Web-Service Security and The Digital Skills of Users: An Exploratory Study of Countries in Europe

Borka Jerman Blazic[1*], Primož Cigoj[2] and Andrej Jerman Blažič[3]

[1*]Institut Jožef Stefan, Laboratory for Open Systems and Networks Ljubljana, University of Ljubljana, Department of Economics, Ljubljana, Slovenia. jerman-blazic@ijs.s, Orcid: https://orcid.org/0000-0001-9002-4548

[2]International Postgraduate School Jožef Stefan, Ljubljana, Slovenia. cigoj@e5.ijs.si, Orcid: https://orcid.org/0000-0002-5161-7380

[3]Institut Jožef Stefan, Laboratory for Open Systems and Networks Ljubljana, Slovenia. andrejcek@e5.ijs.si, Orcid: https://orcid.org/0009-0002-8629-9770

Received: June 02, 2023; Accepted: August 10, 2023; Published: August 30, 2023

Abstract

This study explores the impact of internet users' and web owners' knowledge, measured by the level of digital skills, on the number of insecure websites based on a survey of the internet. The influence of the affordability of internet access to the web space on the vulnerability of a particular European country is also considered. The study introduces a quantifiable index for assessing the insecurity of websites that is incorporated into a newly developed tool that scans websites and identifies the vulnerability in the Web Content Management System (WCMS). The collected vulnerability data and the digital skills are analyzed with statistical methods for finding the interdependences and relationships. Higher levels of digital skills and lower fixed-internet-access costs contribute to a smaller number of insecure websites. The vulnerability of the websites for different economic sectors is explored as well. The paper discusses the differences in the digital development pathways and governmental policies applied in European countries that have been affected by user knowledge and digital skills. The study brings original results and findings, as there are no similar studies addressing the impact of the knowledge of a country's population on the level of insecurity found in the WCMS, including plug-ins.

Keywords: Web Content Management Systems, Vulnerability, Insecurity, Digital Skills.

1 Introduction and Background

The development of innovative digital services and the growth of a secure digital market have been two of the main priorities in the policies of the European Union (EU) for many years. In this context, the EU provides comprehensive financial support to member states for topics related to security initiatives through funding programs that focus on cyber-security awareness and applications. The purpose of these policies is to achieve an economic alignment with cybersecurity-protection provisions in the heterogeneous digital markets of the EU member states. The advance of the EU member states towards a secure digital economy and society is an interesting subject for studies, as the EU member states still

Journal of Internet Services and Information Security (JISIS), volume: 13, number: 3 (August), pp. 41-57.
DOI: *10.58346/JISIS.2023.I3.004*

*Corresponding author: Institut Jožef Stefan, Laboratory for Open Systems and Networks Ljubljana, University of Ljubljana, Department of Economics, Ljubljana, Slovenia.

demonstrate great variety in the pace of economic development and the degree of digitalization of their markets and societies, where in many cases the security aspects are not given sufficient consideration (Labędowicz & Urbanek, 2017).

Digital services are offered through web applications and represent the interface between the service provider and the consumer. The web service itself is usually supported by a complex software infrastructure that typically includes an application server, a web content management system (WCMS), and a set of external systems such as databases, payment gateways and other applications dedicated to the consumers of the service. The multi-layered architectures of web-based systems and their sophisticated interactions with different types of subsystems on the web increases the number of weaknesses that can be exploited by attackers with malicious intentions (McGuire & Dowling, 2013). The number of vulnerabilities that expose a website to malware and identity theft is growing, with successful web attacks leading to substantial economic and other types of damage, such as the credibility of the website and the service, including financial losses. According to Symantec (Symantec 2019), undiscovered web vulnerabilities are the reason why the world witnessed a 56% global increase in the number of successful web attacks in 2021, with 23% of them having serious consequences. Sfakianakis et al., (2020) reported that 351,913,075 unique websites with flaws were detected in the second quarter of 2020 alone. Due to the continuously increasing number of web vulnerabilities, as well the growing number of successful attacks, website security was ranked as the number-one issue among the identified serious cybersecurity problems for the whole of the internet (Sfakianakis et al., 2018).

In addition to the economic impact, the damage caused by successful cyberattacks provokes social consequences, as the attacks affect many different web-service categories, such as health services, scholar and financial services, personal property (including hardware or software), service performance, theft from bank accounts or unauthorized access to devices and private information (Clough, 2012). Moreover, the indirect impacts of cyberattacks affect the social and business worlds, which includes a loss of trust in e-commerce (consequently reducing e-purchases and the acceptance of e-services), a loss of trust in websites, which contributes to an increased difficulty in communicating with banks, and increases the threat to a country's infrastructure (Anderson et al., 2013; McGuire & Dowling, 2013).

Good knowledge of existing website vulnerabilities accompanied by a higher level of awareness about security threats among a country's population are expected to impact on the use of protective measures either by the website owner, the web maintainer or sometimes also by the website user, especially in cases when it is supported by governmental policies in education. Having the appropriate skills and understanding or possessing knowledge about threats, on the one hand, and the existence of vulnerabilities within the systems, on the other, could contribute to a greater engagement and ensuring behavior in line with cybersecurity recommendations. This might reduce the odds of negative outcomes, such as the theft of data, money or personal information (Park, 2013).

The level of digital skills among the population of the EU member states was recognized as having a crucial role in the progress of European digital society; its value was specified as an indicator that measures the achieved success of digital development. The "European 2020 Strategy Act" adopted in 2016, by the European Commission (EU, 2016) introduced a digital-performance measurement system known as the Digital Skill (DS) index for tracking the evolution of the EU member states in terms of digital competitiveness (Joshi et al. 2021; Nedelcheva, 2021). Two years later, a more complex index known as the DESI (Digital Economy and Society Index) was introduced by the European Commission to monitor Europe's overall digital performance. It included elements that are present in the old DS index, but the new DESI is enriched with several economic parameters such as the level of employment in the country. Eurostat (2020) measures the indicator levels each year by carrying out regular surveys

among the EU member states. The DS index consists of several items that evaluate the skills of a country's population, for example, copying or moving files or folders, saving information from the internet, obtaining information from public authorities or service websites, finding information about goods or services, and searching for health-related information. Information about the communication skills of individuals is also included in the DS index, for example, sending or receiving emails, participating in social networks, making and receiving phone calls or video calls over the internet and uploading self-created content to any website on the net. Problem-solving skills include those that are required for transferring files between computers or other devices, installing software or applications, or changing the settings of software, including the operating system or security programs used for protection. The included software skills enable the use of word-processing software, spreadsheets or editing software for photographs, videos, and audio files, as well as a familiarity with online services that covers online buying or selling in a secure way, the use of online learning resources and internet banking. Additional skills that contribute to the DS index include the user`s safety awareness in creating presentations or documents, integrating text, pictures, tables or charts, or the use of advanced functions in spreadsheets to analyze data (use of formulas, charts, etc.) and writing code in a programming language are also included in the DS index (Eurostat 2020). The performance of these tasks includes some awareness of cybersecurity, especially during the interaction with web services when shopping, paying, using bank services, communicating with health systems, etc.

