.

From the Bulgarian team, responsible for the implementation of this task was Sen. Ass. Svetlana Syarova, PhD. She distributed the specific tasks among the members of the Bulgarian team. The entire work process was coordinated by the project leader of the Bulgarian team, Assoc. Prof. Eugenia Kovatcheva.

A number of national and European documents outlining information technology education policy and cyber security in particular, were studied. The national training programmes in the secondary education and in the system of higher education institutions were studied in detail.

The list of the examined documents is published at the end of the document.

The analysis in this report is structured into 5 main sections:

- The Background section outlines the main Bulgarian and European policy documents on the basis of which the current education system in Bulgaria is developing. A general overview of the development of the academic disciplines related to the study of ICT, including the elements of Cyber-security, was made at the national level;
- The peculiarities in structuring the educational content in ICT and cyber-security are examined in the 2 main sections:
    - Cyber Security in the Secondary Level of Education in Bulgaria; and
    - Cyber Security at the Level of Higher Education in Bulgaria;
- Section Conclusions and Recommendations outlines the main conclusions of the desktop research held and based on them, the recommendations that shall be taken in considerations when defining the strategy for the future project implementation.
    -

Background

The systematic monitoring, planning and application of information and communication technologies (ICT) in school education marks its beginning in the last decade of the last century. It is carried out within the framework of the PISA, PIRLS student achievement assessment programmes of the Organisation for Economic Co-operation and Development (OECD) using data from national statistical

institutes and Eurostat. In a joint report by Eurostat and the Eurydice information network on education in Europe for 1999/2000, one of the sections is devoted to ICT indicators in the field of education.

In 2001, a systematic study of the Eurydice for their application in educational systems was also published. With the establishment of the European Union (EU) and the adoption of the Lisbon Strategy, the application of ICT in school education is a major indicator for tracking progress. This provides a better understanding of the nature and scope of national initiatives in this area. Programs are being developed to implement the measures identified in the strategies.

The “Minerva” Sectoral Programme within the Socrates Programme (2000-2006), Lifelong Learning Horizontal Activities (2007-2013), Erasmus+ Programme (2014-2020) , the priority axes and measures of the EU Structural Funds support initiatives and projects that contain clear potential and expected results in the field of implementation of Information and Communication Technologies, open access methods and resources and distance learning in different contexts and at different levels of the education.

At the current stage, ICT priorities are outlined in the European Union Strategy for Smart, Sustainable and Inclusive Growth "Europe 2020" and more specifically in: "The Digital Agenda for Europe 2020" adopted in 2010 and The "Digital Single Market Strategy" approved in May 2015. The priorities in the field of education are presented in the "Strategic Framework for European Cooperation in Education and Training ('ESET 2020')" and the plans for its implementation.

In November 2017, a special action plan on digital education was announced at the Gothenburg Summit. In this regard, the European Commission is taking new initiatives to improve the key competences and digital skills of European citizens. The new European Skills Agenda proposes a revised European Reference Framework for Key Competences for Lifelong Learning, which sets out the knowledge, skills and attitudes people need in their lives, including digital competences. The Digital Education Action Plan (DEA Plan) describes how education and training systems can make better use of innovation and support the development of relevant digital competences for living and working in today's information society. The action plan sets out three priority directions: a) better use of digital technologies for teaching and learning; b) developing the digital competences and skills necessary for life and work in an age of digital transformation; c) improving education through better data analysis and prediction. Initiatives include helping schools with high-speed broadband connections, wider use of self-assessment tools on the use of technology for teaching and learning in schools, and a public awareness campaign on online safety, media literacy and cyber security. Three European frames have been developed which aim to provide a common basis for discussions and analyses at national, regional and local levels. They offer a consistent set of tools for self-reflection and monitoring aimed at citizens and learners (DigComp), teachers (DigCompEdu) and schools (DigCompOrg).

General Analysis at a National Level

According to the Digital Europe Progress Report, Bulgaria ranks last in the European Commission's Digital Inclusion Index (DESI 2020), although its overall score has risen to 36.4%. The share of people with at least basic digital skills is around 29%, while the EU average is 58%. This indicator has maintained its values since 2017. Only 11% of people have skills above basic, which is less than a third of the EU average. A similar trend is seen among young people: 54% of 16-24 year olds have at least basic digital skills (compared to an EU average of 85%). Only 31% of Bulgarians have basic software skills, compared to the EU average of 61%. The report states that this indicator is strongly influenced by socio-demographic aspects.

According to a study of the competences of teachers with the DigCompEdu toolkit, a significant share of them - 42.4% - have digital skills at level A 2 - researcher.

In the current programme period, the development of ICT in school education is planned in the "Strategy for effective application of information and communication technologies in education and science of the Republic of Bulgaria (2014 - 2020)". Although the measures taken and their implementation activities are not fully in sync with the scale of the digital transformation, the emphasis on improving the digital skills of students and pedagogical specialists has been strengthened. From the academic year 2018-2019, the subject of computer modelling is introduced in the third grade, and in the upper secondary education, more hours focused on ICT are planned. According to the national programme "Training for an IT career", extracurricular activities are implemented in the secondary schools. In 2019, the National Programme "Digital Bulgaria 2025" was adopted, one of the goals of which is the modernisation of school education in the field of information and communication technologies. Main measures related to: provision of adequate infrastructure in the field of ICT in schools are planned; assessment of students' digital competences upon completion of the first high school stage (grade X); modernization of educational content and teaching methods; introduction of the study subject "Computer Modelling" at the initial stage and introduction of training in the "Software and Hardware Sciences" profile; improving the skills of teachers; strengthening cooperation between education, industry and the non-governmental sector; establishing a coordinated approach for effective measures in the field of digital skills and employment.

The continuous and increasing digitisation in society, as well as changes in the technology itself, mean that strategies and policies are rapidly becoming obsolete. European countries must constantly review and develop new strategies, policies and measures to meet the new demands for high-quality digital education.

Cyber Security in the Secondary Level of Education in Bulgaria

"Information Technologies" subject in the Bulgarian school

The subject “Information technologies” was introduced for the first time in the Bulgarian school in 1994 in the ninth grade of the secondary education. From 1999 to 2000, it was studied in the compulsory preparation of the ninth and tenth grades. Subsequently, two levels of preparation (compulsory preparation and profiled preparation) are distinguished for the subject of Information Technologies in the high school stage (IX - XII grades). Since 2006, Information Technology has been studied by students as a compulsory subject in junior high school and primary education.

The core set of information technology knowledge and skills acquired in secondary education are a foundation of digital competences on which students improve their future professional skills and increase their confidence and self-esteem.

The goal of creative use of the possibilities of modern information technologies for communication is clearly set in school education in information technology. When determining the state educational standard for general education in the ORDER No. 5 of 30.11.2015 (of the Ministry of Education and Science), the expected knowledge, skills and attitudes in the area of competence "Electronic communication" are described in detail. For example, for the junior high school stage of the basic level of education we read: "Knows the applications of the Internet for communication and information sharing, interacts in a networked environment for data exchange and use of shared resources, collaborates through digital channels, has an idea of the importance of electronic communications for the functioning and development of society in the secondary course".

The Communication is one of the five areas included in the European Digital Competence Self-Assessment Framework and this includes knowledge and skills in: using a wide range of communication tools (mobile devices, SMS, e-mail, chat, video conferencing, blogs, social networks, etc.); create and manage files for collaboration, collaboration, data exchange, and file and application sharing.

With the entry into force of the new Law on Preschool and School Education, promulgated in SG No. 79 of 13.10.2015, in force from 01.08.2016, the subject “Information Technologies” is studied as a general educational preparation for 1 hour per week (total 34 hours per year) in junior high school stage of education (grades V - VII), 1 hour each per week (total 36 hours per year) in the first high school stage of education (grades VIII – X). "Computer Modelling" is studied 1 hour per week (total 32 hours per year in grade III and total 34 hours per year in grade IV) in the initial stage of education (grades I - IV).

Information technology training is aimed at mastering knowledge, skills and attitudes related to building students' digital literacy. The curricula contain topics that cover all areas included in the European framework for self-assessment of digital competences (Digital competencies - Self-assessment grid - Europass - Europa EU, 2018), (A common European Digital Competence Framework for Citizens, 2018): information processing, content creation, communication, cyber security and problem solving. The more important of them are presented in the subsections below:

Communicate safely on the Internet

Attention is paid to safe communication on the Internet and the concept of "online bullying" is analysed. The characteristics of online bullying are outlined, the risks and pitfalls of the Internet are indicated. Forms of cyberbullying are discussed.

Attention is paid to technical safety and virus protection, which are important skills in the digital environment.

Basic rules are outlined to help students stay safe online. It is important that students know the ways to seek help outside the school (Bulgarian Centre for Safe Internet https://www.safenet.bg/bg/).

Protection of intellectual property

The protection of intellectual property includes a large number of international agreements prepared with the help of the World Intellectual Property Organisation (WIPO) and the World Trade Organisation (WTO). In addition, the European Union has created additional laws aimed at achieving more effective protection of intellectual property. One part of them regulates the protection of: trademarks, patents and copyrights.

International agreements related to the protection of intellectual property, various license agreements for the use of author's works and their designations are briefly discussed in the secondary school curricula.

The table 1 below presents the topics related to cybersecurity, distributed by class and the knowledge that should be acquired at the end of the training course.

Table 1

Grade	Topics	Acquired knowledge
3 grade	Electronic communication and digital identity	He/she distinguishes between digital and physical identity. Knows the main threats when working in a digital environment and knows where to seek help.
	Safe and responsible online behaviour	Knows the basic rules and threats when working in a digital environment. He knows how to get help. Recognizes false information on the Internet.
4 grade	Information in modern society	Understands that digital resources may not be free to use, copy and distribute. Understands that not all information in the virtual space is reliable.
	Safety conditions in a digital environment	Does not provide personal data in a digital environment. Knows more known threats when working in a digital environment. Knows how to get help when needed. Knows ethical norms when working in an online environment.

6 grade	Real-time communication tools. Rules for children's safety on the Internet	Describes real-time communication software settings for security purposes; Knows the possibilities of real-time communication on the Internet. Knows and follows the rules of safe behaviour on the Internet.
7 grade	Means and methods of information protection	Explains the nature of computer viruses Explains and applies specific means and methods to protect information.
	Use of antivirus programs	Uses an anti-virus program, making the necessary settings; Recognizes security system messages and responds appropriately.
	Computer system and data protection in it - exercise	Improve your skills to: selection of computer configuration components; recognition of threats and viruses in the computer world; use of anti-virus programs.
	Social networks and protection of personal privacy	Gives examples of popular social networks; Respects the right to privacy on the Internet; Describes the actions to be taken in case of violation of his personal privacy in a social network; Sets settings to protect his personal information when using a social network.
	Internet	Improve your skills to: dealing with different situations when communicating in social networks; protection of content shared by him in a social network.
9 grade	Information security in a networked environment	Understands the risks associated with working in a networked environment and implements appropriate protection measures; Knows basic regulatory documents related to: personal data protection, copyright (for programs and data) and electronic signature; Knows the principles, main ways and means of protecting the network from unauthorized access; Sets access rights to resources on a local network. Researches major security threats such as viruses, worms, hacker attacks; Prioritizes threats; It searches the web and selects the best protections for each of the top three priority security threats.
10 grade	Assessing the validity and reliability of information	Understands information dissemination mechanisms and effective ways of searching in an online environment; Evaluates information received electronically for credibility and reliability; Filters e-mail messages to categorize them as spam; Researches in which countries spam is declared illegal and punishable and what is the legal framework for it in Bulgaria.
	Technical and organizational security when working in a digital environment	Gives examples of problems that arise when working in a networked digital environment and possible solutions; It indicates ways of reliable digital identification when using public services; Knows the purpose of macros in office applications and knows how to manage their inclusion when using public services; Uses online tools to identify compromised networks; Identifies the presence of a macro in a document; Examines what biometric data is used for identification; Checks if a personal device offers biometric identification; Compares identification methods that can be used to use electronic banking.
11 grade	Security and data protection	Lists security and data protection risks; Describes basic methods and means of data protection; Describes basic data backup methods; Describes components of the main regulatory documents related to the ethical use and guarantee of privacy of personal data.

Cyber Security at the Level of Higher Education in Bulgaria

The ever-growing role of the new technologies in education and training brings to the fore the need to increase the digital culture of students and acquire certain skills and competences for learning in a digital environment.

The Cybersecurity knowledge is the need for a broad competence and practical skills of every student in the virtual educational space, even in the computer room, in the classroom, regardless of the scope of the studied discipline and specialty. It means new in nature scientific qualification and competence, high responsibility and demandingness. It is a definite necessity imposed by the will of the real world.

The rapidly emerging digitalization and the implementation of artificial intelligence, combined with the generational characteristics of learners, increased international cooperation and the desire to ensure equal access to education for all layers of society have placed qualitatively new requirements on the nature and characteristics of teaching. Part of the answers to these challenges were given through the opening of academic programmes in distance learning, equipping halls, creating the necessary infrastructure, virtual libraries, etc. At the same time, the system proved to be understaffed and unprepared to meet the demands and expectations for innovative methods and forms of teaching. This necessitates the creation of a programme for the training of teachers and professors in the field of information and communication technologies (ICT), who in turn train pupils and students with skills and attitudes for learning in an electronic environment. The lack of sufficiently qualified teachers in higher education institutions who possess digital skills corresponding to modern trends and requirements is the result of several factors. In the last decade, the increased demand for ICT personnel on the labor market has led to a great interest on the part of prospective students in these specialties and, accordingly, to the opening of the corresponding professional directions in many higher schools. At the same time, the system proved to be unprepared in terms of the required number of trained teachers. The likelihood that more graduate students will choose an academic career and become a teacher is decreasing due to the high income that comes with working in the specialty in the real sector. Naturally, deficits in the higher education system affect the functioning of the preschool and school education system as well.

