ISBN: 978-628-95207-8-1. ISSN: 2414-6390. Digital Object Identifier: 10.18687/LACCEI2024.1.1.666

Cybersecurity, State, and Law: A look from the scientific literature

1st Yasmina Riega-Virú*
Directorate of innovation, research & social responsibility
Universidad Privada del Norte
Lima, Peru
yasmina.riega@upn.edu.pe
*Corresponding author

2nd Mario Ninaquispe -Soto
Virtual Campus
Universidad Privada del Norte
Lima, Peru
mario.ninaquispe@upn.edu. pe

3rd Juan Luis Salas-Riega
Pontificia Universidad Católica del Perú
Lima, Peru
jlsalasr@pucp.pe

4 th Kiara Nilupu-Moreno
Faculty of Law
Universidad Privada del Norte
Lima, Peru
n00115494@upn.pe

5 th José Miguel Salas-Riega
Pontificia Universidad Católica del Perú
Lima, Peru
jmsalasr@pucp.edu.pe

6th Edgar Puga -Ayala
Faculty of Law
Universidad Privada del Norte
Lima Peru
edgarmpuga@gmail.com

***Abstract* — The degree of vulnerability to cyberspace threats sometimes goes unnoticed; However, it currently involves States worldwide; The objective of the study is to know the policies and programs on cybersecurity that the States have implemented, as well as the knowledge about cybersecurity that the population has. Through a systematic review of the literature, 50 articles from the Scopus database were analyzed; The analysis method was based on the five international pillars established by the International Telecommunications Union. It was found that States are responding through policies and programs that allow the population's knowledge of cybersecurity; in addition to identifying ways to reinforce it. The work of the United States and the United Kingdom stands out, they show significantly positive progress. It is concluded that most countries in the study are still evaluating their population on Cybersecurity issues. No studies could be identified that present training plans oriented to the stages of basic education, this population being identified as vulnerable. It is expected that Latin American countries will soon begin their research on cybersecurity policies; During the process of this paper, no studies from this region were identified.**

Keywords* — *cybersecurity policies, cybersecurity programs, cybersecurity trends, pillars, ITU

I. Introduction

Cloud computing, mobile devices, and broadband networks have allowed for a deeper transformation in governments and companies [1]; It is unknown to anyone that cyberspaces not only created benefits for society; but also, a unique opportunity for criminals, who take advantage of the speed, convenience, and anonymity of the Internet to commit criminal activities that know no borders [2]. Cybercrime is considered a service that can be purchased. Crime as a Service is a new business model that facilitates the commission of crimes around the world; Hackers, like any other company that adopts cloud computing to store their files on services like Google Drive, and Amazon, use stolen credit cards, fake identities, and front companies to rent space to legitimate companies like Amazon, to host malware on their servers. They also make extensive use of virtual private networks (VPNs) and proxy servers that hide their Internet Protocol addresses and hide their locations; In addition, they buy accommodations in Russian or Ukrainian companies where they do not require the identity of their clients and accept anonymous payments in Liberty Reserve and Bitcoin [3].

As expected, the increase in cyber risks forces companies and governments to integrate cybersecurity into their processes, in the acquisition of technology, and in the selection of personnel to respond to cybercrime [1]. According to the Cyber Center of Excellence (2016), demand for cybersecurity products increased by 14.7% between 2011 and 2013, while consumer demand increased by 10.7%. Therefore, it can be stated that cybercrime has gone from being a specialist topic to becoming a general policy concern [4]; Therefore, it is considered to ask: Are the States responding with Cybersecurity actions? What cybersecurity policies and programs have been implemented? And lastly, but not least, what is the population's knowledge of cybersecurity?

A. Cyberspace, cybersecurity, and cyber defense

Cyberspace is real, since although it is true it is artificial created by computers connected to the Internet; It is there where people interact and where various computer crimes occur; Faced with this, cybersecurity arises as preventive, corrective or monitoring actions carried out by natural or legal persons, aimed at ensuring the use of their own networks and denying it to third parties; to preserve confidentiality, availability, and integrity of the information. Cyber defense consists of the resources, activities, tactics, techniques, and procedures that the Armed Forces oversee, to guarantee the security of the command-and-control systems and allow the exploitation and response of the necessary systems that allow free access to cyberspace. for the effective development of military operations [4] Currently, the framework is widely disseminated in the business sector as one of the best practices for Cybersecurity.