The digital development of a country's society is frequently assessed using information-communication technology (ICT) data such as the frequency of internet use and the country's underlying infrastructure for internet access. Depending on the time when these indicators were designed and used (ITU, 2020)], most of them have recently become obsolete as the technologies that were used for their definition and measurement reached some level of widespread presence, like the use of TV, fixed or mobile telephone lines, the use of personal computers, etc. For this reason, the most relevant and widely considered indicators for assessing the status of digital development today are those that reflect digital skills, the economic aspects of the digital economy including cybersecurity and the development of the ICT infrastructure (Kavitha R., et.al (2018). These indexes are measured by the International Telecommunication Unit, a UN agency, and the most used are as follows: the frequency of internet use by the population [FoIU], the number of households connected to the internet [HH], and the cost of fixed access to the internet [Fixed] which is expected to reflect accessibility to the internet infrastructure.

The scientific literature addressing the digital-knowledge inequality among different regions is mainly focused on the identification of socio-economic and institutional factors that explain the different levels of digital development in a country or at the regional level (Monedero et al., 2012; Greco et al. 2019; Micheli et al., 2018, Noussan & Tagliapietra, 2020; Büchi et al., 2018). The differences between the digital-skill levels as a factor that influences other more technical areas like cyber security have been studied much less, although a number of authors have found that in some cases the geographical proximity of the neighboring countries may have an influence on the scale of digital development and, consequently, on the digital skills (Salemink et al., 2017). Recent studies of digital knowledge among a country's population were focused on the gains that come from the use of the internet and look into the gaps in the capacity of individual users to translate the use of the internet into favorable offline outcomes (van Deursen & Helsper, 2018), in economic, social, political and cultural terms (Lutz 2019). Dodel and Mesch (2018) tried to connect digital skills and the adoption of safety behaviors, but their study was focused mainly on antivirus behavior, based on a sample of 1850 interviews. When considering these findings, it becomes apparent that the impact of digital knowledge on the technological properties of the internet, such as web security, have not yet been sufficiently studied and analyzed. (Thorncharoensri, P., 2019)

This study presents attempts to find an answer to the question of whether and how the differences in the knowledge in a country's population measured through the values of the DS index and the affordability of the communication infrastructure impact on the increased insecurity of internet-connected websites. The presented research looks to identify the dependencies between the population's skills and the detected vulnerability in the connected websites by analyzing millions of pieces of data collected from European internet web spaces, by inspecting web vulnerability, the severity of the detected flaws in the visited web sites, and the inequality in the digital skills among the populations of European countries. Although the search of web vulnerability was spread over all internet websites, due to the absence of reliable digital skills data about country populations from trustable sources like Eurostat outside Europe, this prevented the study from including other countries.

The paper has several sections. After a presentation of the background, a section describing the design of the research comes next. Then, a section presenting the methodology used for collecting the data is presented with an analysis of the data collected and a presentation of the results. An evaluation of the findings compared with previous studies is presented in the discussion section. The paper concludes with a reflection on the presented study and the obtained results.

2 Design of the Study

The vulnerabilities of a web system can be identified using either a static or a dynamic inspection. A static inspection is performed on the source code before the service goes live. A dynamic vulnerability inspection is performed on an active internet web space with web scanners that automate the process of examining the web security (Alshreef, 2017). Most of the known studies about web vulnerability involve tools developed and used to discover web vulnerabilities, but they tend to focus on the web server itself and usually they have limited capabilities. The most-often used tools in the reported studies of web vulnerability are Zmap (Durumeric et al., 2013) and Masscan (Graham, 2020). These tools are capable of scanning for web vulnerabilities, but only at the level of server plug-ins; the other applications are not affected by the scan. Reports of these scans can be found in a public database on the internet (Schagen et al., 2018; Nappa et al. 2014; Kim et al. 2018). Other web-vulnerability studies are focused on analyzing a selected website set taken from a public database that lists the identified vulnerable websites (Alexa, 2020), but the information is usually restricted to several thousand websites, as the analyzed sets are taken from the top of the Alexa database (Alexa, 2019) that ranks websites according to their internet popularity.

The web-service applications with content for different types of users are normally developed and offered with an application known as a content management system (CMS). One of the most popular CMSs is provided by the company WordPress. The product is known as the Word Press Content Management System (WPCMS). This WPCMS is very popular, due to the low cost of the software, the friendliness of its use and the easy maintenance of the website. The abundance of available plug-ins for the provision of rich web services enables the development of almost any type of web service and multiple scenarios for different types of users, such as blogs, social networks, banking, e-commerce, or educational services, all of which contribute to the popularity of the WPCMS. Plug-ins are used for the provision of different web-service applications. They are individual pieces of software that act as add-ons within the basic web software (e.g., the web-content system's core) to provide additional rich features for the web service. Currently, the estimated number of plug-ins that can be applied for a website's content is close to 56,000. According to a survey carried out by the W3Tech Consortium, about 52.9% of internet websites use some version of the WPCMS (W3Tech 2021). As these systems are known for their popularity, they become a frequent target of malicious attacks. These attacks are

often successful, which has triggered an urgent need for the CMS to be upgraded and protected with additional security features.

For our study, the website-scanning tool that was designed to access and inspect the websites built with the WPCMS application was called VULnet. The WPCMS system was chosen because it is the most widely applied, open-source tool for internet websites, and is used by both professional and non-professional users for the provision of web services. WPCMSs are normally maintained by ordinary users or the owners of web pages for blogs and other platforms. However, it is well known that many of them do not possess sufficient knowledge to install security features to protect their systems and remove the vulnerabilities from the web core or from the installed plug-ins. WPCMS applications, despite having the status of a popular open system, can be found in the website services of many well-known companies, such as NBC, CNN, TED, New York Times, Forbes, eBay, Best Buy, Sony, UPS, CBS Radio, TechCrunch and others (WordPress 2021).

The major difference between the developed scanning tool called Vulnet (Cigoj & Jerman, 2019) used in this study and other vulnerability scanners is the in-built automatic scoring system for assessing the security of the CMS core and the plug-ins of the inspected websites (Mell, 2007, CVSS, 2020). The scoring mechanism uses the identified vulnerability in a particular web-core system and the present plug-ins and calculates the insecurity index of that particular website. The risk level for a single vulnerability is obtained from a publicly available Common Vulnerability and Exposure (CVE) database maintained by the organization Mitre (Lalet, 2020). The CVE database contains more than 300 identified vulnerabilities of the WordPress web-core version and over 2168 identified plug-in vulnerabilities. The total risk level of a website is calculated as a sum of the detected exploitability of the number of vulnerabilities in the web core and in the plug-ins. The calculated risk of each website is described as low, medium or high. For example, functionalities such as an authentication requirement can receive the value none, single or multiple; similarly, the confidentiality can be none, partial or complete. The website-score system of Vulnet gives risk values that can be between 0 and 10, where 0 represents the lowest identified risk and 10 is the highest risk deriving from the exploitability of the identified vulnerability.