The improvement of the quality of higher education with a view to digital transformation is in accordance with the Law on Higher Education, the Strategy for the Development of Higher Education in the Republic of Bulgaria for the period 2021 - 2030, the policies for the development of state higher education institutions, the Conclusions of the Council of the EU on digital education in the European knowledge societies and the Rome Communiqué of the Ministers of the Member States of the Bologna Process.

In the digital environment, which is a basic element of the information society (A. Toffler) or in the network society (M. Castells), the ability to make a quick and adequate decision, to make a choice and to take responsibility for the choice turns out to be a cornerstone before the personal and professional success of the modern young man. Giving the opportunity to choose, develops cognitive and non-cognitive competences, teaches the young person to balance the rational and emotional component in every decision and action. Achieving a balance in the development of cognitive and non-cognitive competences is set as measure 1.1.2 in the Strategic Framework for The Development of Education, Training and Learning In The Republic of Bulgaria (2021 - 2030). In it, the topic of digitization of the university educational process is set, or as it is precisely said, "universal digitization". The issue of the regulation of copyright and the protection of intellectual property in the conditions of a digitized, electronic and online learning environment is touched upon.

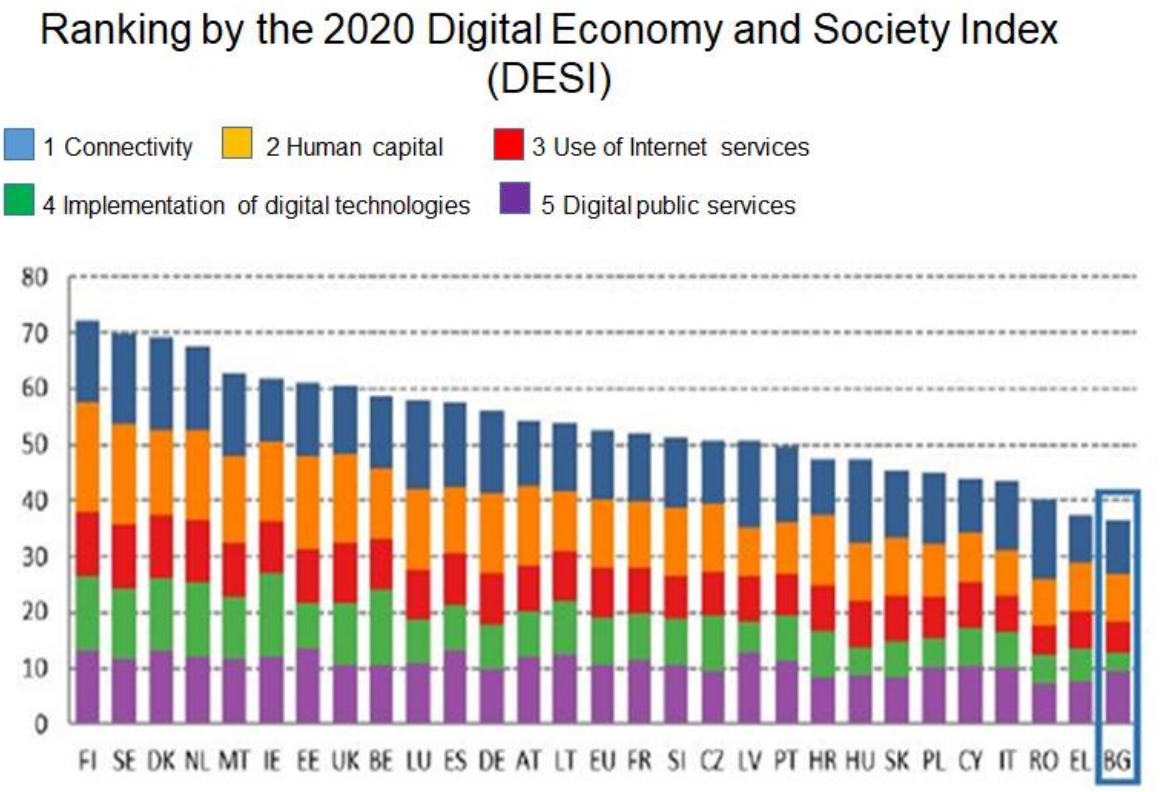
More and more professional environments require at least basic skills in working with digital devices, and without them it is very difficult to carry out any professional realization. On 11.05.2021, the Industrial Capital Association (ICA) signed a contract for the implementation of project BG05M9OP001-1.128-0004 "Development of Digital Skills". The project is financed by the Operational Programme (OP) "Development of human resources 2014-2021", under procedure BG05M9OP001-1.128 - Development of digital skills - Component 2 (2021).

"The main goal of project BG05M9OP001-1.128-0004 "Developing our Digital Skills", which ICA is implementing, is to contribute to bringing digital skills and knowledge in line with the needs of business, and hence accelerating digitalization in Bulgarian enterprises. Through its implementation, a connection will be ensured between the necessary knowledge and skills and the requirements of the future labour market to achieve a competitive and developing economy, based on technological development and providing sustainable jobs", said Dr. Milena Angelova, Secretary General of the Association and a Project Manager.

Based on the conducted research, 67 key professions/positions were identified, as well as the basic and specific digital skills required for each one of them. They are divided into five categories, according to the European Digital Competence Framework DigComp 2.1. These are 'Information and data literacy', “Digital communication and collaboration”, “Digital content creation”, “Safety' and 'Problem solving”. In addition, we can say that training is increasingly closely related to digital skills. Retraining and acquiring new competencies is also unthinkable without digital knowledge and skills.

In the EU document "DIGCOMP - a Framework for Developing and Understanding Digital Technologies in Europe" (Ferrari, Punie & Brecko, 2013), digital competence is described as the confident, critical and creative use of ICT to achieve work-related goals, suitability for employment, training, recreation, inclusion and/or participation in society. Digital competences are seen as a cross-cutting key competence enabling people to acquire other key competences such as language, mathematics, study skills or cultural awareness.

Despite all the factors, digitization in Bulgaria is still at a low level compared to the other countries of the European Union. At the beginning of June 2020, the European Commission published the annual report Index on the penetration of digital technologies in the economy and society (DESI - Digital Economy and Society Index). It compares EU Member States and their digital progress across five indicators – connectivity, human capital, use of internet services, adoption of digital technologies and digital public services (2020). According to the human capital indicator, Bulgaria has climbed 2 places in the ranking, but despite this, the skills of citizens in the field of digital technologies are among the lowest in the EU. Basic digital skills are possessed by 29% of the adult population (for comparison, this share amounts to 58% on average for the EU), and slightly above the average level – 11%. According to DESI 2020, Bulgaria needs to increase the digital skills, increase the qualification and requalification of the elderly population, and participation in adult learning is low. This is a serious reason to review and stimulate the development of these skills.



https://www.ipa.government.bg/bg/indekst-desi-po-vreme-na-covid-19-i-kde-e-blgariya

Fig. 1

The system of higher education in Bulgaria includes 49 higher education institutions, of which 36 are public and 13 are private. Higher education institutions in Bulgaria are of three main types: universities, specialized higher education institutions and independent colleges. They train students, doctoral students and specialists.

The Higher education in Bulgaria is compatible with the European one and includes the following degrees:

- Professional Bachelor in... – with the acquisition of no less than 180 credits and a minimum period of preparation of 3 years according to the curriculum;
- Bachelor's Degree – with the acquisition of no less than 240 credits and a minimum period of preparation of 4 years according to the curriculum;
- Master's Degree - with the acquisition of no less than 300 credits and with a study period of 5 years according to the curriculum or no less than one year after a "bachelor's" degree (60 credits), respectively no less than two years after "Professional Bachelor of..." (120 credits);
- Doctor - educational and scientific degree after the master's degree.

The preparation in each of the degrees is conducted in accordance with the Classifier of Higher Education Areas and Professional Fields. There are 9 areas of higher education divided into 52 professional fields. Within the framework of academic autonomy, each higher education institution

independently determines the professional areas and specialties in which it conducts training. The forms of education are regular, part-time and distance learning.

Table 2 below contains a list (in alphabetical order) of the universities, higher schools and colleges in Bulgaria.

Table 2

No	University
1	Agricultural University Plovdiv
2	Academy of Music, Dance and Visual Arts - Plovdiv
3	Academy to the Ministry of Internal Affairs - Sofia
4	American University in Bulgaria - Blagoevgrad
5	Burgas Free University
6	Varna Free University "Chernorizets Hrabar"
7	University of Veliko Tarnovo "St. St. Cyril and Methodius"
8	Higher Naval School "Nikola Yonkov Vaptsarov" - Varna
9	Lyuben Karavelov Higher School of Construction - Sofia
10	"Todor Kableshkov" Higher Transport School - Sofia
11	Higher School of Agribusiness and Regional Development - Plovdiv
12	Higher School of Insurance and Finance - Sofia
13	Higher School of Management - Varna
14	Higher School of Security and Economics - Plovdiv
15	Higher School of Telecommunications and Posts - Sofia
16	Military Academy "Georgi Stoykov Rakovski" - Sofia
17	Varna University of Economics
18	College of Management, Trade and Marketing - Sofia
19	College of Tourism - Blagoevgrad
20	Forestry University - Sofia
21	Medical University - Pleven
22	Medical University - Plovdiv
23	Medical University of Sofia
24	Medical University "Prof. Dr. Paraskev Stoyanov" - Varna
25	International Business School - Botevgrad
26	University of Mining and Geology "St. Ivan Rilski" - Sofia фия
27	Vasil Levski National Military University - Veliko Tarnovo
28	National Academy of Theater and Film Art "Krastyo Sarafov" - Sofia
29	National Academy of Music "Prof. Pancho Vladigerov" - Sofia
30	Vasil Levski National Sports Academy - Sofia
31	National Art Academy - Sofia
32	New Bulgarian University - Sofia
33	Paisii Hilendarski University of Plovdiv
34	Rousseau University "Angel Kanchev"
35	Sofia University "St. Kliment Ohridski"
36	Business Academy "Dimitar Tsenov" - Svishtov

37	Theater College "Lyuben Groys" - Sofia
38	Technical University Varna
39	Technical university-Gabrovo
40	Technical University of Sofia
41	Thrace University - Stara Zagora
42	University "Prof. Dr. Asen Zlatarov" - Burgas
43	University of National and World Economy - Sofia
44	University of Architecture, Construction and Geodesy - Sofia
45	University of Library Science and Information Technologies - Sofia
46	University of Food Technology - Plovdiv
47	Chemical Technology and Metallurgical University - Sofia
48	Shumen University "Bishop Konstantin Preslavski"
49	Southwest University "Neofit Rilski" - Blagoevgrad

Higher education institutions in Bulgaria are of three main types: universities, specialized higher education institutions and independent colleges. They train students, doctoral students and specialists.

The Higher education in Bulgaria is compatible with the European one and includes the following degrees:

- Professional Bachelor in... – with the acquisition of no less than 180 credits and a minimum period of preparation of 3 years according to the curriculum;
- Bachelor's Degree – with the acquisition of no less than 240 credits and a minimum period of preparation of 4 years according to the curriculum;
- Master's Degree - with the acquisition of no less than 300 credits and with a study period of 5 years according to the curriculum or no less than one year after a "bachelor's" degree (60 credits), respectively no less than two years after "Professional Bachelor of..." (120 credits);
- Doctor - educational and scientific degree after the master's degree.

The preparation in each of the degrees is conducted in accordance with the Classifier of Higher Education Areas and Professional Fields. There are 9 areas of higher education divided into 52 professional fields. Within the framework of academic autonomy, each higher education institution independently determines the professional areas and specialties in which it conducts training. The forms of education are regular, part-time and distance learning.

The bachelor's degree is the main stage of higher education. The training period is 4 years. Training programmes are aimed at acquiring fundamental knowledge in the chosen field, which have an applied nature. The training in the master's programmes is focused on the acquisition of more in-depth theoretical knowledge in a narrower specific area of the discipline, which is necessary for those who will engage in research and continue with the next (doctoral) degree.

For this reason, the study is focused on undergraduate (Bachelor) studies.

In figures 2 and 3 below a comparison of universities by number of bachelor's programmes studied in them is shown.