B. Cybersecurity and the Role of the State

Faced with the risks of the stability and security of cyberspace that violate or may violate protected legal assets, including cybersecurity itself [5]; the State must respond

Digital Object Identifier: (only for full papers, inserted by LACCEI).
ISSN, ISBN: (to be inserted by LACCEI).
DO NOT REMOVE

legitimately; In this regard, the European Union approved the joint communication from the European Parliament and the Council called "Resilience, deterrence and defense: strengthening EU cybersecurity", through which a so-called Cybersecurity Package is presented that includes the creation of the Agency of Network and Information Security of the European Union (ENISA), whose function is to help Member States, EU institutions and companies to confront cyberattacks [6] In 2013, the United States commissioned the National Institute of Standards and Technology (NIST) to develop the Cybersecurity Framework for the protection of critical infrastructure, today known as the Cybersecurity Framework (CSF). which constitutes a tool for cybersecurity risk management applicable in all critical infrastructure sectors. Its preparation under a participatory methodology of the government, industry and academia considers standards already accepted by the cybersecurity ecosystem, such as NIST SP 800-53 Rev.4, ISO/IEC27001:2013, COBIT 5, CIS CSC, and others. cybersecurity governance [7].

C. The International Telecommunication Union (ITU)

The ITU is committed to connecting every global citizen, regardless of their location or resources by carrying out various actions, defending and supporting the universal right to communication. The Global Cybersecurity Index developed by the International Telecommunication Union (ITU) has launched four editions, the most recent being in 2020, published in June 2021 [8].

The fourth edition of ITU 2020 is a reliable reference that measures the commitment of countries to cybersecurity worldwide, to raise awareness about the importance and different dimensions of the topic; The index is made up of five pillars:

1. Legal Measures (Regulations on cybercrime and cybersecurity).
   a. Countries with some type of cybersecurity legislation
   b. Data protection regulations
   c. Regulation on essential infrastructure.
2. Technical Measures (Application of technical capabilities through national and sectoral organizations).
   a. EIII (Intervention Team in cases of Computer Incidents).
   b. Participate in a regional EIII.
   c. Online child protection reporting mechanisms.
3. Organizational Measures (National strategies and organizations that apply cybersecurity).
   a. National cybersecurity strategies.
   b. Cybersecurity agencies.
   c. Information is provided on online child protection strategies and initiatives.
4. Capacity Development (Measurement of awareness campaigns, training, education, and incentives for cybersecurity training).
   a. Countries that carry out awareness-raising initiatives.
   b. Countries with R&D programs in cybersecurity.
   c. Countries that declare they have national cybersecurity industries.
5. Cooperation (Measurement of associations between organizations, companies, and countries).

Each nation is examined considering its degree of progress or involvement in each of these pillars and aggregated into an overall score.

D. Trends

Among the measures to improve cybersecurity, as Goodman [3] points out, that data reduction must be a permanent practice, since accumulated data, whether personal records, medical records, banking records, government secrets, or corporate intellectual property, are subject to leaks and can be exploited by organized crime. Some models allow managing the information life cycle. These models contemplate:

1. Creation of information: Compilation and capture of information through various media.
2. Information storage: At this stage, we must answer the following questions: Where is the information stored, locally or internationally? Are legal issues such as data privacy considered?
3. Exchange and use of information: It is the stage where data is available to users of the organization and allows value to be generated for organizations.
4. Data archiving: This is the stage where the data is no longer necessary for the organization's management, but its storage is needed for legal issues such as litigation. It is important to know at a legal level how long the information is required to be stored.
5. Deletion of information: At this stage, the data is securely deleted.

Regarding passwords, a study carried out by Deloitte Consulting in 2014 found that the use of username and password is completely broken because more than 90% of them can be forced and decrypted in just a few hours; multi-factor authentication is recommended, which involves the use of 2 of these elements:

1. Something you know: Like passwords and security questions.
2. Something you have: Like tokens, temporary access codes, and credit cards.
3. Something you are: Like biometrics.

Another study conducted by HP in 2014 found that 70% of data shared over a network does not have any encryption, which means that anyone can access it. Additionally, Microsoft and Apple operating systems have built-in hard drive encryption tools; However, not many consumers are aware of its use or existence. Smartphones, Google, and Apple include encryption of ongoing messages, preventing all communication from being read by criminals.