The scoring mechanism that calculates the total risk uses two sets of the detected exploitability: the first is the risk to the website's core C_([s]), and the second is the exploitability of the attached plug-ins P_([s]). The risk score for the website A_([s]), which denotes the insecurity of that website, is calculated as an aggregated score obtained from the score of the web-server core C_([s]) and the score of the attached plug-ins max(P_((s))) using the following equation:

$$A_{[s]} = \max\left(C_{[s]}, \max\left(P_{[s]}\right)\right). \qquad (1)$$

Equation 1: Vulnerability risk score calculation.

Where A_([s]) is the final risk score, maxf_0(P_[s]) is generated from the highest score detected among the risk scores of the plug-ins, and maxf_0(C_[s]) is the highest risk score among the vulnerabilities detected within the web server (the web core). The highest identified value between the two scores defines the web-risk score of the website.

The first scan across the whole internet with Vulnet was carried out in January 2021, providing 126,086,633 website connections. Among these websites, there were 16,274,980 with WPCMS installations and 17,126,445 with plug-in installations.

The web spaces of European countries were scanned in February 2021, and as a result a set of 23,131,336 websites was obtained. Of these, 3,738,654 websites (16%) were found to run WPCMS applications. In the European sample, the hosted websites on the same web server were selected as

individual websites according to the country-specific suffix of their domains, and this feature was not used before in any of the published studies with much smaller numbers of accessed websites. The collected sets of websites were from the following European countries: Germany (DE), Netherlands (NL), France (FR), Great Britain (GB), Italy (IT), Denmark (DK), Poland (PL), Spain (ES), Sweden (SE), Switzerland (CH), Czech Republic (CZ), Ireland (IE), Finland (FI), Austria (AT), Romania (RO), Belgium (BE), Hungary (HU), Bulgaria (BG), Norway (NO), Slovakia (SK), Estonia (EE), Slovenia (SI), Portugal (PT), Croatia (HR), Lithuania (LV), Luxembourg (LU), Greece (GR), Iceland (IS), Latvia (LT), and Cyprus (CY). The choice of these countries was based on the availability of the DS indexes and other relevant country data provided by Eurostat. The second source of data addressing the infrastructure in the study came from the databases of the International Telecommunication Union (ITU).

The smallest sample of inspected web spaces was 3554 websites belonging to Cyprus, and the largest sample was 805,279 belonging to Germany. This indicates a wide variability in the number of websites per country in Europe. As the number of websites with WP installations in Malta was too small, this country was not included in the study. Out of the total European sample of 3,738,654 WP websites, 1,339,325 were found to be vulnerable. The results are presented in Table 1. On average, a vulnerability status was identified in 34% of all the detected WP websites. For some websites the vulnerability could not be assessed because the WordPress application version of either the core or the plug-ins were not available, because it was hidden. This is a common practice of some web owners or maintainers. They decide to not provide information about the version number of the WPCMS application because they believe that when the version of the software is hidden, the probability that the website will be attacked is much lower, due to the fact that attackers will not know about the existing vulnerabilities. However, studies have shown that this belief is unfounded (Fonseca & Vieira, 2014).

Each plug-in or WP core-version insecurity was assessed according to the scoring system presented in equation 1. The websites were then classified based on the calculated scores into one of three categories: secure, insecure, and unknown. A website was considered secure if the core version and all the plug-ins (if any) were also secure, meaning that no vulnerability was detected.

Table 1: Summary Statistics of all WPs Found in the European Sample, with the Percentage of Vulnerable Websites

	Total WP	unknown [%]	Secure [%]	Insecure [%]	Critical [%]
Mean	124621.8	34.02	27.6	38.38	30.98
Std	183737.33	3.56	4.66	4.52	4.57
Min	864	27.38	21.22	30.31	22.1
25%	14924.75	31.38	24.19	35.32	27.29
50%	53261	34.21	26.05	39.44	31.97
75%	140195	36.98	30.98	41.57	34.76
Max	805279	40.15	37.85	47.37	41.31

The other set of data used in the study was obtained from the Eurostat survey data about the Digital index collected in 2021 (Eurostat 2021). The main reason for using the Eurostat statistics was the availability of the data for all the EU member states, in addition to the data of two other European countries that are not EU members (Switzerland and Norway). Another reason for this country selection was the fact that the Eurostat data are standardized at the international level and are reliable, which ensures that the results will have a high degree of reliability.

The use of DS as an indicator of digital development was presented for the first time in 2016, and from that time new data about DS levels are provided regularly each year. Eurostat recognizes three

levels of digital skills: low, medium (basic) and high. These are based on the required skills in four knowledge domains: information, communication, problem solving, and software usage. Individuals with an "above basic (high)" skill level have "above basic skills" in all four domains of knowledge specified in the Eurostat DS definition. Individuals with a "basic (medium or middle skill level)" skill level display at least one "basic" skill among the four defined areas, but they do not have ("no skills") in the other four domains, with the exception of the only area for which it has been proven that basic skills are present. Individuals with a "low" skill level are missing basic skills: from one to three "no skills" in the four domains. Other data used in the study were taken from ITU surveys (ITU, 2021). These are as follows: the frequency of internet use by the population [FoIU], the number of households connected to the internet [HH], the cost of fixed access to the internet, the content-creator index [CC] and the gross national income of the country (GNI).

3 Applied Study Methods

The differences between the number of vulnerabilities in the web spaces across Europe and the impact of the digital-skill levels on a higher or lower level of security were studied using a statistical method known as factor analysis [FA], which is a multi-variate statistical technique that allows us to analyze the interdependences between a broad set of variables, and at the same time also enable the selection of common and unique influential factors that are not correlated. Authors such as Crusz-Jezus et al., (2012) and Corrocher & Ordanini, (2002) consider FA to be an especially appropriate statistical technique to analyze digital development with the underlying digital infrastructure. The following variables were considered in the study: digital skills [DS], gross national income [GNI], the cost of fixed access to the internet [Fix], number of households with access to the internet [HH], frequency of use of the internet by the population [IU], and the content-creator index [CC].