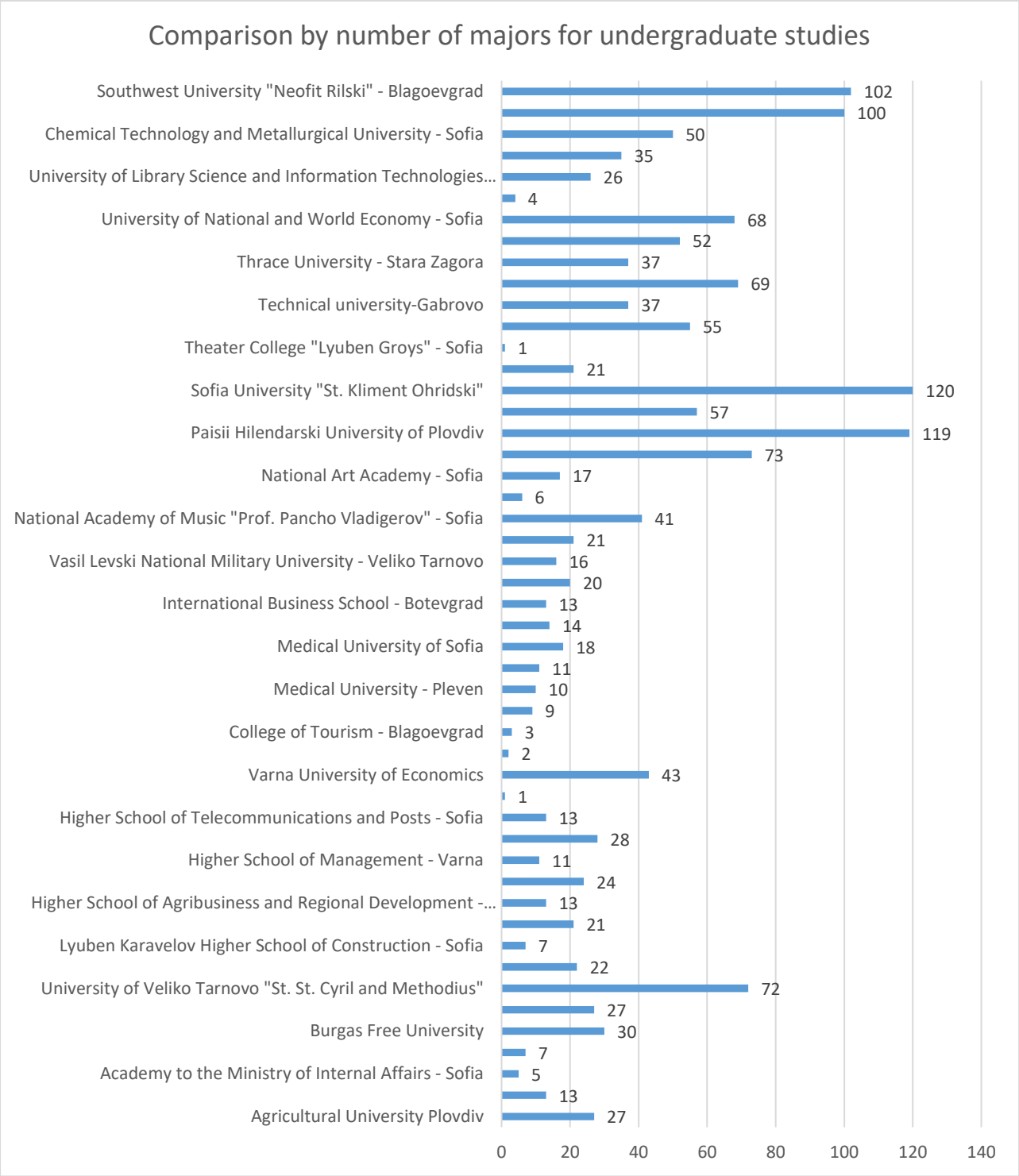

Comparison by number of majors for undergraduate studies
Southwest University "Neofit Rilski" - Blagoevgrad
102
100
Chemical Technology and Metallurgical University - Sofia
50
35
University of Library Science and Information Technologies...
26
4
University of National and World Economy - Sofia
68
52
Thrace University - Stara Zagora
37
69
Technical university-Gabrovo
37
55
Theater College "Lyuben Groys" - Sofia
1
21
Sofia University "St. Kliment Ohridski"
120
57
Paisii Hilendarski University of Plovdiv
119
73
National Art Academy - Sofia
17
6
National Academy of Music "Prof. Pancho Vladigerov" - Sofia
41
21
Vasil Levski National Military University - Veliko Tarnovo
16
20
International Business School - Botevgrad
13
14
Medical University of Sofia
18
11
Medical University - Pleven
10
9
College of Tourism - Blagoevgrad
3
2
Varna University of Economics
43
1
Higher School of Telecommunications and Posts - Sofia
13
28
Higher School of Management - Varna
11
24
Higher School of Agribusiness and Regional Development -...
13
21
Lyuben Karavelov Higher School of Construction - Sofia
7
22
University of Veliko Tarnovo "St. St. Cyril and Methodius"
72
27
Burgas Free University
30
7
Academy to the Ministry of Internal Affairs - Sofia
5
13
Agricultural University Plovdiv
27
0
20
40
60
80
100
120
140

Fig. 2

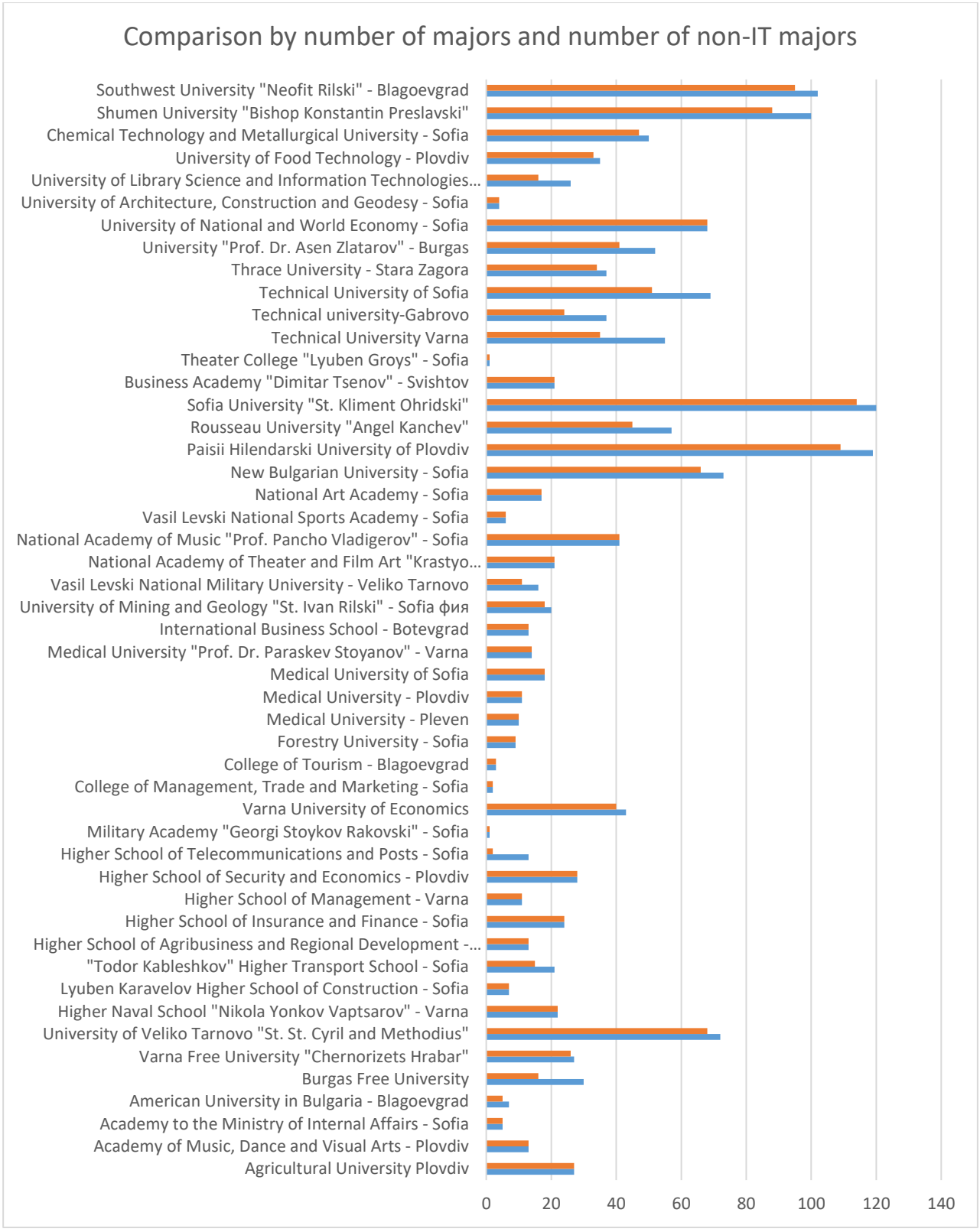

Comparison by number of majors and number of non-IT majors
Southwest University "Neofit Rilski" - Blagoevgrad
Shumen University "Bishop Konstantin Preslavski"
Chemical Technology and Metallurgical University - Sofia
University of Food Technology - Plovdiv
University of Library Science and Information Technologies...
University of Architecture, Construction and Geodesy - Sofia
University of National and World Economy - Sofia
University "Prof. Dr. Asen Zlatarov" - Burgas
Thrace University - Stara Zagora
Technical University of Sofia
Technical university-Gabrovo
Technical University Varna
Theater College "Lyuben Groys" - Sofia
Business Academy "Dimitar Tsenov" - Svishtov
Sofia University "St. Kliment Ohridski"
Rousseau University "Angel Kanchev"
Paisii Hilendarski University of Plovdiv
New Bulgarian University - Sofia
National Art Academy - Sofia
Vasil Levski National Sports Academy - Sofia
National Academy of Music "Prof. Pancho Vladigerov" - Sofia
National Academy of Theater and Film Art "Krastyo...
Vasil Levski National Military University - Veliko Tarnovo
University of Mining and Geology "St. Ivan Rilski" - Sofia фия
International Business School - Botevgrad
Medical University "Prof. Dr. Paraskev Stoyanov" - Varna
Medical University of Sofia
Medical University - Plovdiv
Medical University - Pleven
Forestry University - Sofia
College of Tourism - Blagoevgrad
College of Management, Trade and Marketing - Sofia
Varna University of Economics
Military Academy "Georgi Stoykov Rakovski" - Sofia
Higher School of Telecommunications and Posts - Sofia
Higher School of Security and Economics - Plovdiv
Higher School of Management - Varna
Higher School of Insurance and Finance - Sofia
Higher School of Agribusiness and Regional Development -...
"Todor Kableshkov" Higher Transport School - Sofia
Lyuben Karavelov Higher School of Construction - Sofia
Higher Naval School "Nikola Yonkov Vaptsarov" - Varna
University of Veliko Tarnovo "St. St. Cyril and Methodius"
Varna Free University "Chernorizets Hrabar"
Burgas Free University
American University in Bulgaria - Blagoevgrad
Academy to the Ministry of Internal Affairs - Sofia
Academy of Music, Dance and Visual Arts - Plovdiv
Agricultural University Plovdiv
0
20
40
60
80
100
120
140

Fig. 3

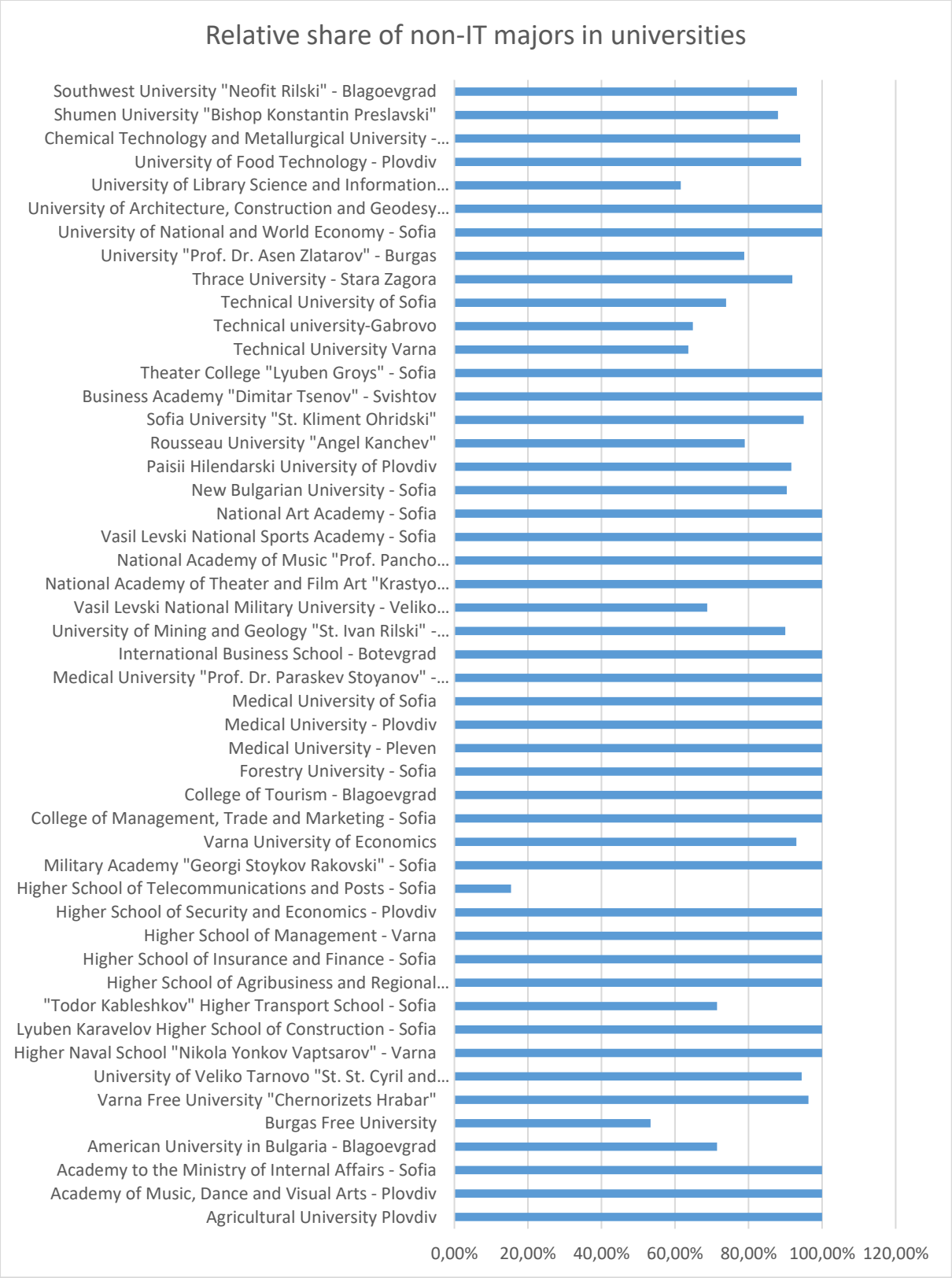


Fig. 4

In the context of a widespread dependence on increasingly complex digital systems, cyber threats are outpacing societies' ability to effectively prevent and manage them. The main reasons for this are

related to the development of information and communication technologies (ICT), the digitization of production processes and the ubiquitous use of electronic devices and networks to support various business activities. As a result of the electronic interaction at all levels in the organisations, the development of electronic commerce and business, of various electronic services, huge amounts of data are accumulated in terms of volume, variety and rate of growth and change, including sensitive information about employees, customers, products, finances, etc. Quite naturally, the big data collected and used by organisations has become a strategic resource, with a view to extracting useful knowledge from it and improving decision-making and management processes. At the same time, digital assets are subject to deliberate and accidental threats, due to the presence of vulnerabilities in the protection of information systems.