Cybersecurity education is vitally important; since it allows users to recognize and avoid cyber threats such as phishing, malware, and identity theft, although these threats are highly evolved, they always require the computer user to naively open the message and perform the actions requested by the cybercriminal [9]. Additionally, it encourages secure online habits, such as using strong and unique passwords, regularly updating software, and protecting devices from intrusions; promotes responsibility and protection of personal and confidential information; An informed public contributes to the protection of digital infrastructure and the prevention of

cyberattacks that could cause financial, personal, and even national damage [3].

According to the above, the objective of the systematic review is to know the cybersecurity policies and programs that the States have implemented, as well as the knowledge about cybersecurity that the population has.

II. Methodology

The study responds to a systematic literature review (SRL); considering that in 2020 the IDB and OAS report [10] on advances in cybersecurity will be issued; The search was carried out for the articles published and indexed in the Scopus database during the years 2020 to 2022. Likewise, the terms "education" OR "politics" OR "knowledge" AND "cybersecurity" were established as search criteria.". The inclusion criterion was that the articles be open access and articles about medicine were excluded; A total of 573 articles were obtained, of which, applying the selection process in the graph shown, a total of 50 articles suitable for analysis in the present investigation were obtained; (see figure 1), regarding the paper by Hong et al. It was published in 2022, and it emerged on the date of the search for the articles that are part of the study; However, he was assigned to a magazine in January 2023; Therefore, the publication year of January 2023 is being maintained.

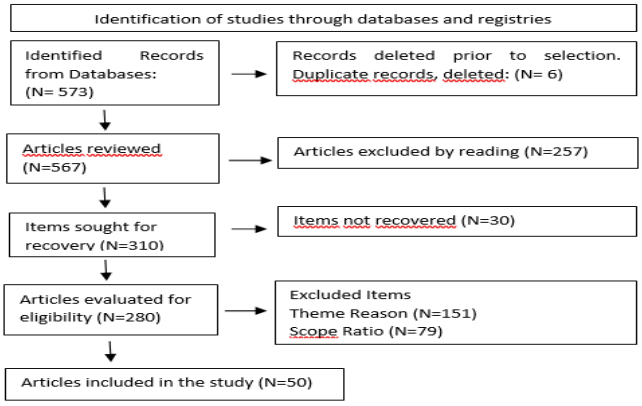

Fig. 1. Flowchart for the systematic literature review adapted from Page et al [11].

III. Results

Figure 2 shows the number of articles analyzed by country of origin; European countries, especially in the United Kingdom, publish with greater emphasis articles related to knowledge and implementation policies on cybersecurity.

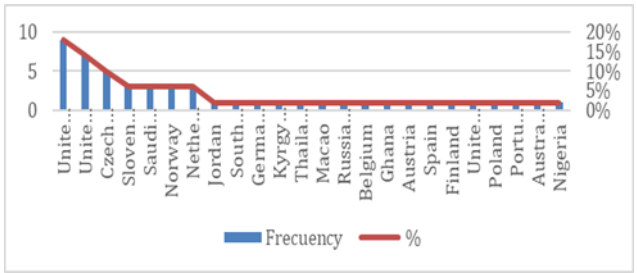

Fig. 2. Number of articles analyzed by country of origin.

50 articles were analyzed, with SCOPUS being the database where the largest number were found in 2022 with 23 publications; in 2021, 17 publications; in 2020, 9 publications and in 2023, 1 publication.

A. Policies applied to cybersecurity implementation.

Research articles were found on viable cybersecurity policies, eight belonging to Europe and one from the Arab States Region.

Of the nine articles reviewed, three correspond to the United Kingdom, among their proposals is: an adaptive governance model that is based on "planned adaptive regulation", the development of cyber capabilities in international debates to support the countries of the South in promoting technical and policy strategies on cybersecurity and the practice of integrating peer review as part of a cybersecurity policy evaluation task to support assessment literacy in computer science and software engineering graduates [12], [13], [14]. Two from Norway, in which they propose the creation of policies that contain cyber capabilities (CCB), as part of global policy and ten common aspects in the policies of five companies (health, finance, education, aviation, and electronic commerce) [15], [16]. The Russian Federation has an article, which seeks to define the concept of "digital sovereignty", to find effective mechanisms to guarantee sovereignty in the digital space without prejudice to the digital revolution [17]. Poland also has a publication that emphasizes three points "The entities of the national cybersecurity system" "the obligations of operators of essential services" and "the authorities responsible for cybersecurity" [18]. An article from Germany introduces legal aspects of cybersecurity in the financial sector, taking stock of existing cybersecurity schemes. Establishes key elements for the regulation of cybersecurity in the financial sector of the European Union [19]. Finally, an article from the United Arab Emirates addresses the review of National Strategic Cybersecurity Plans and presents a proposal to adopt the Goal-Question- Outcomes (GQO)+ Strategies paradigm based on the development of infrastructure, digital services and technology, defense against cyber threats and enriching people's knowledge of it [20].