The FA method involves several steps, and the technique depends on the correlation structure of the studied sample. This correlation structure of the data sample was inspected using a correlation matrix and the results showed that the variables from the Eurostat and ITU databases are closely correlated, so that the dominating factors had to be identified. The suitability of the data sample was evaluated using the Kaiser–Mayer–Olkin (KMO) method and Bartlett's test. The KMO test is a statistical measure to determine how suitable a data sample is for a FA. The test measures the sampling adequacy for each variable in the model. The KMO value varies from 0 to 1, if these values are between 0.8 to 1.0 the sampling is considered to be adequate. Bartlett's sphericity test provides information about whether the correlations in the data are strong enough to use a dimension-reduction technique such as common-factor analysis, while numbers below 0.05 suggest that there is substantial correlation in the data. Bartlett's test gave the following values: the chi-square was 320,655425 and $p < 0.001$, which confirmed that the result was statistically significant. The KMO test for the suitability of the data returned a value of 0.869799, which is higher than 0.77, and thus confirmed the suitability of the data sample. Cronbach's alpha index is a measure of the internal consistency of the data and how closely related a set of data is as a group, and is used to measure the reliability scale of the factors and informs us about the internal consistency and the reliability scale of the data. This index gave a result of more than 0.7, which is considered a good result for the reliability of the data. The next step was the identification of the latent dominating factors and the interpretation of these with the use of varimax rotations and the factor loadings. The results of the FA are presented in Table 2, which provides the factor loadings, while the varimax rotated factor loadings are provided on Table 3. The loading pattern determines the factor that has the most influence on each variable in the data set. Numbers close to -1 or 1 indicate that the factor strongly influences the variable. Values of 0.7 or higher for the factor loading suggest that the factor

extracts sufficient variances from the variables. The selected factor, DS and the cost of fixed internet access (0.96 and 1.02) were appropriate values. The rotated values of the loadings with the varimax method, and the communalities presented in Table 3 are also appropriate as the numbers of rotated loadings are close to 1 (0.92 and -0.88). The communalities appeared to be appropriate as they are higher than 0.7 (0.86 and 0.75). The cumulative and proportional variances presented in Table 4 are also higher than 0.6 (0.74 and 0.79).

Table 2: Factor Loadings

	Factor 1	**Factor 2**
DS	0.96	0.03
DESI	0.89	0.09
GNI	0.66	-0.26
HH	0.93	-0.01
IU	0.89	-0.13
FoIU	0.97	-0.02
Fixed	0.03	1.02

Table 3: Rotated Loadings with the Varimax Method: Factor Loadings and Communalities

	Factor 1	**Factor 2**	**Communalities**
DS	0.92	0.08	0.86
DESI	0.82	0.14	0.69
GNI	0.83	-0.11	0.79
HH	0.93	0.05	0.86
IU	1.00	-0.09	0.65
FoIU	0.99	0.05	0.98
Fixed	0.14	-0.86	0.75
CC	0.58	0.44	0.52

Table 4: Variances

	Variance	Proportional variance	Cumulative variance
Factor 1	5.91	0.74	0.78
Factor 2	0.37	0.79	0.73

Based on the FA results, two factors were selected for analyzing the data as they were found to accumulate the largest-possible amount of information from the data set (the accumulated total variance explained is close to 80%, and this is in line with Pearson's criterion and the Kaiser method). The oblique rotation varimax of the factors (the loadings used to achieve a better split of the original indicators provided the factor number 1) is more strongly connected to the variables DS, DESI GNI and the variables connected with internet use, like IU and FoIU, while the variable cost of fixed access loads on factor 2. This factor, therefore, reflects the influence of the internet infrastructure's affordability (as the cost of fixed internet access was normalized with the GNI of the country), while factor 1 reflects mainly the underlying socio-cultural influences.

Among the methods available to interpret the relationships between the variables, linear regression is the most-used method. The linear method summarizes the functionality and parametric relationship between the variables. The linear method distinguishes two types of variables, i.e., independent and dependent variables, and makes it possible to follow the changes of the independent variables on the values of the dependent variables. In our case this applies to the appearance of higher or lower insecurity of the websites. The model presented is in the form of a linear equation between the variable Yi and the independent variables Xi1, Xi2, … Xin (Hastie & Chambers, 1992).

The regression between digital skills and the number of WP websites marked as insecure gave r = -0.68, which suggested a linear dependence. The calculated model of the appearance of insecurity was found to be:

$$insecure = 50.38 - 0.2 * DS \quad (2)$$

Equation number2: insecurity model

With R^2 = 0.463 and RMSE = 3.25. These values were significant, with F (1, 29) = 24.11 and p < 0.001. The RMSE is the square root of the variance of the residuals. It indicates the absolute fit of the model to the data and how close the observed data points are to the model's predicted values. Lower values of RMSE indicate a better fit of the data. R squared is a relative measure of the fit, and an improvement in the regression model was made that showed an increase in R squared. The improvement to the model was based on the removal of the residual outlier (LT) and the leverage points (IS) and (LU). These three countries have very low populations: IS has only 357,000 inhabitants; LU (which is also a very small country similar to IS) is characterized by the concentration of businesses from banking, finance, and commerce where information security is very important, but shows only very moderate skill levels in the country's population. This can be explained by the fact that most employees within these sectors are not citizens of Luxembourg, most of them do not live in Luxembourg and are not captured in the population surveys. The new model provided the following regression equation:

$$insecure = 52.64 - 0.25 * DS \quad (3)$$

Equation 3: the improved web insecurity model

Where R^2 increased to 0.67 and RMSE dropped to 2.48. The summaries of both regression models are presented in Table 5. The linear regression shows that a higher level of digital skills has a negative impact on the presence of insecure WPCMS websites. It is assumed that a population with a higher DS index of digital skills possesses more knowledge and is more aware of the potential security risks among users and web owners, and as consequence either demand the maintainers improve the security or if they are the website owners, they do that themselves. This behavior can impact on the number of vulnerable WP websites, making that number lower. These facts lead to the conclusion that the DS of a country's population is a negative factor for web insecurity. The regression-analyses summary is presented in Table 5.

Table 5: Regression-Analysis Results

		Summary of regression results											
		95% CI					Goodness of-fit						
Model	regressors	coef	SE	beta	lower	upper	residuals	F-static	p-value	AIC	BIC	R^2	RMSE
1: insecure~DS	const	50.38	2.52		45.22	55.55	28	24.11	<0.001	160	162.8	0.463	3.25
	DS	-0.2	0.04	-0.68	-0.29	-0.12							
2: insecure~DS	const	52.65	2.11		48.30		25	50.68	<0.001	129.7	132.3	0.67	2.48
	DS	-0.25	0.04	-0.82	-0.33	-0.18							

4 Results

The regression analysis indicated that a higher level of digital skills may have a negative impact on the number of insecure WP websites. In a country having a population with higher DS indexes and more digital knowledge a smaller number of insecure websites is detected. Higher numbers for digital skills contribute to a greater awareness and knowledge about security and the need for protective measures to be applied for the web users, owners or maintainers. This finding can also be generalized to the presence of a greater awareness among a country's population about the security risks and applying sufficient precautions when using web services. The percentage of web insecurities in European countries and the value of DS are illustrated in Fig. 1

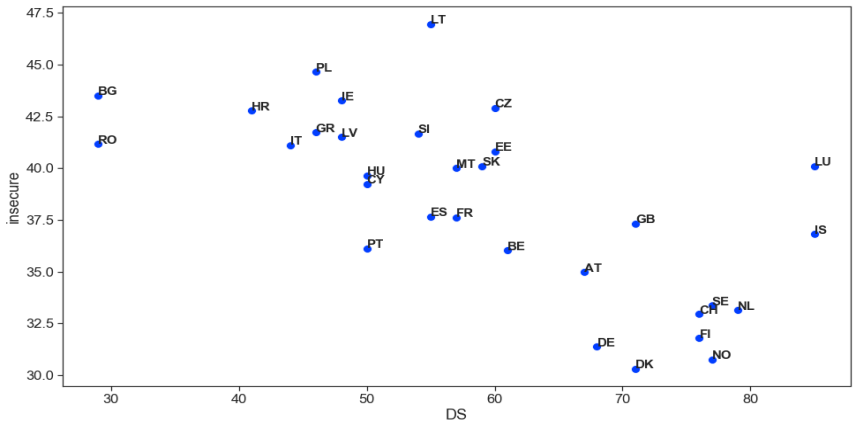

Figure 1: DS Values in European Countries and the Percentage of Insecure Websites