As a result of the above-mentioned factors and their constant development and redefinition, the educational system opens up many new opportunities, but also many new problems and challenges.

Today, there is a need for a new vision in teaching and building literacy for working with data, which also includes ensuring information safety when working with modern ICT. Universities are realizing the need for new innovative programs covering information security training even in non-technical (non-IT) specialties.

The curricula in the higher education institutions are built on the understanding that ICT skills are sufficiently formed in secondary school and can be the basis for successful upgrading with specific skills. The observations show that the entry level of ICT with which first-year students enter is satisfactory and cannot be a good basis for a successful upgrade. The Secondary school curricula are focused mainly on theoretical knowledge in the field, and practical performance tasks remain isolated from real-world situations. As a result, after exiting the specific learning content, the ICT tasks cannot be recognised. In this situation, students choose to find and take a ready-made solution to the problem, which they present as their own, because they do not have the necessary competence to perform the task and the requirements set for it. In this way, they do not actively participate in the individual stages of the process of building the information product and do not independently walk the path to the final decision. Their training remains at the level of an ordinary computer-literate user of information resources who uses technology at a superficial level.

The digital training of future specialists is an actual task for all levels of educational structures. It is a guarantor of adequate interaction between specialists and society. In order to form the components of digital competence - interactive use of technologies and didactic interpretation of the possibilities of ICT, higher education institutions should direct the training to concrete deepening of the available knowledge and skills. For this purpose, it is necessary to diagnose the level of ICT knowledge and skills possessed by first-year students, to find out where the gaps are and the most frequently occurring errors. This diagnosis will guide the way in which ICT training should be conducted for first-year students. Realising the potential of ICT requires students to have a basic level of preparation to recognize the basic activities they can perform with the computer. The students must be able to solve basic tasks that involve specific sequences of activities. They need to be able to name and explain the activities performed. This is a prerequisite for the manifestation of reflexive processes that have developing potential for learners.

In the higher education institutions, there is no special training on the use of ICT in the individual fields of study. Each student must independently develop these skills on the basis of the general digital competence that is formed in the first year of higher education. In order for this process to run optimally, it is necessary that the students do not have obstacles of a basic nature in terms of digital competence. ICT training has a clearly expressed practical orientation, which is a prerequisite for students to use technology more often to carry out activities and prepare materials for classroom and extracurricular employment. In this way, a style of working with ICT will be formed, which can be

successfully transferred to another situation. The education at a university requires in the first year to work with students to build the general stage of their digital competence, which is logical, because it is assumed that the first stage - the basic one - is formed in secondary school. Towards the end of the bachelor's degree studies, it is expected that the professional stage of the students' digital competence has been formed. Practice shows that there are discrepancies between expectations and reality.

Every student, as an individual user of Web technologies, as a networked citizen of the digital society, must pass the way from elementary school computer literacy to continuously upgraded high digital literacy, which means knowing the relevant standards, directives, regulations, normative and subnormative acts and instructions, to comply with the requirements, norms and have developed behaviour and practical habits. Areas of conduct that everyone must comply with are also identified such as: etiquette, communication, education, access, commerce, responsibility, rights, safety and security. In summary, key areas are formed: digital competence, digital ethics, digital sensitivity and digital participation. Each student as a user must take care of their own cybersecurity immune system, as one unwise or even inadvertent action can destroy the global immune system of society.

There is a wide variety of IT subjects studied in non-technical university specialties that touch on fundamental aspects of ICT and build applied knowledge and skills. Such are basic disciplines such as Information Technology, Information Systems, Informatics, Digital Technologies, Information Systems and Technologies, Information and Communication Technologies, etc. In some cases, the disciplines aim at both the formation of basic information and digital skills and competences, as well as their orientation in a specific field, for example the discipline "Information and communication technologies in education and work in a digital environment" in the specialty "Primary school pedagogy" or "Digital Technologies in Agriculture" in the specialty "Agricultural Engineering", etc.

The figure 5 below presents comparison of studying IT in nonIT specialties:

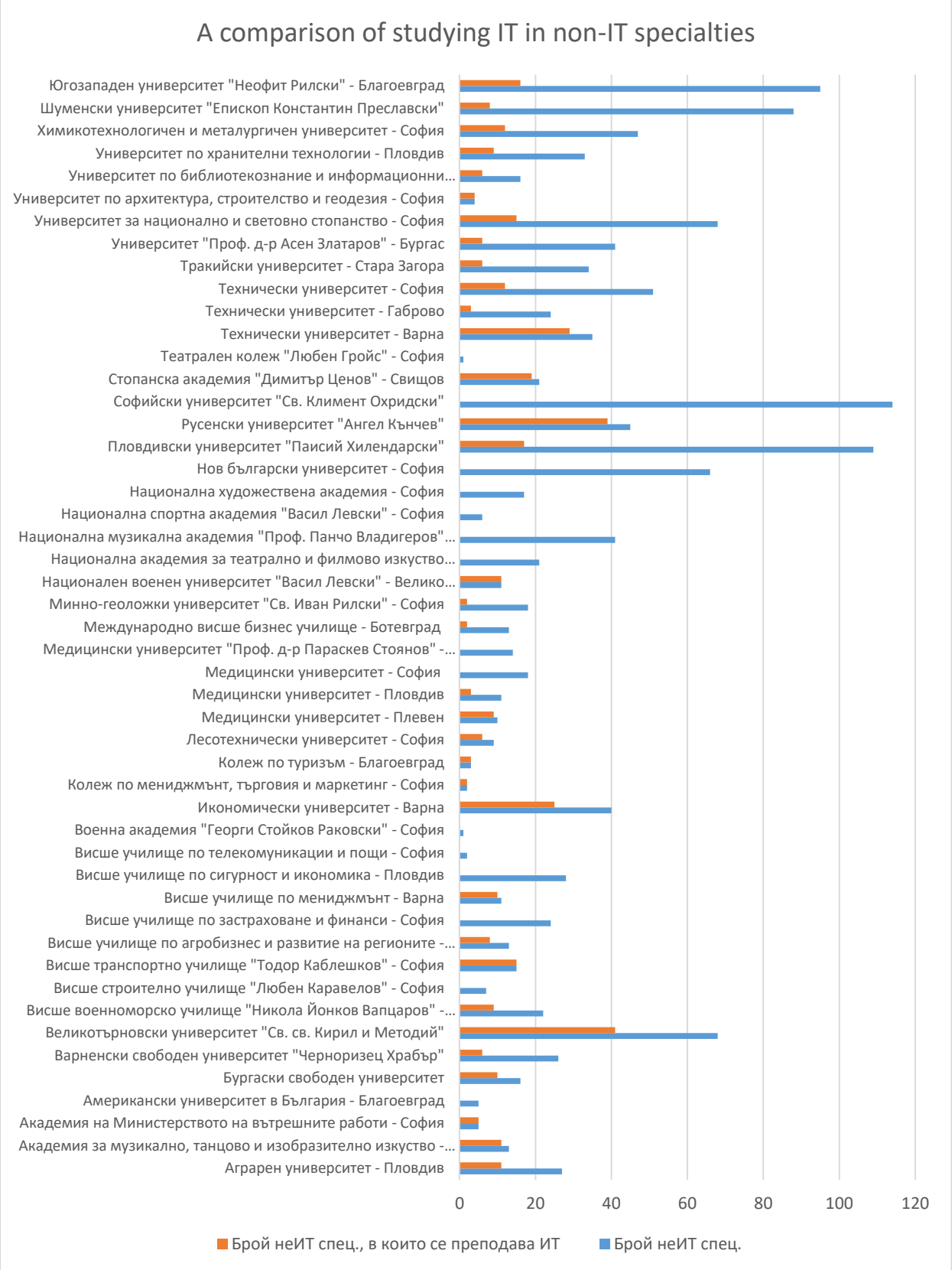


Fig. 5

The figure below presents comparison of studying IT in nonIT specialties:

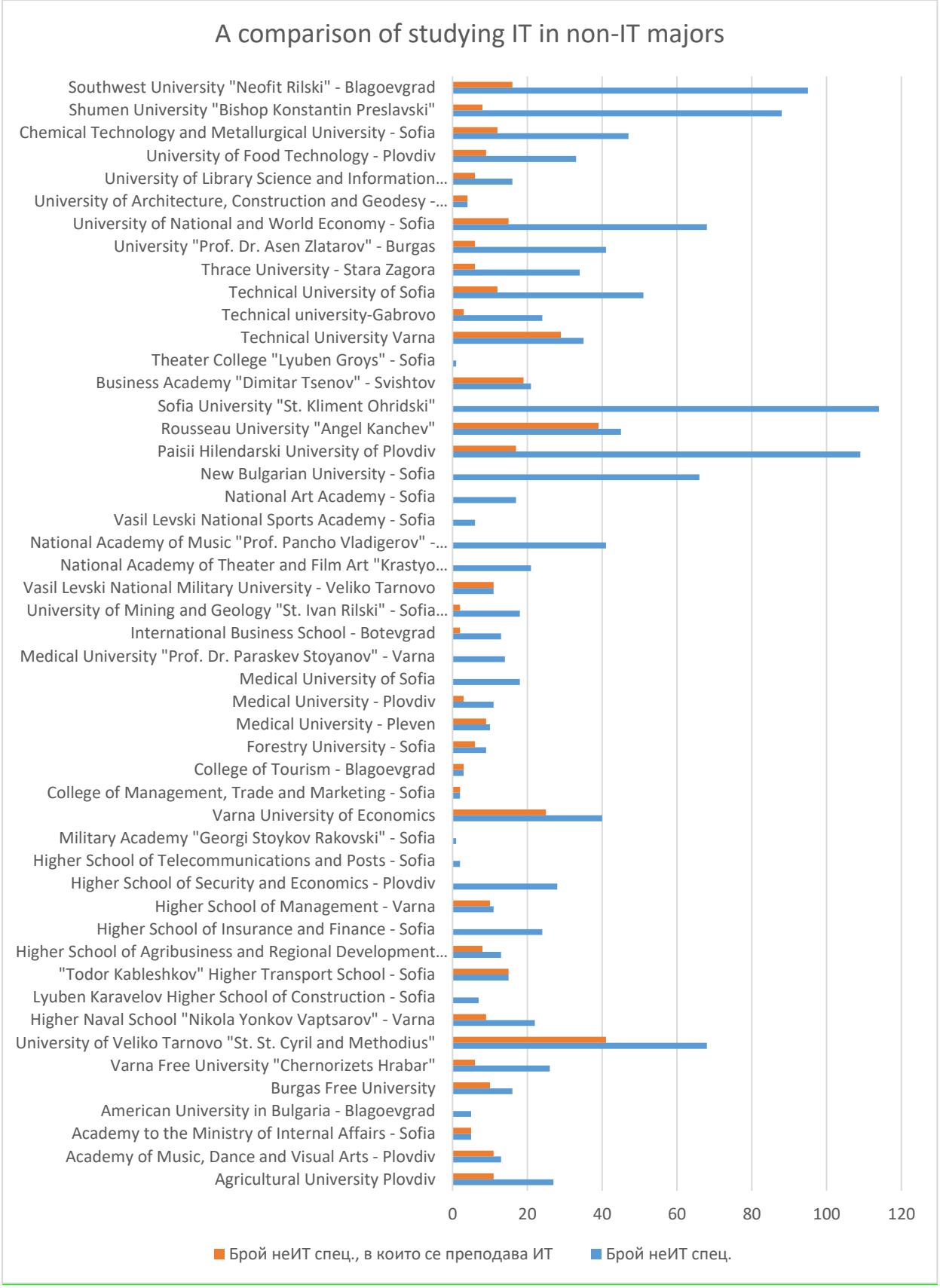

A comparison of studying IT in non-IT majors
Southwest University "Neofit Rilski" - Blagoevgrad
Shumen University "Bishop Konstantin Preslavski"
Chemical Technology and Metallurgical University - Sofia
University of Food Technology - Plovdiv
University of Library Science and Information...
University of Architecture, Construction and Geodesy -...
University of National and World Economy - Sofia
University "Prof. Dr. Asen Zlatarov" - Burgas
Thrace University - Stara Zagora
Technical University of Sofia
Technical university-Gabrovo
Technical University Varna
Theater College "Lyuben Groys" - Sofia
Business Academy "Dimitar Tsenov" - Svishtov
Sofia University "St. Kliment Ohridski"
Rousseau University "Angel Kanchev"
Paisii Hilendarski University of Plovdiv
New Bulgarian University - Sofia
National Art Academy - Sofia
Vasil Levski National Sports Academy - Sofia
National Academy of Music "Prof. Pancho Vladigerov" -...
National Academy of Theater and Film Art "Krastyo...
Vasil Levski National Military University - Veliko Tarnovo
University of Mining and Geology "St. Ivan Rilski" - Sofia...
International Business School - Botevgrad
Medical University "Prof. Dr. Paraskev Stoyanov" - Varna
Medical University of Sofia
Medical University - Plovdiv
Medical University - Pleven
Forestry University - Sofia
College of Tourism - Blagoevgrad
College of Management, Trade and Marketing - Sofia
Varna University of Economics
Military Academy "Georgi Stoykov Rakovski" - Sofia
Higher School of Telecommunications and Posts - Sofia
Higher School of Security and Economics - Plovdiv
Higher School of Management - Varna
Higher School of Insurance and Finance - Sofia
Higher School of Agribusiness and Regional Development...
"Todor Kableshkov" Higher Transport School - Sofia
Lyuben Karavelov Higher School of Construction - Sofia
Higher Naval School "Nikola Yonkov Vaptsarov" - Varna
University of Veliko Tarnovo "St. St. Cyril and Methodius"
Varna Free University "Chernorizets Hrabar"
Burgas Free University
American University in Bulgaria - Blagoevgrad
Academy to the Ministry of Internal Affairs - Sofia
Academy of Music, Dance and Visual Arts - Plovdiv
Agricultural University Plovdiv
0
20
40
60
80
100
120
Брой неИТ спец., в които се преподава ИТ
Брой неИТ спец.