TABLE I. Policies applied to cybersecurity implementation y Training Programs

N	Author(s)	Types of policies
1	Willers.	Creation of global policies that contain the strengthening of cyber capabilities (CCB), as part of global policy.
2	Rebro et al.	Defining political sovereignty and national independence through "digital leadership"
3	Brass and Sowell	Centralized risk regulatory frameworks with operational knowledge and mitigation mechanisms
4	Karpiuk	The national cybersecurity system aims to ensure cybersecurity at the national level, which involves the uninterrupted provision of essential and digital services
5	Calderaro et.al.	General Cyber Agreement: seeks to strengthen resilience to cyber threats through national cybersecurity strategies, incident response teams

		(CSIRTs), cybercrime laws, public-private collaboration, and education to raise public awareness
6	Mishra et al	Corporate Cybersecurity Policies.
7	Maguire and English	Cyber Security Literacy
8	Calliess and Baumgarten	Cybersecurity in the EU, the example of the finance sector
9	AlDaajeh et al.	It reviews a set of world-leading National Cybersecurity Strategic Plans and discusses existing associated cybersecurity education and training improvement initiatives.

B. Training programs

Of the articles found, 15 of them focus on cybersecurity training programs, which would respond to the capacity development criteria used by the Global Cybersecurity Agenda [21]. The countries included in the Global Cybersecurity Index (since its appearance in 2014) have developed different strategies, with the European continent taking the lead with eight articles found in the United Kingdom where the challenge of teaching Cybersecurity to students is developed. general computer science students at a university in the same country [22]; In articles from the United Kingdom, Slovenia, the Czech Republic, and Portugal, the contribution of programs towards the European Union with an integration model, a skills center to educate about cybersecurity, and the SPARTA CSF program for implementation, education, and training are proposed. cybersecurity study programs; as well as a diagnostic strategy for evaluating risk attitudes and behaviors and cyber awareness, respectively [23], [24], [25], [26].

North America, has three articles from the United States, in which four modules are developed (application security, web security, firewall configurations, wireless network security) that support the development of cyber skills for undergraduate students and postgraduates, in 2021; a review of digital forensics programs in universities, and a design for the undergraduate course in software and web security using active learning strategies in the cybersecurity course developed at York College of the City University of New York (CUNY); all of them fulfilling the characteristic of teaching about critical topics in cybersecurity [27], [28], [29].

In Africa, two articles were found, one carried out a systematic review on the use of artificial intelligence to combat cybercrimes, and the second proposed a cybersecurity curriculum from a perspective of best practices for universities and other educational institutions top [30], [31] .

From the Arab states, two articles were found that measure the knowledge of university students after the placement of a module that teaches three essential topics, relating to password security, and browser security, and the second validates the cybersecurity knowledge, skills, and abilities (KSA) competencies of cybersecurity degree programs using a fuzzy language group decision-making method [32], [33].