Five groups of countries can be identified in Fig. 1. The first group of countries with a low percentage of insecure sites and high levels of DS indexes contains the following: Denmark, Germany, Switzerland, Norway, Finland, Sweden, and Netherlands. The second group of countries with a higher number of in-secure websites and a moderate level of DS includes Great Britain, Austria and Belgium. The third group of countries that have more insecure websites includes Estonia, the Czech Republic, Slovakia, Malta, and Portugal. The fourth group with a higher number of in-secure websites includes Cyprus, Latvia, Greece, Ireland, Poland, Croatia, Hungary, Italy, Slovenia, and Lithuania. The group composed of Romania and Bulgaria has the lowest values of DS in their populations.

The dependencies between the next digital index that contains in addition to DS information about some economic factors DESI and the websites' insecurity are presented in Fig. 2 with an indication of the DS values in each country denoted with a different color. The second selected factor—the fixed cost of access to internet normalized with GNI—provided similar groupings of European countries regarding the percentage of insecure websites. GNI (Gross National Income) is a measure of a country's economic power, and as such has an impact on the cost of digital services. Fig. 3 presents the distribution of European countries in terms of the percentage of insecure websites and the cost of fixed internet access normalized with GNI, with represented levels of DS in different colors. Countries with low values of DS and a high cost of access to internet have a much higher numbers of insecure websites, while those with low costs of fixed internet access and higher values of DS have fewer insecure websites. Only Romania and Cyprus show a moderate cost of fixed internet access, but both countries have a higher percentage of insecure websites.

The grouping of countries in Fig. 3 is similar to those in Fig. 2. The first group with the smallest percentage of insecure websites and a low cost of internet access is composed of Sweden, Netherlands, Denmark, Norway, Switzerland. The next group consists of the same group of countries identified with moderate levels of DESI, as in Fig 2. Belgium, Great Britain, and Austria, but Spain and France show lower levels of internet-access cost and a moderate percentage of insecure websites. The next group of countries with a higher percentage of insecure websites and moderate costs of internet access is composed of Estonia, Cyprus, Slovakia, Ireland, and Romania. More differences can be observed in the fourth and fifth groups, where Greece, Czech Republic, Croatia and Latvia can be allocated to the fourth group, and the fifth group is composed of Slovenia, Hungary and Italy, which have joined Bulgaria, identified as a country with very low DS index. Romania, which has advanced its ranking as the cost of internet access is more affordable compared to the other countries (as the communication infrastructure was recently improved), but the DS index has not changed much when compared with some earlier studies.

The low cost of fixed internet access is a positive factor for a higher percentage of secure websites. Although the members of each of the identified groups in both studies illustrated in Fig. 1, Fig2 and Fig 3. do not overlap completely, the country allocations in each of the identified groups are similar.

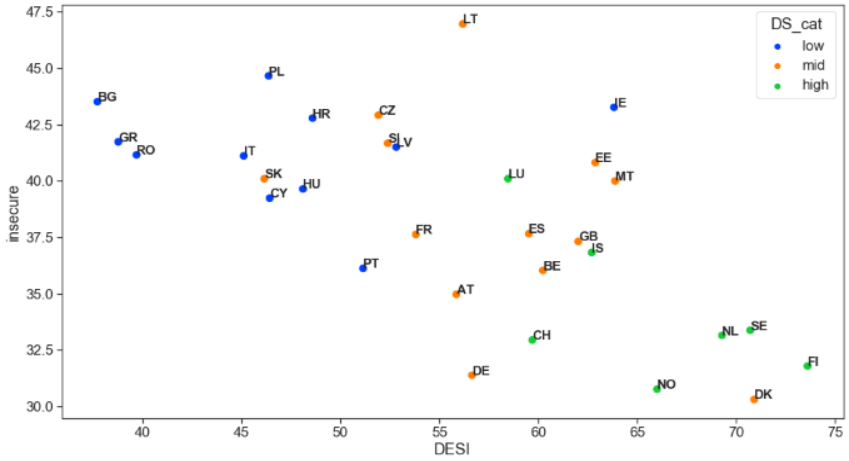

Figure 2: DESI Values of the European Populations and the Percentage of Insecure Websites

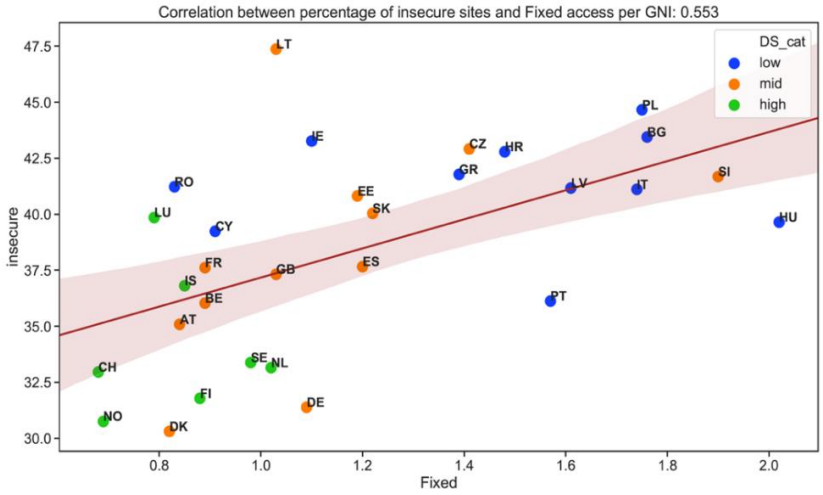

Figure 3: Fixed Cost of Access to the Internet and the Percentage of Insecure Websites

The results presented above confirmed that the inequalities in the digital skills of a country's population make a difference regarding the percentage of insecure websites in the country's web space. The same applies to the affordability of the digital infrastructure, which differs among European countries and impacts on the overall security of a country`s web space. The reason for that can be found in the level of investments and the introduction of policies to speed up the digital development by the country's authorities. Leading countries with a lower percentage of insecure websites are countries with greater economic power and developed economies where the investment in digital development is high. These are Germany, Denmark, Austria, Sweden, Belgium, Finland, Netherlands, Switzerland, and Norway. These countries have high DS values for their population, and this leads to the conclusion that digital skills in a country's population have an important role in the overall security of the internet web spaces. A higher DS index implies a lower percentage of vulnerable websites, and a more affordable use of the internet infrastructure contributes to a lower percentage of insecure websites as well. The bivariate statistical outliers that were found to be Lithuania, Luxemburg, and Iceland, did not change the image much.