Fig. 6

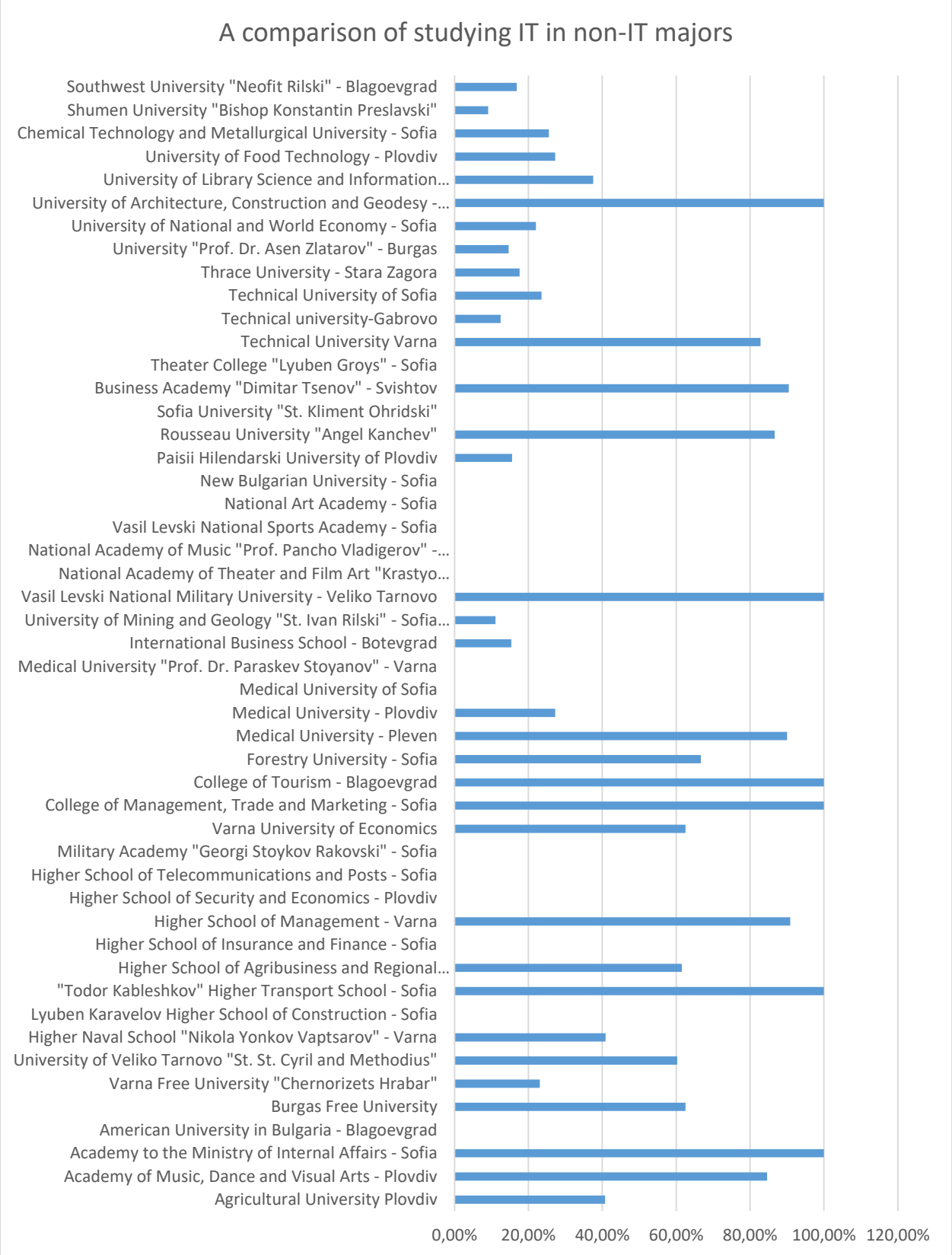

A comparison of studying IT in non-IT majors
Southwest University "Neofit Rilski" - Blagoevgrad
Shumen University "Bishop Konstantin Preslavski"
Chemical Technology and Metallurgical University - Sofia
University of Food Technology - Plovdiv
University of Library Science and Information...
University of Architecture, Construction and Geodesy -...
University of National and World Economy - Sofia
University "Prof. Dr. Asen Zlatarov" - Burgas
Thrace University - Stara Zagora
Technical University of Sofia
Technical university-Gabrovo
Technical University Varna
Theater College "Lyuben Groys" - Sofia
Business Academy "Dimitar Tsenov" - Svishtov
Sofia University "St. Kliment Ohridski"
Rousseau University "Angel Kanchev"
Paisii Hilendarski University of Plovdiv
New Bulgarian University - Sofia
National Art Academy - Sofia
Vasil Levski National Sports Academy - Sofia
National Academy of Music "Prof. Pancho Vladigerov" -...
National Academy of Theater and Film Art "Krastyo...
Vasil Levski National Military University - Veliko Tarnovo
University of Mining and Geology "St. Ivan Rilski" - Sofia...
International Business School - Botevgrad
Medical University "Prof. Dr. Paraskev Stoyanov" - Varna
Medical University of Sofia
Medical University - Plovdiv
Medical University - Pleven
Forestry University - Sofia
College of Tourism - Blagoevgrad
College of Management, Trade and Marketing - Sofia
Varna University of Economics
Military Academy "Georgi Stoykov Rakovski" - Sofia
Higher School of Telecommunications and Posts - Sofia
Higher School of Security and Economics - Plovdiv
Higher School of Management - Varna
Higher School of Insurance and Finance - Sofia
Higher School of Agribusiness and Regional...
"Todor Kableshkov" Higher Transport School - Sofia
Lyuben Karavelov Higher School of Construction - Sofia
Higher Naval School "Nikola Yonkov Vaptsarov" - Varna
University of Veliko Tarnovo "St. St. Cyril and Methodius"
Varna Free University "Chernorizets Hrabar"
Burgas Free University
American University in Bulgaria - Blagoevgrad
Academy to the Ministry of Internal Affairs - Sofia
Academy of Music, Dance and Visual Arts - Plovdiv
Agricultural University Plovdiv
0,00%
20,00%
40,00%
60,00%
80,00%
100,00%
120,00%

Fig. 7

In the non-IT specialties of the different universities, IT is taught in the interval from 0 to 41 of the cases (grouped into 19 variants depending on the repetitions) in some universities. Fig... shows the graph of the distribution of studied IT disciplines in non-IT specialties.

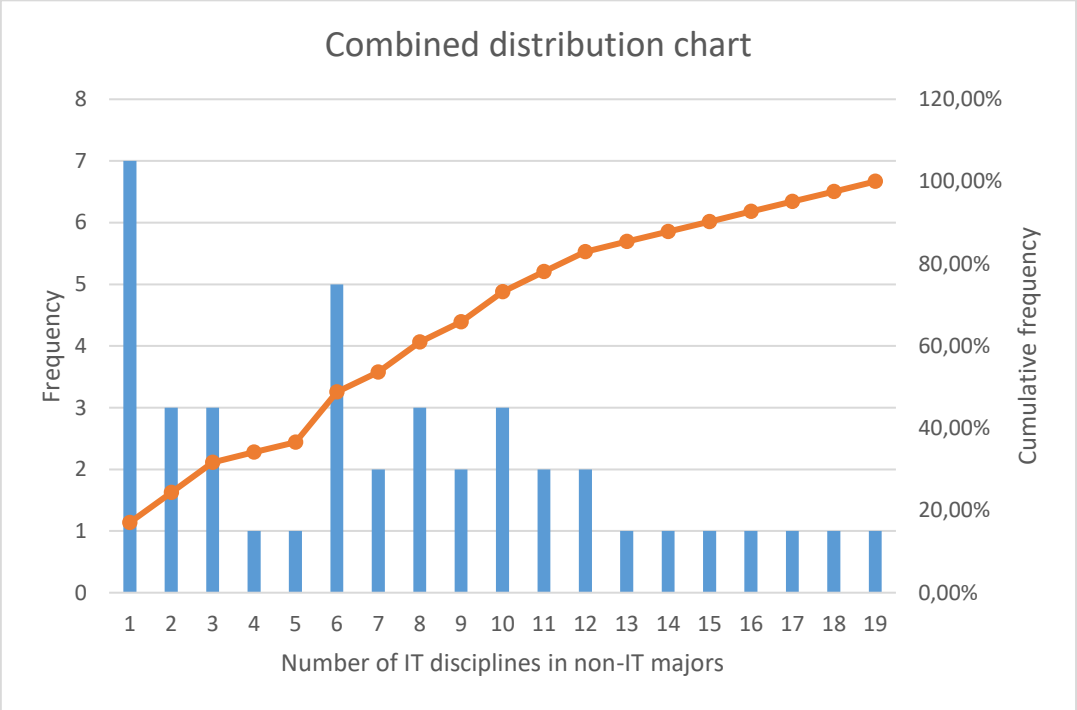


Fig. 8

The study covered 49 universities whose curricula were examined. At some of the universities, the curricula were not available, so the number of universities considered is 41. On average, 9.51 of the non-IT majors in these universities teach IT disciplines. In 7 universities, IT disciplines are not taught in non-IT majors (Minimum = 0), and in one of the universities (Velikoturnovo University "St. St. Cyril and Methodius") in 41 non-IT majors, IT disciplines are taught.

Descriptive statistics	
Mean	9.51
Standard Error	1.52
Median	8
Mode	0
Standard Deviation	9.74
Sample Variance	94.91
Kurtosis	3.31
Skewness	1.74
Range	41
Minimum	0
Maximum	41

Sum	390
Count	41
Largest(1)	41
Smallest(1)	0
Confidence Level(95.0%)	3.074947

Fig. 9

Conclusions and Recommendations

The massive penetration of technology into the daily life and the economy is transforming the possibilities for work, learning, communication, access to information and spending the free time. The result is a global electronic environment that provides new opportunities for communication and interaction to individuals and communities worldwide. Today, the development of all economic spheres strongly depends on data and competencies for their processing and analysis. The Data is all around us, and its volume is growing exponentially, so it needs to be delivered, processed, retrieved and managed, secured, communicated through, made decisions based on, etc.

The adaptation of students to the challenges of the digital society and new learning practices requires determining more effective ways to attract, encourage and motivate them in the direction of acquiring quality theoretical and practical-applied knowledge and skills for working with ICT. The access to computers and the Internet, the ability to work with some basic software applications and tools does not always lead to the acquisition of digital competence by students - many of the young people who come to university do not have the necessary skills to use digital technologies, due to the fragmented and superficial use of information.

In this regard, the efforts of university teachers should be directed to support various appropriate ways of using ICT and interactive communication in the learning process, which can improve students' abilities for critical thinking, effective communication and collaborative scientific problem solving. An important place in this direction is the inclusion of students in various courses to increase their digital competence. The compulsory (not only optional) study courses represented in the curricula of various specialties, are particularly suitable, which would provide the necessary knowledge and skills for using digital technologies.

The competencies related to data security and ensuring proper access to data is another component of data literacy. This raises a number of issues and challenges related to data ownership, privacy and other sensitive areas of data access and transfer. As it becomes clear from the research, in the curricula of non-IT majors, information security does not occupy its important place, which is assigned to it by the current reality of an ever-increasing threat of cyber attacks.

Attracting the students to additional short-term or long-term study courses (paid form of study) can also contribute to the acquisition of important knowledge and skills that are not given enough space in the curricula. The holding of scientific seminars, the possibility of access to online lessons, e-textbooks and other forms of increasing the digital competence of students, through which one can expect to develop a wide range of skills for searching, identification, critical evaluation, should not be underestimated and use of information for a more independent and creative behavior in a digital environment.

In order to master these skills, a solid basic training in ICT is needed, which guarantees the permanent preservation of what has been learned and its transfer to different situations. The sequential passage through the stages of formation of digital competence and the activities involved in them, ensures the transformation of general concepts in the understanding of ICT in the educational process into concrete implementations of individual ideas, reflecting the place and role of ICT in the educational process. With a successful transition from basic ICT skills to digital competence, the cognitive outlook of the students also changes.

References

1. ICT@Europe.edu. Information and Communication Technology in European Education Systems. Eurydice The Information Network on Education in Europe. July 2001;
2. Digital Competence Framework for Educators (DigCompEdu). https://bit.ly/3FuUtg7 ;
3. Socrates Programme (2000-2006), in particular MINERVA sectoral programme. https://bit.ly/3sG7zQi;
4. Lifelong Learning Horizontal Activities (2007-2013);
5. Erasmus+ Programme (2014-2020);
6. Communication from the Commission EUROPE 2020: A strategy for smart, sustainable and inclusive growth. COM (2010) 2020. https://bit.ly/2IXpXvc
7. A Digital Single Market Strategy for Europe. {SWD(2015) 100 final} https://bit.ly/3DlHr26
8. Strategic Framework for European Cooperation in Education and Training ('ESET 2020') https://education.ec.europa.eu/about-eea/strategic-framework;
9. Digital Education Action Plan 2021-2027 https://bit.ly/3DlhVKc;
10. Bulgaria in the Digital Economy and Society Index. https://bit.ly/3U7ds4A;
11. Strategy for effective Application of Information and Communication Technologies in Education and Science of the Republic of Bulgaria (2014 - 2020). https://bit.ly/3DLWuna;
12. National Programme "Digital Bulgaria 2025. https://bit.ly/3TRvEzk;
13. Law on Pre-School and School Education. https://www.lex.bg/bg/laws/ldoc/2136641509;
14. Law on Higher Education in Bulgaria. https://lex.bg/laws/ldoc/2133647361;
15. Ranking of Higher Education Institutions in Bulgaria for 2021. https://rsvu.mon.bg/rsvu4/#/
16. Terziev, Venelin, Prof. Dr. Internal and External Challenges in Front of the Higher Education. https://bit.ly/3fjWmSh;
17. László Tőkés. Report on the Modernization of Higher Education Systems in Europe. Committee on Culture and Education https://bit.ly/3DIwjxB;
18. Hristova, Teodora. Always Connected: Digital Skills among the Students. Postmodernism problems, Volume 7, Number 3, 2017. https://bit.ly/3sHpGFh;
19. Shopova, Tatiana. Development of Digital Competence among Students. Southwest University "Neofit Rilski", Blagoevgrad http://notabene-bg.org/read.php?id=290.