TABLE II. CYBERSECURITY TRAINING PROGRAMS

N	Author(s)	Training Programs	Programs Implemented
1	Alqahtani	Informative module to assess the cybersecurity awareness of university students in password, browser, and social media security.	Cybersecurity Assessment and Knowledge Module for Students
2	Srivatanakul y Annansingh	Cybersecurity course designed at York College, CUNY.	Cyber Security Course
3	Dočkalová Burská et al.	Tool to analyze learning in a practical session, compare students, and identify flaws in assigned puzzles [34].	Training Analysis Tool
4	Ben Salamah et al.	Educate about cybersecurity challenges in social media. Analyze the feasibility of an adaptive training and awareness-raising system, gathering information from various sectors.	Adaptive Cybersecurity Training and Awareness System [35].
5	Kuzminykh et al.	Model for integrating EU cybersecurity frameworks into Ukrainian education, promoting European good practices in the business sector, legal regulators, governmental, scientific, and educational institutions.	Model for the continuous integration of EU cybersecurity frameworks into Ukraine's education process
6	Antunes et al	Triple strategy of cybersecurity and cyber awareness for basic education students, which includes evaluation of risk attitudes and behaviors.	Diagnostic strategy for the assessment of risk attitudes and behaviors and cyber awareness
7	Jerman	Accreditation of cybersecurity programs and certifications in European institutes. Improvement actions and proposal of the educational panorama.	Competence centers to create an integrated and user-centric cybersecurity ecosystem in the EU, seeking European digital sovereignty.
8	Da Veiga et al.	Proposed curriculum with core modules in Networking, Cryptography, Cybersecurity, Forensics and Programming, based on current best practices.	Networking, Cryptography, Cybersecurity, Forensics & Programming
9	Hajny et al	Shortage of cybersecurity bachelor's degree programs (19 out of 89). Need to increase cybersecurity subjects from the first year.	SPARTA CSF, to reflect new trends and directions in cyber security
10	Crick et al	Teaching Cybersecurity to computer science students at a university in the United Kingdom, with a two-year computer science foundation before specializing.	External Network Policies (JANET). Binary Programming
11	Wang et al	Learning basic and advanced skills through well-designed modules and hands-on cybersecurity labs.	Application, web, firewall and wireless network configuration.
12	Alammari et al	Validate cybersecurity KSA in degree programs using fuzzy linguistic group decision method.	Fuzzy Language Group Decision-Making Method
13	Mendivil et al [36]	The ability to deal with cybersecurity issues depends on staff training and awareness, and a framework that identifies the indicators needed for each position.	Competency-based model for training and sensitizing non-ICT staff according to their job profile.
14	McCullough et al	U.S. universities offer digital forensics courses on ethics, cyber law, investigation, and forensic lab. The least offered are memory forensics, IoT, and software.	An Exploratory Analysis of Digital Forensics Programs in the United States

15	Wiafe et al	Artificial intelligence is proposed to develop more robust cybersecurity methods that make real-time decisions and respond effectively to sophisticated attacks, thus combating cybercrime.	Methods to ensure cybersecurity (CyberSec) with Artificial Intelligence

C. Sources of knowledge, topics, and vulnerable population

Of 26 articles, fifteen of them correspond to Europe and address studies on how senior managers can establish a global cybersecurity model, concluding that the global cybersecurity model (GCS) helps managers visualize, establish, and manage cybersecurity strategies. risk mitigation; the knowledge of young people about cybersecurity, concluding that schoolchildren between 12 and 14 years old were interested in the technical topic of cybersecurity in which different attacks are described; survey applied to 106 legal professionals from 19 countries that explore four thematic areas referring to human capital, social capital, knowledge and technology transfer, present evidence that threats to cybersecurity, inadequate and limited IT training, Excessive paperwork and lack of efficient teamwork, collaboration, and communication are key challenges to innovation adoption; in the United Kingdom, three articles were found, Trim and Lee [37]; Nicholson et al [38]; Michalakopoulou et al [39].

In the Netherlands, three articles, the first by Van Steen et al [40], analyzed 17 cybersecurity awareness campaigns to measure their effectiveness; Barth et al [41]interviewed 20 privacy and cybersecurity experts about their views on online privacy concerning mobile applications; despite the technical knowledge they resembled that of non-professional users; Witsenboer et al [42], explores the extent to which Dutch students develop cyber-safe behavior in primary and secondary school, this being scarce and recommending its implementation as soon as the student has contact with an online computer.

In the Czech Republic, three articles were found, Svabensky et al[43] through a systematic review of the literature of the main conferences in computing education, found technical topics about programming, teaching approaches, and the impact on communities; only 31% of these provide a replicable result for other educators and researchers; Švábenský, et al[44]propose shell -based graphical models to visually evaluate the progress of university students, concluding on the effectiveness of these models during classes; Švábenský and Vykopal et al[45] studies a data set of 18 cybersecurity training sessions, revealing their typical behavior, errors, solution strategies, and difficult training stages; concluding that these are adequate means for students to find solution approaches and grouping them according to their behavioral patterns.

In Slovenia, two articles were found in Jerman and Jerman [26] elaborate analysis of the state of cybersecurity skills and knowledge in European secondary school students, establishing the most important topics that should be introduced in the educational program; Jerman [46] identified that the answers to the cybersecurity skills gap can be found in the enrichment of HEI study plans with new content from less covered areas of knowledge, such as the organizational or human aspects of cybersecurity, and with better use of cybersecurity.