To complement the study, the security of the internet web spaces among the websites offering services in different economic sectors of Europe was explored as well. The explored websites were in the following sectors: healthcare, finance, news, education, research institutions and the services offered by different types of societies or associations. For each of these six sectors, keywords (up to 60) were selected to describe their content. These sectors were selected according to a survey carried out by the Concordia Cybersecurity Competence Center, which focused on specific industry sectors by relying on the web services for which data protection and the overall security of their infrastructure were found to be of utmost importance (Concordia, 2022). The keywords denoting the areas where these sectors act were translated into the national languages spoken in each of the European countries. Some European languages have specific letters or use a non-Latin alphabet (e.g., Cyrillic or Greek), and as a consequence may have several synonyms for the selected words describing a particular sector. The selected keywords were translated, and the synonyms were included in the data set as well for some countries with several official languages, for example, Luxembourg, Belgium and Switzerland, several sets of keywords were written in different languages and included in the dataset of keywords. A summary of the sample statistics is presented in Table 6.

A one-way variance analysis for analyzing the effect of the sector/field type (news, education, health, institute, finance, society, others) on the percentage of insecure websites gave the following result, $F(6, 203) = 7.92$, $p - value = 0.000$, with an effect size $\omega = 0.17$. Turkey's HSD test was used to determine which field (or sector) had a significantly lower average percentage of insecure websites. It was found that news (where $p = 0.001$) was the sector with the lowest percentage of insecure websites. However, no significant statistical differences were found among the other sectors, although the highest percentage of insecure websites belonged to the sectors of education and finance.

Table 6: Summary Statistics of the Percentage of Insecure WP Websites for Each Sector

					95% CI	
SECTOR	**N**	**Mean**	**SD**	**SE**	**Lower**	**Upper**
EDUCATION insecure	30	38.58	6.72	1.23	36.14	41.03
FINANCE insecure	30	38.25	6.56	1.2	35.86	40.63
HEALTH insecure	30	37.64	5.68	1.04	35.57	39.71
INSTITUT insecure	30	38.88	6.04	1.1	36.69	41.08
NEWS insecure	30	29.05	7.91	1.44	26.17	31.93
SOCIETY insecure	30	36.69	9.12	1.66	33.37	40.01
OTHER insecure	30	38.5	4.61	0.84	36.82	40.18

Within the whole sample, the education sector appeared to have the highest percentage of insecure websites in the following countries: Slovenia, Latvia, Spain, Great Britain, Austria, Netherlands, Germany, and Norway. The finance sector showed the highest share of insecure websites in Lithuania, Iceland, Ireland, Estonia, France, and Switzerland. The largest share of insecure websites in the health domain was found to be in Bulgaria, Italy, and Sweden. The institute/association sector had the largest percentage of insecure websites in Cyprus, Poland, Luxemburg, the Czech Republic, Belgium, and Slovakia. For the news sector, the largest percentage of insecure websites was found in Denmark and Finland, while the societies had the highest percentage of insecure websites in Croatia, Greece, Hungary, and Portugal.

Figure 4 presents the results of the study in the form of clusters. The different levels of insecure WP websites are marked with different colors, where each color represents the percentage of insecure websites. Green squares indicate a low percentage of insecure websites, reddish squares indicate the highest percentage of insecure websites. The sector clustering in Fig. 4 shows that the sectors Finance and Institute together with the sectors Education and Health have a similar distribution of insecure

websites per country. Two big groups of countries with similar distributions across all sectors were identified. The first group is composed of Estonia, Iceland, Denmark, Finland, Netherlands, Austria, Germany, Norway, Sweden, and Switzerland, showing a lower percentage of insecure websites in all sectors, while the rest of the studied countries form the second group with a higher percentage of insecure websites. The smallest number of insecure websites was found to be in the news sector. This can be explained by the fact that this sector normally uses familiar commercial platforms, and consequently the number of detected websites with WPCMS applications in this sector is very small compared to the other sectors. It is well known that commercial platforms are usually much better maintained and are more frequently checked for vulnerabilities. Any identified vulnerabilities are removed and the sites are updated with the newest software.

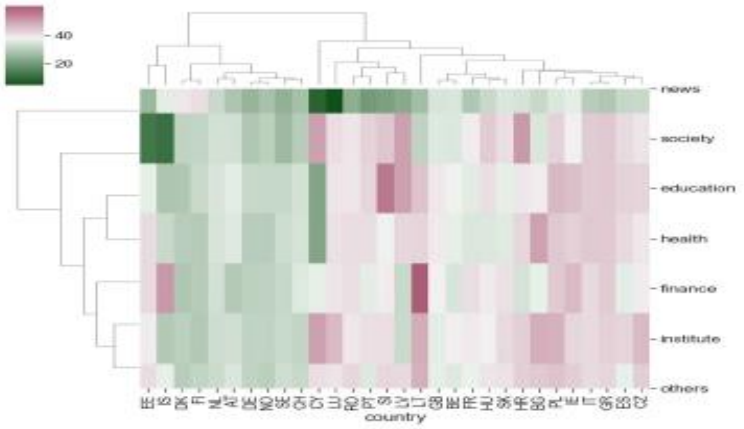

Figure 4: Clustering of the Economic Sectors According to the Web Security

5 Discussion

Most of the digital-inclusion studies agree with the idea that the ICT uptake and engagement for improving the digital literacy among a country's population contribute to the level of digital skills. The adopted knowledge leads to a range of positive outcomes for the individuals and society (Robinson et al., 2018). A study of the inequality of digital skills and the adoption of online safety behaviors (Dodel & Mesch, 2018) proposes two different scenarios for a better uptake and more secure user behavior (van Deursen et al. 2017; Robinson et al. 2018; Livingstone & Helsper 2013). The first scenario, which is based on technological diffusion followed by an educational pathway, contributes equally to the knowledge and the skills in all countries and segments of society. The other scenario known as the stratification model of technology diffusion supposes that social groups and countries with pre-existing advantages derived from older socio-economic stratifications will maintain their edge in the digital economy as well. The associated skills by the population will advance even in the case of an increase in the digital uptake worldwide (Cruz-Jezus et al., 2012). Which of these scenarios is true can be determined by looking at the study of the digital inequalities and the digital development of European countries carried out 10 years ago and compared with our findings (Cruz-Jezus et al., 2012).