R1/A1

GUIDELINE FOR ANALYTICAL REPORT ON THE NATIONAL DESKTOP ANALYSIS IN ALL 5 PARTNER COUNTRIES

POLAND

ANALYTICAL REPORT ON THE NATIONAL DESKTOP ANALYSIS IN POLAND

Introduction

Social and economic development is more and more dependent on fast and unhindered access to information and its use in the management, production and service sector and by public entities. Continuous development of network and information systems, including analysing larger data sets, helps develop communications, commerce, transport, or financial services.

Ensuring information security is a challenge for all entities that form the national cybersecurity system, i.e. business entities providing services using ICT systems, users, public authorities, and specialised entities dealing with ICT security at the operational level.

This study aims to understand the possibility and request for non IT oriented courses in Higher Education institutions in the development of cyber security skills.

Bibliographical Research

There are 2 main documents that formed cybersecurity policy of the Poland.

The National Framework of Cybersecurity Policy of the Republic of Poland for 2017-2022 is a strategic document in a continued process of actions taken by the governmental administration, aimed at raising the level of cybersecurity in the Republic of Poland, including the Policy for the Protection of Cyberspace of the Republic of Poland adopted by the government in 2013. The National Framework document was prepared by a group composed of representatives of the Minister of Digital Affairs, Minister of Defence and Minister of the Interior and Administration and representatives of the Internal Security Agency, the Government Centre for Security and the National Security Bureau.

The National Framework of Cybersecurity Policy identifies, in particular:

- the ICT security objectives;
- the main actors involved in the implementation of the national framework of cybersecurity policy;
- management framework for achieving the objectives of the national framework of cybersecurity policy;
- the need to prevent and respond to incidents and to restore services to normal after an incident, including the principles of cooperation between public and private sectors;
- the approach to risk assessment, • educational, information and training programmes related to cybersecurity;
- activities related to research and development plans in the field of ICT security;
- directions of international cooperation in the area of cybersecurity (National, 2017).

The Cybersecurity Strategy of the Republic of Poland for 2019–2024 is a continuation and extension of actions taken by the government administration to increase the level of cybersecurity in the Republic of Poland.

The Cybersecurity Strategy of the Republic of Poland for 2019–2024 supersedes the National Framework of Cybersecurity of the Republic of Poland for 2017–2022 adopted under

Resolution no. 52/2017 of the Council of Ministers of 27 April 2017 regarding the National Framework of Cybersecurity of the Republic of Poland 2017–2022.

The purpose of this document is to define strategic objectives and relevant political and regulatory measures to achieve a high level of cybersecurity, principally a resilience to cyber threats of information systems used by operators of essential services , critical infrastructure operators, digital service providers and the public administration, as well as to increase information protection in the information systems by means of standardised safeguards. The achievement of the strategic objectives shall also contribute to increasing the national security, improving the effectiveness of law enforcement agencies and judicial authorities in detecting and combating cybercrime, events of a hybrid nature (including events of a terrorist nature) and cyberespionage.

The Cybersecurity Strategy of the Republic of Poland for 2019–2024 is aligned with ongoing operations related to ICT systems used by critical infrastructure operators. It also takes into account the need to enable the Armed Forces of the Republic of Poland - in domestic, alliance and coalition contexts - to conduct military operations in the event of cyber threat which requires defensive operations. By implementing the Cybersecurity Strategy of the Republic of Poland for 2019–2024, the government will fully guarantee the right to privacy and hold the position that free and open Internet is an important element of the functioning of a modern society (The Cybersecurity, 2018).

Main goal of Cybersecurity Strategy id Increasing the level of resilience to cyber threats6 and protection of information in the public, military and private sectors, as well as promoting knowledge and good practices to enable the citizens to better protect information.

The Strategy takes into account, in particular:

- cybersecurity objectives and priorities;
- entities involved in the implementation and deployment of the Strategy;
- measures used to achieve the objectives of the Strategy;
- specification of means for readiness, response and restoration, including principles of public-private cooperation;
- risk assessment approach;
- activities related to educational, information and training programmes regarding cybersecurity;
- activities related to research and development plans regarding cybersecurity.

Furthermore, the Strategy takes into account international cooperation regarding cybersecurity. Introduced by way of a resolution of the Council of Ministers, the Cybersecurity Strategy of the Republic of Poland for 2019–2024 directly affects entities of the government administration and, indirectly, after the adoption of applicable general law on the initiative of the Council of Ministers, other public authorities, businesses and citizens.

State of the Art in the Secondary Education

According to Check Point Research 2021, 2,700 attacks on schools, academic and research centers happen in Poland every week in August 2021. The report's authors said: "The Polish education sector is in the world top in terms of the amount of cyber security incidents" (According to, 2021).

The report of CERT Polska operating within NASK structures shows that in 2020, after the spring lockdown, as many as 94 percent of school websites did not have properly configured security mechanisms that allow protection against spoofing e-mail addresses in their domains. Less than half of the sites (44%) had a properly configured TLS certificate to encrypt the connection. According to CERT, attacks using the vulnerabilities found could lead to the interception of data present on servers, placing undesirable content on websites, and even, if the website was maintained within the school network, breaking into its infrastructure (Podczas, 2021).

Poland's Ministry of National Education issued in August 2017 a document titled Safe School –the threats and recommended preventive measures for [protection of physical and digital safety of students. A program started in September 2017 as a set of safety recommendations and guidelines for school heads and school authorities. In its particular components and general outlook, the document focuses on school safety problems, with propositions for their resolve. The whole document consists of two separate parts. The first chapter –Prevention of physical hazards and ensuring physical safety at school – discusses such material factors as the description of a typical school building, its equipment and its surroundings (areas adjacent to school buildings), entry/exit procedure, alarm system, escape routes, and recommendations for school activities in relation to its material factors. It also underlines duties of the school headmaster, teachers and other school staff, based and in relation to the Teacher's Charter. The second chapter – Cyber threats prevention and digital security at school – is a significant novelty (Bezpieczna, 2017).

According to Iwanowicz study ensuring the digital safety of students – children and adolescents – is as important as ensuring physical and mental security. The threats to student's safety are often mixed – for example, it begins with harassment during lesson brake, and then continues on the Internet. The weight of these problems must be understood by both teachers and school principals, as well as their leading bodies and parents. Only permanent – not incidental – collaboration of all these entities can minimize of moving children in the digital world.

Digital security should be one of the elements of the school's educational and preventive program, for which the entire group of pedagogues is responsible. It should be remembered that even if a person responsible for digital security (school mentor) was selected at school, this does not absolve the responsibility for providing it to other employees of the institution.

The key to ensuring security in school is prevention, including the entire school community – pupils, their parents/guardians and teachers.

In the activities undertaken by the school for the safety of pupils, they must play an important role. Therefore, it is worth engaging students and student self-governments for everyday work, e.g., by entrusting the organization of events to the student self-government and selecting, for example, the "student leaders of digital school security".

The student has contact with the digital world almost all the time outside of school: at home, in its peer environment, on the road or in public places. Ensuring digital security is therefore a challenge for parents on a par with school. The school should actively inspire parents to take control and educational activities and provide them with a minimum level of training support in this field.

In the activities for school safety, it is worth using good practices developed by other institutions – e.g., to ask schools from the region to present their activities, or use the materials developed by non-governmental organizations, public institutions and business entities.

A safe school is a school of competent teachers. This is why teaching staff should constantly update and deepen their knowledge about safety in the school environment, especially in the field of digital competences. This is to be achieved by the recommendation of all teachers to complete the online course (Iwanowicz, 2018).

Panskyi, T. et al. decided to investigate the impact of the pandemic period and the resulting limitations in Polish primary school online security education. The first part of the study investigates the impact of the COVID-19 pandemic on students' educational learning outcomes in information and Internet security. The study has been performed via a student-oriented survey of 20 questions. The statistical analysis confirms the significant difference before and after the pandemic in several questions at most.

Nevertheless, this justifies the statement that pandemics had a positive impact on post-pandemic Internet-related security education. The second part of the study has been focused on students' perception and self-awareness of cyberspace problems. For this purpose, the authors used novel majority-based decision fusion clustering validation methods. The revealed results illustrate the positive tendency toward the students' self-awareness and self-confidence of online security problems and e-threats before, during and after the challenging pandemic period.

Moreover, the presented validation methods show the appealing performance in educational data analysis, and therefore, the authors recommended these methods as a preprocessing step that helps to explore the intrinsic data structures or students' behaviors and as a postprocessing step to predict learning outcomes in different educational environments (Panskyi, 2022).

The majority of Polish society lives in the world of digital content and services, permeating everyday life like no technology in the past. Therefore, Polish schools must fully, substantively and safely operate in the digital environment, using educational resources available online: multimedia content, applications, platforms and associated interactive teaching methods. Fully—that is, not selectively, but consistently across all subjects; substantively—that is, understanding the specifics of online digital resources and tools and their methodological applications, as well as safe—and therefore being aware of e-threats and knowing how to react to them.

Polish schools introduce the annual minimum scope of prevention measures that include: meetings of the entire school community, meetings of the school community with experts, organisation of a school digital safety day, competitions and contests organisation—based on the rivalry between classes—on Internet security, extracurricular activities, educational projects considering new ICTs, etc. The subject of online security, in some schools, has already appeared on the school's website and the school's profiles on social networks as a separate issue.

Teachers participate in different pieces of training, courses and workshops on selected issues of online security and e-threats, using funds at the disposal of the school management to raise the qualifications of teachers or funds from external projects (e.g. EU, curatorial offices, Ministry of National Education). In their daily didactic work, many teachers strive to include

Internet security issues in teaching non-informatics subjects, to a greater extent including them in STEM subjects (Panskyi, 2022).

The subject of online security is insufficiently known by primary school students. Taking into account the revealed results, the authors believe that teaching programs in the field of online security should be revised and complemented by the additional classes devoted to this subject, with particular emphasis on active teaching methods based on case studies, flipped education, problem-based and game-based learning. These modern teaching methods will show students the existing online security problems in an interesting, interactive and creative way.

State of the Art in the Higher Education System

The HE sector plays an important role in providing the building blocks for courses in cyber security. A number of generalist courses that contain a cyber security module are available to students. At the Higher Education level, students can opt for a technical or non-technical route into cyber security. The options are to: undertake either a course in computer science and specialise in cyber security; take a generalist or specialist cyber security course; or opt to combine cyber security with another STEM-subject, the most common ones being Mathematics or Engineering. The majority of students who study cyber security have a background in STEM subjects. This is mainly because employers know extra training and skills development for graduates is required, so they look for Maths and Science graduates to fill the gaps left by those without a cyber security academic background.

Generally at the HE level, there is a number of HE courses and modules that focus on or that can be combined with cyber security at undergraduate and postgraduate levels. Degrees in cyber security-related fields include: generalist computer science courses with a module or specialism in cyber security (e.g. 'Computer Science with Cyber Security'); cyber security generalist or specialist courses (e.g. Cybernetics, Digital Forensics); STEM subjects with a module or specialism in cyber security (e.g. Engineering with Cyber Security); or non-technical courses with a cyber security module or specialism, such as Management, Business Studies or Psychology with Cyber Security.

Polish universities and business schools continue to increase cybersecurity awareness. They offer cybersecurity study programmes. There are more than 55 universities in Poland that propose master of cyber security course (List).

Most of the courses offered are postgraduate studies. They mostly address technical aspects of cybersecurity, but also international standards, law regulations and security tests and management. Many courses were prepared with the cooperation with the security companies and organizations operating on Polish IT market. The university staff members are frequently assisted by practitioners, experts in the cybersecurity domain.

However, many schools and universities do not have the typical cybersecurity courses addressing organizational, procedural, and behavioral cybersecurity issues. They supplement their courses in the area of IT (e.g. management information systems, business informatics, information management) with topics related to information security. Cybersecurity courses are provided mostly for IT students and IT specialists (postgraduate studies). So, we can observe lack of courses addressing knowledge and "soft" skills prepared for business students

that in the future will become managers, owners of companies and organization who will have to deal with many cybersecurity threats.

If about the major types of cyber security threats in education institutions include phishing, malware, ransomware, spam, social engineering and denial of service attacks. Cybercriminals are using these means to target educational institutions for financial gain.

Also in Poland there are many events deal with cybersecurity. Among them Cyber Lab, a project that engages students and graduates from various universities across Poland in disseminating knowledge about digital security and related subjects.

"The idea came into being during the CyberSecurity Challenge PL2020 tournament, organised by The Bridge foundation under the patronage of the Ministry of Digitalisation. Its participants agreed that interdisciplinary education about cybersecurity and the challenges of digital transformation is now essential", says Rafał Sawicki, the ambassador of the project at WUST.

He adds that basic cybersecurity skills should be as commonplace today as smartphone or computer literacy. Students are active in regional teams, where they look at digital security issues from legal, business, medical, military, and of course, IT perspectives (Our, 2021).

The CYBERSEC Forum is the key cybersecurity event in Europe and one of its kind in the world. Since 2015 CYBERSEC has become a space for a worldwide multistakeholder, cross-sectoral, inclusive debate connecting decision-makers, authorities, and experts from different backgrounds, to discuss the most pressing cybersecurity challenges. With this unique event – a combination of high quality debates with an EXPO dedicated to the cyber industry, we underlined that our potential and strength in cyberspace depend on building national capabilities and accelerating them through joint action and mutual support (Cybersec, 2023).