In Finland, Kyytsönen et al [47] describe the self-assessed information security skills of the Finnish population and the factors associated with it, concluding that the population shows a positive association between Internet skills and information security skills. information, people between 20 and 54 years old felt more confident about their abilities compared to people over 54 years old.

In Norway, Bromander et al [48], found that although sharing information on threat intelligence is crucial, classification and trust, unclear use of terminology, and great flexibility within STIX hinder development in the field of CTI.

In Belgium, De Kimpe et al [49], include perceived knowledge and trust on the Internet, concluding that the tendency of Internet users is often too optimistic, which could cause them to be vulnerable online.

In Austria, Klimburg-Witjes and Wentland [50] concludes that responsibility for cybersecurity is individualized through three different lines of argument, "the outsider employee," "code and social speaking," and "correcting human failures."

In Asia, five articles were found, by Jordan, Khader et al [51] propose a Cybersecurity Awareness Framework for Academia (CAFA), concluding that the CAFA presented in this work can serve as a starting point for academic institutions to establish new policies and procedures or modify existing ones. In Saudi Arabia, Alharbi and Tassaddiq [52]investigated and evaluated the level of cybersecurity awareness and user compliance among university students at Majmaah University using a scientific questionnaire based on several factors; They recommended that said university should promote the most common cybersecurity factors such as vulnerabilities and attacks and incidents to its students, as well as training and awareness programs. In Kyrgyzstan, Erendor and Yildirim [53],present the extent to which students at the Kyrgyz-Turkish University of Manas know about cybersecurity in the distance education process, finding that most students did not have sufficient knowledge about Internet use and cyber threats. In Thailand, Daengsi et al [53], focused on the cybersecurity awareness of approximately 20,000 employees nationwide at a large financial institution in Thai territory through phishing attacks, finding that the cybersecurity awareness of Thai employees of this organization It was “very good” security for Internet use. In Macau, Hong et al [54], proposed an extended knowledge-attitude-behavior (KAB) model, which postulates that the influence of the educational level of society, in general, is a moderator of the relationship between knowledge and attitude, finding that The study is one of the first attempts to compare active college students and graduates to examine the cognitive and behavioral changes of well-educated people; contributing to the methodology, theorization, and practice of the aforementioned model.

In America, four articles were found, all of them from the United States, Sleeman et al [55], showed how to apply dynamic topic models to a set of cybersecurity documents to understand how the concepts found in them change extracted from Wikipedia, finding that the proposed approach uses an ontology to extract phrases that can improve readability about topics in cybersecurity. Sample et al [56] examine two higher education institutions with programs that offer interdisciplinary courses

that can more effectively address threat analysis and IoT in both programs have maintained the traditional cybersecurity courses that can be found in most universities, and both noted the need for fundamental skills. Jawad and Tout [57], this article suggests gamifying computer science subjects to improve the learning experience of Generation Z through classes, finding that the students who attended responded positively to this type of learning through games. Lasisi et al [58] , investigate the AI courses and/or topics needed to improve cybersecurity education to prepare future AI-enabled cybersecurity leaders.

In Africa, an article was found where Garba et al [59] identified the level of awareness about the cybersecurity of students in the northeast of Nigeria, finding that the students surveyed have shown a high level of awareness about cybersecurity in some elements, including Internet banking, while other elements such as cyber bullying, self-protection, and Internet addiction are moderate.

In Oceania, an article was found from Australia where Akter et al [60], the study results show that personnel (knowledge, attitude, and learning), management (training, culture, and strategic orientation), and infrastructure capabilities (technology and data governance) are thematic dimensions to address cybersecurity awareness challenges.