The research findings presented in the study show that the leading countries in Europe in terms of digital development and the associated digital skills have the lowest percentage of insecure websites and a safer internet infrastructure. The leading countries that have maintained their edge are located in the north of Europe. They are Denmark, Sweden, Netherland, Finland, and Norway. The data in the study from Cruz-Jezus et al., (2012) about the digital inequalities in Europe published before the DS index was developed, concluded that the leading countries in Europe were Denmark, the Netherlands, and

Sweden. These countries were best ranked regarding the level of digital development and the skills among their population. The next group of countries was identified as a group of moderate advancers like Finland, Switzerland and Norway, where the advantage in the socio-economic stratification contributed so that after 10 years of development, they become leading countries. Great Britain, Belgium and Luxembourg stayed in the group with a moderate level of digital development and a moderate percentage of insecure websites. Bulgaria and Romania formed the group of the least digitally developed countries in the EU-27, having extremely low levels, on average, for all dimensions used in the Eurostat study (Eurostat 2019; Robinson et al. 2018). They formed the group of "digital laggards". Our study brought similar results as these two countries still have very low levels of DS and a high percentage of insecure websites. Other European countries, such as Hungary, Latvia, and Slovenia, were evaluated as countries with a well-developed ICT infrastructure, but with a very low level of using e-business and services (Cruz-Jezus et al., 2012). This was considered to be a group with a highly unbalanced digital development. Ten years later our study shows that the pathways for digital development in these countries were different. Slovenia has a high cost of fixed internet access, a moderate level of DS and a large number of insecure websites. Hungary is not a follower of the advanced countries and belongs to the group with a high percentage of insecure websites and a low DS level. For Cyprus, the Czech Republic, Greece, Italy, and Lithuania, they were known to have an unbalanced digital development. The situation ten years later has not changed. In our study, Lithuania appeared as an outliner, but also as a country with unbalanced development, while Luxembourg as a leading country in the past study did not advance as expected. The other three countries that were found to have an unbalanced development are joined by Croatia, Latvia, Ireland, and Poland. These countries have a high cost of internet access, low DS levels and a large percentage of insecure websites. The unbalanced development in this country was obviously not resolved in the past 10 years. The Czech Republic together with Slovakia, Spain, and Portugal remained in the middle group with a moderate or low level of DS and a considerable percentage of insecure websites. Changes in the development were noticed in Romania, where the ICT infrastructure was much improved, the cost of internet access is not high and more affordable services are offered to the country's population.

Geographically, the intermediate values of digital development were found in the European regions located in the central zone spanning from the west to the east of the continent: Spain, Ireland, Slovakia, Slovenia, Latvia, Lithuania. The lowest values of digital development were found in South-East Europe and also in some regions belonging to Portugal, Greece, and Italy. These findings are very close to the results of the current study presented above as these countries together with the Baltic countries (with the exception of Estonia) belong to the fourth and fifth groups of countries that show the highest percentage of vulnerable websites and low levels of digital skills.

These findings show that the second scenario of digital development dominates among the European countries, as the pre-existing advantages derived from older socio-economic factors maintained the edge in digital development in the 21st century and not the spread of IT technology. The knowledge and the affordability of internet access in a country's population, being a pre-existing advantage, was confirmed to be an important factor for the digital development and the provision of secure digital services. The advanced state policies for digitalization in the past maintain the edge of the leaders, but if properly applied, they still can help the newcomers join the group of leaders.

It that context it is important to note that that the awareness and the knowledge of the flaws of web systems among the web owners contribute much to the presence of web-space insecurity being lower. The responsibility for remediating the web resources with vulnerabilities should be shared between web maintainers and the software providers such as WordPress. Frequently, they are accused of not regularly

informing their consumers and not doing enough to remove the vulnerabilities in their products. Fortunately, this is changing over time. The current local database of available WPCMS systems contains 430 different web-core versions of the Word Press supplier. In recent years, the users of these systems were informed that 90 of them contain critical vulnerability flaws. However, due to the warnings regarding web insecurities in 2019, the number of applications with flaws dropped to only 8 vulnerabilities and as a consequence the web users updated their systems. This trend shows that although the number of new WordPress versions delivered to the users increases with the years, the number of identified vulnerabilities decreases. The updated, old application versions and their replacement with clean versions are changing the WPCMS insecurity statistics. However, the problem of plug-ins applied to web systems is still a major contributor to vulnerability and remains unsolved.

6 Conclusions

The presented study clearly confirms that the knowledge of the country's population impacts on the insecurity of web spaces. The same holds for the affordability of the internet access. The developed tool Vulnet that was used for collecting the data about the vulnerabilities on the internet was acting as an ethical tool (the website is not attacked) and is capable of inspecting the website and collecting information without attacking it. The collected data enabled us to identify the impact factors for higher insecurity among European web spaces. A higher value for the population's digital skills and a lower cost of internet access in the studied countries have a positive impact on the availability of more secure websites. The applied tool and the developed security-score mechanism showed good reliability when compared to other available tools for inspecting the vulnerability of the WPCMS and the conducted studies for digital inequality. The study introduced a new index for measuring the affordability of internet access in a country. The designed indexes were found to be relevant and important factors that reflect the insecurity in a country's web space.

References

[1] Alexa, (2019). http://www.alexa.com, Accessed November 17, 2019

[2] Anderson, L., Ostrom, A.L., Corus, C., Fisk, R.P., Gallan, A.S., Giraldo, M., & Williams, J.D. (2013). Transformative service research: An agenda for the future. *Journal of Business Research*, *66*(8), 1203-1210.

[3] Büchi, M., Festic, N., & Latzer, M. (2018). How social well-being is affected by digital inequalities. *International Journal of Communication*, *12*, 3686-3706.

[4] Cigoj, P., & Blazic, B.J. (2019). An intelligent and automated WCMS vulnerability-discovery tool: the current state of the web. *IEEE Access*, *7*, 175466-175473.

[5] Concordia, (2022). https://www.concordia-h2020.eu

[6] Corrocher, N., & Ordanini, A. (2002). Measuring the digital divide: a framework for the analysis of cross-country differences. *Journal of Information technology*, *17*(1), 9-19.

[7] Cruz-Jesus, F., Oliveira, T., & Bacao, F. (2012). Digital divide across the European Union. *Information & Management*, *49*(6), 278-291.

[8] da Fonseca, J.C.C.M., & Vieira, M.P.A. (2014). A practical experience on the impact of plugins in web security. *In IEEE 33rd International Symposium on Reliable Distributed Systems*, 21-30. https://www.researchgate.net/publication/286668217

[9] Dodel, M., & Mesch, G. (2018). Inequality in digital skills and the adoption of online safety behaviors. *Information, Communication & Society*, *21*(5), 712-728.

[10] Durumeric, Z., Wustrow, E., & Halderman, J. A. (2013). {ZMap}: fast internet-wide scanning and its security applications. *In 22nd USENIX Security Symposium (USENIX Security 13)*, 605-620.