Warsaw Cyber Summit – an international conference focused on cybersecurity from national and international perspectives. The event was held under the patronage of the President of the Republic of Poland. Conference discussed issues around the functioning and development directions of cyberspace, drawing attention to regulatory matters, military operational matters, new wars and private-public partnerships for online security. For the first time, the conference addressed subjects related to aerospace law and challenges as an operational area of businesses (Summary, 2022).

Building societal resilience by raising public awareness of cyber threats and enhancing the role of cyber education is focus of the 2022 Cyber/ICT Security Conference in Łódź, Poland, that was between 20 and 21 October 2022. The conference builds on the Polish Chairmanship's priorities to highlight the importance of strengthening the response to cyber threats.

Set against the backdrop of a cyberspace increasingly threatened by state actors, criminal groups and individuals, the purpose of the conference will be to identify how to build national and regional resilience at all levels, helping insulate the OSCE, its participating States and their respective citizens from future cyber security risks (Łódź, 2022).

Cyber Awareness of the Target Group

There are few investigations that examine cybersecurity awareness in Poland.

Wiechetek et al. evaluate cybersecurity awareness of Generation Z members on the example of Polish business students. Young people, members of Generation Z born after 2000,

use information technology as a main tool for broadening knowledge and skills. They were born in the Internet era, know and like to use ICTs, however not all of them may have an appropriate knowledge and skills in cybersecurity, and, therefore, can be a weak point in cyber ecosystem, so there is a strong need to constantly explore, monitor and improve their digital competences (Wiechetek, 2022).

To get the answers to the research questions, the authors collected data from young people, members of Generation Z – business students. The online survey was completed by 182 students. They were mostly students of Logistics (58%), Economics (19%) and Business analytics (14%).

None of the students reported very good knowledge in the field of cybersecurity. Most of the respondents indicated poor knowledge or no knowledge in this area (respectively 55% and 14%), only 31% reported good knowledge. Analyzing the gender, more familiar with cybersecurity issues were male respondents – about 44% with good knowledge while only 20% of female students indicated good knowledge in this area. This shows that cyber skills of business students must be supplemented and improved. Not only because of fast development of IT solutions, but also because of shortcomings in the basics of cybersecurity in a group of business students.

The higher level of cybersecurity knowledge was declared by second-year Bachelor and second-year Master students. However, thirdyear Bachelor students reported mostly poor and no knowledge in this area. All the PhD students also reported good knowledge of cybersecurity. Analyzing the above results, we can assume that lack of progress in this area may be caused by lack or not enough emphasis on the cybersecurity issue in the courses enclosed in the study programme or poor quality of education in this area. However, to confirm this assumption, more research exploring IT-related study programmes that provide cybersecurity trainings like computer network administration, application development or database design, is needed. The respondents were asked to indicate three terms that they associate with cybersecurity.

Among 516 terms indicated by the respondents the top five were “password” (8.9%), “antivirus” (8.3%), “security” (5.4%), “safety” (2.7%) and “firewall” (2.3%). We conclude that the students are aware of basic mechanisms like strong passwords or dedicated software that can increase the security level. The terms that appeared less frequently in surveys (less than 1%) were: “industrial safety”, “ad blocker”, “social media”, and “account”. It may indicate that young business students notice both the problems of single Internet users like identity theft, but also indicate the threats for business, industry, and intelligent networks. The respondents also indicated three devices that are prone to cyberattacks. The most common devices that in respondents’ opinion are prone to cyberattacks are computers, smartphones, tablets, and laptops. However, some respondents also indicated wearables, TV, ATMs, and routers. That type of hardware was reported quite rarely, less than 0.5%. The results show that members of Generation Z clearly notice the need of securing personal devices computers, smartphones, and tablets, however, more education is needed to transform awareness into action and deliver broad knowledge and skills on how to build secure ecosystem consisted of many common devices, computers, smartphones but also other devices that are frequently used and can be hacked too (wearables, TVs, Bluetooth hardware and network hardware).

To show preferred sources of cybersecurity knowledge, the respondents could choose more than one option from the following list: websites, social media, talking with friends, university classes, radio, television (traditional media), IT journals, industry reports, scientific journals and

being a victim of cyberattack. The most indicated sources were web pages (80%), social media (65%), talking with friends (45%) and university classes (41%). The less popular sources, chosen by less than 10% of the respondents were: scientific journals, industry/business reports, and being a victim of cyberattacks.

The main threats indicated by the respondents were loss of money, violation of privacy, loss of data and the possibility to use IT for terrorist attack. The less important were influencing social choices, blocking access to information and business processes, and, finally, unauthorized takeover of devices. The average score for these items was less than or equal 3.5. We can observe also higher importance of all the threats (except for attacks on IT infrastructure) by male students. The biggest differences were observed in spying people and organizations, losing money and data (more than 7%).

Analyzing the year of the study, authors can notice the stronger impact of cyber threats reported by Master programme students (average for the group of respondents equals 3.9). For Bachelor students, the average was between 3.4 and 3.7. We cannot observe the influence of the year of study and the perception of the main cyber threats. Such weak relation can be explained by the lack of expected cybersecurity classes in the study programmes. If the student got appropriate knowledge and skills during the classes the correlation between the perception of main cyber threats and the study year could be positive or negative, but clear. If the students had more knowledge of cybersecurity threats, and the prevention of how to avoid them was weak, the respondents would rather indicate their greater impact. On the other hand, when the students were provided with necessary knowledge, but also skills and attitudes that will allow them to secure the cyber activities, they would probably report lower impact of cybersecurity threats.

Among the most frequently used methods and tools for improving the cybersecurity, the following were recognized: strong password (83%), using antivirus software (76%), and not installing the applications from the unknown source (55%). The mechanisms used by female and male students and the frequency of its usage was quite similar except for software updating – only 32% of female respondents used this method, while 60% of male students performed software updates (Wiechetek, 2022).

Analyzing the types of studies, investigators notice that IT students more often performed security audits, took part in security courses, and used software update. Business analytics students more frequently changed their passwords and used anti-spam software. According to the year of study, PhD students used the most security tools, while the third-year bachelor students reported that they used security mechanisms less frequently.

Since the analysis indicated that the most popular are simple methods, based on password and antivirus software, the cybersecurity courses should widen the catalog of security mechanisms, e.g. using passwords managers, avoiding public networks and computers, regular backup and performing the security audits. As technology development is accompanied by little commitment to cybersecurity courses, the study programmes should enable and encourage students to continuous improvement of cyber competences. Finally, the respondents were asked about their behavior in case of cyberattack and what people or organizations would they inform in that case.

Authors can observe that the respondents were polarized. 42% reported that they rather know how to behave and 29% stated that they probably would not know what to do in case of the attack. There were not big differences in terms of the gender, but female respondents

were more determined (only 13% no opinion answers), however, they more frequently reported lack of knowledge about how to behave. Also, Information technology students were more sure how to behave (67%), while the majority of Management students did not know how to act in case of a cyberattack (57% of students answered rather no and definitely no). Analysis of study year also did not indicate a clear relation between knowledge and the study year and level. There can be stated that also in this case we can observe the deficiencies in the curricula. In study programmes addressing IT security issues we should have more students who know how to behave in the later years of study, especially Master and PhD students should know exactly know how to behave. So it could be noticed the gap in study programmes for business students. To fill in this gap, the syllabuses should be supplemented with the methods and tools increasing the cyber security level, but also procedures and recommendations how to act or communicate in case of a cyberattack.

Most students (56%) indicated that they have not attended cyber security classes or trainings. Only slightly over 20% have taken part in those trainings. The students are also willing to attend cybersecurity classes – almost 50% would rather or attend such trainings. Only 19% were rather not interested in taking part in such trainings. Thus, most of business students have no educational experiences in cybersecurity, also they are willing to take part in the courses. In addition, the students stated that their current education has only slightly affected their cyber security awareness (Wiechetek, 2022).

Szumski in the reseach argue that universities is not playing the major role in rising of cybersecurity awareness. People tend to search on their own information related to cybersecurity area on the Internet or asking other users.

The findings of this study show that qualified sources of knowledge about cybersecurity such as University and Professional courses are not as popular as should be. It can be noticed that such training is almost marginal for respondents in comparison to internet and friends. Collected results give the impression that university doesn't meet the major responsibility to be the major source of knowledge about cybersecurity. Author might speculate that the reason behind such situation lays behind content or not effective teaching methods of provided courses.

The most common source of information about cybersecurity comes from the Internet and Friends and Colleagues. It is common trend observed from many aspects although author is suspicious about the quality of such source of data also considering the amount of information that has to be processed by ordinary person to get the reliable set of information. The proof of such situation can be shown by the most common method within students in password management approach. Most of students use only human memory to store the passwords and concluding that it means that either passwords are simple and easy to remember or are used the same or very similar passwords within different applications and portals. In the opposition to the memory there were also people that break any security approaches putting down passwords in the most accessible way – sticking the post it note with a password to the computer. What is scary 6 people out of those who stick the password to the computer said that they apply cybersecurity in their everyday life and all of those people indicated Internet as major source of information about cybersecurity.

Received results indicate that either employer or university was not interested in promoting good behavior patterns nor the training was the target for respondents. And it can be a reason that users of modern technology put more trust in Internet than in qualified sources of

knowledge. Also questionable is the content of such training that people concluded as not beneficial from the perspective of cybersecurity awareness. It gives a great space for improvement within educational institutions. Author might speculate that such training didn't fit for purpose or people were not interested in such training. Although Internet and friends and colleagues treated as experts in the area of cybersecurity is the leading source of information it is noticed that respondents also indicate the need for reliable knowledge transfer about cybersecurity.

11.8% of non–working students declared to participate in training offered at school or university its even less than within the working students group (15.1%) Author raises the question what is the reason of not benefiting from university courses in this important and risky area of life. Would that be the course itself not meeting expectations, would that be the teaching staff with not relevant knowledge answer to this questions would allow to recreate new approach to courses provided by universities.

Over 63% of all respondents declared to use approach called by them "best practices". Such results indicate moderate level of cybersecurity awareness, although considering the number of possible results given by google it also can give the impression that the statement "best practices" is not fully clear to the respondents and is subjectively emphasized as best practices or other suggested behavior that assure protection over the internet.

Even though users don't feel the risk that their passwords are too weak they still have concerns about the security issues but those might have been of other characteristics than password protection. The presented study has preliminary character and was concerned on distinguished population of University Students (Szumski, 2018).

Conclusion & Recommendations

Cybersecurity issue becomes a very important not only because of the increasing number of Internet interactions, developing new technologies that generate new possibilities and threats, but also because of the COVID-19 pandemic situation that forced people to move their entertainment, educational and professional activities online, and made the future more digital/virtual than ever.

Cybersecurity is not a state but a continuous process. Literature shows that cybersecurity courses should be prepared not only for IT specialists, but also managers, office workers or just casual users of information systems. Course attendants should be both young children, should be the concern to all members of the society. Trainings should be interesting, i.e. prepared in different forms, with various delivery methods. To improve the actual situation of cybersecurity awareness in student community, an access to open sources of knowledge should be increased by, e.g. preparing massive open internet courses (MOOCS) that will constantly provide proven and useful information regarding cybersecurity.

Such widely available courses, confirmed by university prestige, could create safe places and platforms that would offer reliable and comprehensive information, understandable not only for advanced IT users. At the same time, due to the increasing use of IT technology specialized cybersecurity-related courses should appear in major university curricula – such courses could provide selected information on cybersecurity, which are especially important from the point

of view of a given field of study teenagers, students, employers, but also older people because cyberattacks

As schools incorporate technology into the classroom, the education system itself is required to train teachers in how to help students identify cyber risks and stay safe from threats. In the increasingly digital world, rather than simply a standalone class, cyber risk education should be incorporated in a multitude of courses so its lessons can be reinforced across different subjects

The most important for ensuring the foundations of digital security at school are preventive measures carried out against and with the participation of all entities of the school community: students and their parents, principals, teachers and other school employees (e.g. psychologists, educators, secretarial staff). These measures should be systemic, continuous, long-term and coordinated, and their scope should be included in the educational and preventive program implemented at the school.

The cybersecurity education requires innovative approaches for building the skills for sustainability development by introducing cyber ranges and serious games that have proven to be more effective in developing the required cyber-related skills. These approaches enable the required interactivity in the training process that leads the learner to take decisions in a safe environment which is similar to real life; this accelerates the learning process. However, the designing and the selection of appropriate serious games is a long and demanding process.

Possible structure for focus group study:

1. Level of cybersecurity knowledge.
2. Organisation of individual cybersecurity.
3. Source of information about cybersecurity.