[11] EU-Commission. (2016). DESI 2016 Country Profiles: https://ec.europa.eu/digital-single-market/en/news/desi-2016-country-profiles
[12] Eurostat (2020). The Digital Economy and Society Index (DESI), https://digital-strategy.ec.europa.eu/en/library/digital-economy-and-society-index-desi.
[13] Eurostat. (2019). Individuals who have basic or above basic overall digital skills by sex. https://ec.europa.eu/eurostat/web/products-datasets/product?code=tepsr_sp410
[14] Graham, R., (2020). Masscan: A Fast and Scalable IP Port Scanner accessible on: https://securitytrails.com › blog › masscan
[15] Greco, S., Ishizaka, A., Tasiou, M., & Torrisi, G. (2019). On the methodological framework of composite indices: A review of the issues of weighting, aggregation, and robustness. *Social indicators research*, *141*, 61-94.
[16] Hastie, J., & Chambers, J.M. (1992). Statistical models in S. Wadsworth & Brooks.
[17] ITU, (2019). World Telecommunication/ICT Indicators Database – ITU, International Telecommunication Unit. https://www.itu.int/en/ITU-D/Statistics/Pages/publications/wtid.aspx
[18] Joshi, D.R., Neupane, U., & Joshi, P.R. (2021). Synthesis review of digital frameworks and DEPSWALIC Digital competency framework for teachers from basic to University Level. *Synthesis*, *13*(2), 108-136.
[19] Kavitha R., et.al (2018). An efficient way of implementing omniscient algorithms for the world wide web. *Eurasian Journal of Analytical Chemistry*, *13*(3), 1207-1213.
[20] Kim, H., Kim, T., & Jang, D. (2018). An intelligent improvement of internet-wide scan engine for fast discovery of vulnerable IoT devices. *Symmetry*, *10*(5), 1-16.
[21] Kos-Łabędowicz, J., & Urbanek, A. (2017). Do Information and Communications Technologies influence transport demand? An exploratory study in the European Union. *Transportation research procedia*, *25*, 2660-2676.
[22] Lalet, P., (2020). MITRE organization, the e-book. https://www.perforce.com/
[23] Livingstone, S., & Helsper, E.J. (2013). Children, internet and risk in comparative perspective. *Journal of Children and Media*, *7*(1), 1-8. https://www.tandfonline.com/doi/abs/10.1080/17482798.2012.739751
[24] Lucendo-Monedero, A.L., Ruiz-Rodríguez, F., & González-Relaño, R. (2019). Measuring the digital divide at regional level. A spatial analysis of the inequalities in digital development of households and individuals in Europe. *Telematics and Informatics*, *41*, 197-217.
[25] Lutz, C. (2019). Digital inequalities in the age of artificial intelligence and big data. Human Behavior and Emerging Technologies, 1 (2), 141–148.
[26] McGuire, M., & Dowling, S. (2013). Cyber crime: A review of the evidence. *Summary of key findings and implications. Home Office Research report*, *75*, 1-35.
[27] Mell, P., Scarfone, K., & Romanosky, S. (2007). A complete guide to the common vulnerability scoring system version 2.0. *In Published by FIRST-forum of incident response and security teams*, 1, 23. http://www.nist.gov
[28] Micheli, M., Lutz, C., & Büchi, M. (2018). Digital footprints: an emerging dimension of digital inequality. *Journal of Information, Communication and Ethics in Society*, *16*(3), 242-251.
[29] Nappa, A., Xu, Z., Rafique, M.Z., Caballero, J., & Gu, G. (2014). Cyberprobe: Towards internet-scale active detection of malicious servers. *In Proceedings of the Network and Distributed System Security Symposium (NDSS 2014)*, 1-15. The Internet Society.
[30] Nedelcheva, Y. (2021). Competitiveness assessment concepts. *Revista inclusiones*, 49-61.
[31] Noussan, M., & Tagliapietra, S. (2020). The effect of digitalization in the energy consumption of passenger transport: An analysis of future scenarios for Europe. *Journal of Cleaner Production*, *258*, 1-15.
[32] Park, Y. J. (2013). Digital literacy and privacy behavior online. *Communication research*, *40*(2), 215-236.
[33] Robinson, L., Schulz, J., Blank, G., Ragnedda, M., Ono, H., Hogan, B., ... & Khilnani, A. (2020). Digital inequalities 2.0: Legacy inequalities in the information age. *First Monday*, *25*(7).

[34] Salemink, K., Strijker, D., & Bosworth, G. (2017). Rural development in the digital age: A systematic literature review on unequal ICT availability, adoption, and use in rural areas. *Journal of Rural Studies*, *54*, 360-371.
[35] Schagen, N., Koning, K., Bos, H., & Giuffrida, C. (2018, April). Towards automated vulnerability scanning of network servers. In *Proceedings of the 11th European Workshop on Systems Security*, 1-6.
[36] Sfakianakis, A., Douligeris, C., Marinos, L., Lourenço, M., & Raghimi, O. (2019). Enisa threat landscape report 2018: 15 top cyberthreats and trends.
[37] Symantec enterprise cloud, (2019). https:// www.broadcom.com, Accessed 8. November 2020
[38] Thorncharoensri, P., Susilo, W., & Baek, J. (2019). Efficient Controlled Signature for a Large Network with Multi Security-level Setting. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)*, *10*(3), 1-20
[39] Van Deursen, A.J., & Helsper, E.J. (2018). Collateral benefits of Internet use: Explaining the diverse outcomes of engaging with the Internet. *new media & society*, *20*(7), 2333-2351.
[40] Van Deursen, A.J., Helsper, E., Eynon, R., & Van Dijk, J.A. (2017). The compoundness and sequentiality of digital inequality. *International Journal of Communication*, *11*, 452-473.
[41] WordPress, (2021). https://wpscan.com/ on 15 May 2021.
[42] WT3 TECH, (2020). hhtps://w3techs.com, accessed 15 May 2021.

Authors Biography

Prof. Borka Jerman Blažič is employed by Jožef Stefan Institute and the Department of Economics, University of Ljubljana, Slovenia. She worked as a scientist at Stockholm University in the period of 2011-2015 in the Unit of Computer Security. She has spent her postdoctoral study at Iowa State University, Ames, USA and has worked as a project development officer for TERENA, the Association of the European research and educational networks, in Amsterdam. She is currently engaged by the EU Competence centre for cyber security CONCORDIA, funded by H2020 EU program. Since 1999 she is a member of the New York Academy of science and a member of the Scientific Council of the European Privacy Association. Most of her activity and work are dedicated to cyber security. The latest research interest and work of Prof. Borka Jerman Blažič is in the area of cybersecurity, education, serious educational games, social application and trust. Prof. Jerman-Blažič has published several hundred articles in international journals, conferences, four books in the area and was an invited speaker in many international conferences or workshop meetings.

Primož Cigoj, **M.Sc.** earned his Master's degree and PhD degree at the Jožef Stefan International Postgraduate School in the area of Information Security under mentorship of prof. Jerman Blažič. He studied computer science at the University of Ljubljana, Slovenia and graduated from the Department of Computer Science and Informatics. His research interests include methods and technics for prevention of cybercrime, training in the area of Digital Forensic. His last research is addressing the web vulnerability at large on the internet.

Andrej Jerman Blažič is holding B.Sc. degree in informatics from the University of Maribor and PhD degree in e-sciences from the International postgraduate school Jožef Stefan. Part of his post graduate study he performed at Sundsvall University Sweden at the Department of computer communications and on the INESC –ID, Department of Information systems and Computer Science, Institute Superior Tecnico, in Lisbon Portugal. His research interest is in the area of technology supported e-learning, networking and cyber security education. He has participated in the EU funded research projects from the areas related to technology enhanced learning (ICamp (Innovative, inclusive, interactive and intercultural learning campus), ELENA (Creating smart space for learning) and UNITE). He is author or co-author of several published papers on international conferences and journal.