References

1. According to a recent Check Point report, cyber attacks on educational and research institutions in the United States, Europe and Asia are growing at double-digit rates. Polish schools are more than twice as vulnerable to attacks as other industries. URL: https://ictmarketexperts.com/en/news/the-growth-of-cyber-attacks-on-polish-schools/

2. Bezpieczna szkoła. Zagrożenia i zalecane działania profilaktyczne w zakresie bezpieczeństwa fizycznego i cyfrowego uczniów (English: Safe School.The Threats and Recommended Measures for Physical and Digital Safety of Students), Ministry of National Education, Warszawa, August 2017. Cybersec. URL: https://cybersecforum.eu/

3. CYBERSECURITY STRATEGY OF THE REPUBLIC OF POLAND for 2019-2024 URL: https://www.gov.pl/attachment/6a4aafc6-e339-4cd5-a8e6-cd47257f02d8

4. Iwanowicz I. The Praxeology of Safety According to the Polish Ministry of National Education Program “Safe School” Studia Administracji i Bezpieczeństwa, 2018, 5 URL: file:///C:/Users/User/Downloads/Iwanowicz.pdf

5. List Of Top 55 Universities In POLAND Offering Master Of Cyber Security Course. URL: https://gyanberry.com/list-of-top-universities-in-poland-offering-master-of-cyber-security-course/

6. Łódź Cybersecurity conference: strengthening the societal response to cyber threats. 2022. URL: https://www.osce.org/chairmanship/528750

7. National Framework of Cybersecurity Policy of the Republic of Poland for 2017-2022 Ministry of Digital Affairs Warsaw 2017. URL: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Cybersecuritystrategy_PL.pdf

8. Our students operate in Cyber Labs to educate the public about cybersecurity . 2021. URL: https://pwr.edu.pl/en/university/news/our-students-operate-in-cyber-labs-to-educate-the-public-about-cybersecurity-10489.html

9. Panskyi, T., Korzeniewska, E. Statistical and clustering validation analysis of primary students' learning outcomes and self-awareness of information and technical online security problems at a post-pandemic time. Educ Inf Technol (2022). URL: https://doi.org/10.1007/s10639-022-11436-3

10. Podczas pandemii wzrosła liczba cyberataków wymierzonych w edukację. Większość szkół i uczelni nie posiada właściwego poziomu ochrony. 2021. URL: https://innowacje.newseria.pl/news/podczas-pandemii-wzrosla,p329155329

11. Summary of Warsaw Cyber Summit URL: https://www.wojsko-polskie.pl/aszwoj/en/articles/news/summary-warsaw-cyber-summit-2022/

12. Wiechetek, Ł., & Mędrek, M. Human Factors in Security – Cybersecurity Education and Awareness of Business Students. Annales Universitatis Mariae Curie-Skłodowska, sectio H – Oeconomia, 2022, Vol. 56, No. 1.

13. Szumski O. Cybersecurity best practices among Polish students. Procedia Computer Science 126 (2018) 1271–1280.

ANALYTICAL REPORT ON THE NATIONAL DESKTOP ANALYSIS IN SWITZERLAND

Introduction

The desktop analysis (R1A1) is carried out in order to shed light on the focus group study (R1A2) and to prepare an infrastructure for it. As a result of the A1, it is aimed to have an idea about the target group, to create the questions that should be used in the focus group study and to ensure the integrity of the subject by combining the current literature directly or indirectly related to the subject of the project in the partner countries.

After an informative and guiding introduction part, the report should include national bibliographic reviews in five different countries. After a general introduction to the subject, the report should include national bibliographic reviews in five different countries. Subsequently, the conclusion section will be formed by presenting the current local situations, developing suggestions on the issues that are considered important but with lack of studies on a national basis.

Bibliographical Research

Switzerland is a federation comprising 26 federated states (cantons) as well as a centralized government. This leads to a multi-layered legal system and, in some cases, a decentralized regulatory approach to cybersecurity. On a federal level, the Swiss Constitution of 18 April 1999 protects the right to privacy, in particular the right to be protected against misuse of personal data (Article 13). The collection and use of personal data by private bodies are regulated on a federal level and are mainly governed by the Federal Data Protection Act of 19 June 1992 (the FDPA) and its ordinances, including the Ordinance to the Federal Act on Data Protection (the FDPO).
The FDPA was revised to implement the revised Council of Europe's Convention 108 and to align with the EU General Data Protection Regulation (GDPR) more closely. After a protracted revision and parliamentary consultation process, Parliament adopted the final text of the revised FDPA on 25 September 2020. There has been no referendum against the revised FDPA, which is scheduled to enter into force on 1 September 2023. Importantly, the revised FDPA will not only bring about more impactful enforcement powers but will also impose on controllers and on processors, on certain conditions, a duty to notify data security breaches. Additional compliance and documentary measures, such as data protection impact assessments and inventories of data processing activities will also be introduced.

There is no overarching cybersecurity legislation in Switzerland to date. However, on 1 July 2020, the Ordinance on the Protection against Cyber Risks in the Federal Administration (CyRV) entered into force. The purpose of the CyRV is firstly organizational as it allocates roles and responsibilities within the federal government and looks to reinforce the government's capabilities and response to cyber threats. Of note is the set-up, under the CyRV, of a centralized competence center for cybersecurity named National Cyber Security Centre (or

NCSC). In addition, on 18 December 2020, with the aim of implementing proper information security practices within the administration, Parliament approved a draft Information Security Act.

Apart from the CyRV, cybersecurity remains mostly regulated by a patchwork of various acts and regulatory guidance, which deal explicitly or implicitly with cybersecurity in the private sector. These laws include:

- the Budapest Convention on Cybercrime (CCC), which entered into force in Switzerland on 1 January 2012, imposes a harmonization of Switzerland's criminal legislation as well as speedy international cooperation mechanisms.
- the Federal Data Protection Act.
- the Federal Telecommunications Act of 30 April 1997 (FTA).
- the Federal Act on Financial Market Infrastructures and Market Conduct in Securities and Derivatives Trading of 19 June 2015 (FinfrAct).
- The banking and financial markets legislation also leads to the financial markets regulator's (FINMA) issuance of various circulars and regulatory notices.

However, the Swiss government has given cybersecurity increasing attention in the past few years and the absence of an overarching ad hoc law on cybersecurity may appear misleading, given the importance and national relevance of this topic. Nonetheless, this conclusion is unlikely to lead the Swiss legislator (Parliament) to issue any topical legislation on cybersecurity soon. On the contrary, the federal government has been following a national strategy against cyber risks (NCS) for the years 2018–2022. The National Cyber Security Centre (NCSC) is the competence center for cyber security and thus the first contact point for businesses, administration, educational institutions, and the population for all questions relating to cyber security. NCSC is responsible for the coordinated implementation of the National Strategy for the Protection of Switzerland against Cyber Risks (SNPC). In recent years, cyber security has gained importance at all levels. It plays a central role in national and international security policy and is becoming an increasingly important factor for the Swiss economy and population. With the creation of the NCSC under the leadership of the Federal Delegate for Cyber Security, the Federal Council aim to support the population, the private sector, educational institutions, and the administration in protecting against cyber risks and improving the security of its own systems.

At its meeting on 30 January 2019, the Federal Council determined the competencies and tasks around cyber risks and established a cyber security committee in which the heads of the FDF, the Federal Department of Defense, Civil Protection and Sport (DDPS), and the Federal Department of Justice and Police (FDJP) sit.

The Ordinance on the Protection against Cyber Risks in the Federal Administration (OCiber), approved by the Federal Council, has been in force since 1 July 2020 and forms the legal basis for the establishment and expansion of the NCSC. It regulates the structure, tasks, and competencies of the authorities involved.

On 12 January 2022, the Federal Council initiated the consultation procedure concerning the introduction of an obligation for operators of critical infrastructure to report cyber-attacks. The draft lays the necessary legal foundation for the notification obligation and defines the tasks of the National Cybersecurity Centre (NCSC), which will act as a central service for the notification of cyber-attacks.
The NCS is organized around reaching 247 milestones. The 2021 report on the progress of the NCS, published in August 2021, confirms that this strategy remains largely on track in terms of reaching its various milestones. The NCS aims to strengthen cybersecurity in Switzerland and combat cybercrime. It does not foresee the implementation of dedicated cybersecurity legislation, rather focusing on modernizing various pre-existing laws. The NCS is a testimonial to the growing relevance of cybersecurity in Switzerland, as well as perhaps the increased global threat posed by cyber risks.

A further manifestation of the government's interest in cybersecurity is another governmental venture, the Digital Switzerland strategy.

Switzerland, like most EU countries, lags when it comes to cyber security education in secondary schools. Secondary education is harmonized across the German-speaking cantons by means of the project Lehrplan 21, with similar projects existing for the other language regions. A module dedicated to media and computers is part of Lehrplan 21. Its contents include secure data processing, ethical use of (online) media, risks in media and cyberspace, cyber mobbing, etc. Equivalent programs exist for the French-speaking cantons and the Italian-speaking canton of Ticino. The Swiss system of education has a strong focus on apprenticeships. The apprenticeships are concluded with a federally acknowledged certification for their respective profession. People working for businesses are generally expected to hold at least an apprenticeship specific to their job; also, SMEs offer such apprenticeships in collaboration with industrial education bodies. Several apprenticeships are available for ICT specialists. The apprenticeship Informatiker/in EFZ Systemtechnik also emphasizes the aspects of security and information protection. A certification called Cyber Security Specialist EFA offers training specific to the security and defense of an organization's ICT systems. Thereafter, continued specialization is possible by means of the diploma ICT Security Expert ED.
Employees are enabled to holistically assess the security-relevant exposure of an organization and to define and assess security measures. Continued assessment, analysis, and development of processes in an organization is a priority for specialists with this diploma. Hence, they incorporate a bridging role between IT specialists and an organization's management.

Swiss expertise is defined by excellence in engineering, cryptography, and algorithms. Many academic institutions in the Greater Geneva area train experts in the field of cybersecurity.
The EPFL offers a master's degree that trains engineers in cybersecurity. The Haute École d'ingénierie et d'architecture de Fribourg, the Université de Fribourg and the Haute Ecole d'Ingénierie et de Gestion du Canton de Vaud offer programs in the cybersecurity field. The Université de Lausanne hosts the Swiss Cybersecurity Advisory and Research Group, which focuses on scientific research and academic teaching of IT security. The Haute École

spécialisée bernoise is also active in this field with its Institute for Cybersecurity and Engineering ICE. Finally, the Institut de recherche Idiap has made a name for itself internationally with its Swiss Centre for Biometrics Research and Testing. Idiap was chosen as the only European partner of Google's exclusive Abacus research project. IARPA, the US Department of Intelligence, has also collaborated with Idiap on spoofing attacks.
This wealth of talent is what led technology giants such as Hewlett-Packard Enterprise, Logitech, Cisco, and Kudelski Security to choose western Switzerland as the hub for their research and development activities.
In the same context, many start-ups have developed. For instance, Neuchâtel-based Nym Technologies has created an open-source, decentralized infrastructure that offers full-stack privacy by exploiting blockchain technology. Lausanne-based Saporo uses graph theory to help companies model, measure, and increase their resilience to cyber-attacks. Also present is Biel-based company Threatray, which has developed a malware intelligence platform that facilitates defense and effective response to cyber-attacks.
Western Switzerland's innovation infrastructure supports the development of cybersecurity companies at an early stage. Incubators such as Y-Parc, Fongit, MassChallenge, and FriUp offer incubation and acceleration programs to foster the growth of cybersecurity startups. Geneva-based accelerator Rising Star identifies and selects cutting-edge cybersecurity start-ups at pre-seed and seed stages.

Today, Western Switzerland shows a sophisticated local market with quality companies such as ID Quantique and ProtonMail. Every year, new companies move to the region, attracted by its deep talent pool and excellent business conditions. The numerous public authorities, academic institutions, and business players in Western Switzerland help to position the region as an agile, innovative, and efficient force for digital transformation.

Several university degrees specific to cybersecurity and list some examples, as follows:

- the Lucerne University of Applied Sciences and Arts offers undergraduate and postgraduate/advanced training degrees in Cyber Defense, Cybersecurity, and Digital Forensics.
- The Federal Institute of Technology in Zurich (ETH Zurich) offers a master's degree in computer science112 with a specialization in cybersecurity and advanced training degrees in cybersecurity.
- The Ecole Polytechnique Fédérale de Lausanne (EPFL) offers a cybersecurity master's degree114 and Bern University of Applied Sciences offers advanced training degrees in digital forensics and cyber investigation.
- The University of Lausanne offers degrees related to prosecution and legal aspects of cybersecurity, as follows:
    - the School of Criminal Science (École des sciences criminelles) offers a master's degree in Digital Investigation (MSc investigation numérique).
    - Faculty of Law offers a law master's degree (MLaw) on criminality and security of information technology (Droit, criminalité et sécurité des technologies de l'information) in collaboration with the Faculty of Economics.

- The University of Applied Sciences and Arts of Western Switzerland (HES-SO) offers a Certificate of Advanced Studies (CAS) in Forensic Investigation, which is attended by most police IT specialists of the French-speaking cantons.
- HES-SO also offers a Master of Advanced Studies (MAS) in Combat against Economic Crime, which is a multi-disciplinary training course for people wishing to work in the field of economic crime prevention, investigation, and repression. It includes cyber-related disciplines and has existed for 20 years.

Furthermore, any disciplines relevant to cybersecurity (e.g. law, ethics, economics, social sciences) should include modules on cybersecurity in their degree programs. Discussions with stakeholders have shown that cybersecurity-related fields are also offered at university level. We have further found evidence of cybersecurity courses that are aimed at a non-specialist audience.
For example, the Lucerne University of Applied Sciences and Arts offers a variety of courses aimed at different audiences, for example:

- tailored education for specific businesses, courses for children and youth, and courses for professionals who are concerned by the emergence of cyberspace.

Computer science bachelor's degrees do not generally include modules on (non-technical) cybersecurity and rarely involve mandatory modules that focus specifically on IT security.

It is widely recognized that one of the best preventive measures against cyber-attacks is information and awareness of the different attack types and strategies. This is one of the main reasons why the topic of cyber security has become increasingly prominent in the Swiss media, especially by raising awareness of the latest scams and frauds. Even while implementing these strategies to limit possible scams, society needs more professionals in the field. In this context, a major concern of the confederation is the shortage of experienced professionals and students who can protect and maintain the security of digital infrastructures.

Conclusion & Recommendations

The cybersecurity landscape in Switzerland is characterized by a discrete industrial sector with companies active in intelligence and system management services.

At a governmental level, the Swiss Confederation centralizes some offices and contact centers and invests in the collection of incident announcements, the definition of the threat landscape, and trend that emerges from the cases announced spontaneously by citizens, private businesses, and institutions to the central emergency response and awareness offices.

At the Canton level, a certain autonomy is left to the single region which can better adapt laws and messages to the reality of the threat landscape, which in the Country also shows a certain relationship to the linguistic culture (attacks to Swiss German academies sometimes differ from the ones perpetrated in other regions).