TABLE III. SOURCES OF KNOWLEDGE, ISSUES AND VULNERABLE POPULATION

N	Author(s)	Source of knowledge	Topics	Population
1	Witsenboer et al	Internet	Cybersecurity	Basic Education Students
2	Kyytsönen et al	Surveys		Healthcare Users
3	Daengsi et al	There are no sources on knowledge in CS		Population
4	Jerman and Jerman		Cybersecurity Skills	Basic Education Students
5	Jerman	There are no sources on knowledge in CS	Cybersecurity	Population
6	Barth et al		Privacy & Online Behaviors	
7	Bromander et al		Evidence-based knowledge	
8	Garba et al	Courses & Seminars	There is a lack of protocols to detect and manage online risks when they occur.	Basic Education Students
9	Michalakopoulou et al		Roles of human-social capital and transfer of knowledge and technology.	Industry
10	Hong et al	Practical/Work Experiences	Social Education in Cybersecurity Awareness and Behavior	College Students
11	Lasisi et al	Practical/Work Experiences	Frontier in AI-enabled cybersecurity education and resources	Academic Community
12	Erendor y Yildirim	Practical/Work Experiences	Cybersecurity Awareness Online Education	Basic Education Students
13	De Kimpe et al	Internet	Perceived Knowledge, Internet Trust, and Protection	Population
14	Jawad y Tout	Courses and Seminars	Gamification in the teaching of computer science topics	Academic Community
15	Nicholson et al	Practical/Work Experiences	Young people's experiences in cybersecurity	Basic Education Students
16	Trim y Lee	Practical/Work Experiences	Global cybersecurity model based on the resilient partnership agreement	Population
17	Alharbi y Tassaddiq	Courses and Seminars	Cybersecurity Awareness Assessment	College Students
18	van Steen et al		Code intervention materials according to the Behavior Change Wheel and the Taxonomy of Behavior Change Techniques.	Population
19	Sample et al	Courses and Seminars	Relationship between basic cyber hygiene, cybersecurity, and data science to integrate disciplines.	Adult population and non-traditional learners
20	Švábenský et al	Courses and Seminars	Cyber Security Using Data Mining and Machine Learning Techniques	Population
21	Švábenský, Weiss, et al	Courses and Seminars	Evaluation of the teaching-learning process on cybersecurity	Instructors
22	Klimburg-Witjes & Wentland	Courses and Seminars	Basic knowledge of Cybersecurity	Public and private employees
23	Khader et al	Courses and Seminars	Cyber Security in the University Curriculum	College Students
24	Akter et al		Cybersecurity in the Data-Driven Digital Economy	Population
25	Sleeman et al		Cybersecurity Threats	Academic Community
26	Svabensky et al	Courses and Seminars	Educación en ciberseguridad	Academic Community

IV. DISCUSSION

The presented analysis highlights the importance of evaluating countries' progress in cybersecurity, as well as the level of awareness about this issue among the population. By examining the implemented policies and programs, a variety of approaches and measures adopted by different nations to address cyber threats are observed.

A. Cybersecurity policies and programs

They were identified, which underlie the results in this study, legal measures, and organizational measures, each analyzed about the detected countries.

Countries like the United Kingdom demonstrate significant commitment to creating and continuously improving cybersecurity policies, emphasizing their leadership in legal and organizational aspects. This strong legal and structural foundation contributes to a trusted cyberspace environment and enables an effective response to international cybersecurity recommendations. So, there is a cyberspace of trust since it responds to the recommendations made by the BDT

Management Consultative Group and the Budapest Convention [61].

On the other hand, countries like Norway and the United Arab Emirates are showing similar commitments to cybersecurity, albeit with slightly different focuses. While Norway is focused on implementing basic cybersecurity capabilities and analyzing sectoral policies, the United Arab Emirates prioritizes legal measures and shows great potential for growth in organizational measures.

The Russian Federation occupies the Top 5 in the ICG global classification and 1st place in the classification of the countries that make up the CIS region, obtaining 20 in terms of legal measures and 18.98 in organizational measures, being its highest score. low among the five pillars, which is reflected in the results of this systematic review.

Poland is in 30th place in the global classification of the IGC, and in 18th place in the Europe region with a score of 19.35 on legal measures and 14.74 on organizational measures, this pillar being its lowest score.; However, the country is making progress concerning the pillar of organizational measures.

Germany is in 13th place in the global classification, and in 7th place in the European regional classification, with a score of 20 in legal measures and 18.98 in organizational measures. In this regard, the article responds to both pillars since They intend to introduce legal aspects to the financial sector.

The United Arab Emirates is in the Top 5 of the ICG, and in second place in the regional classification of the Arab States with a maximum score of 20 in legal measures and 18.98 in organizational measures, being an area of possible growth. In this regard, the article found responds to an international search for the best cybersecurity plans for education and knowledge in the year 2022.

B. Training programs

Regarding training programs, it is encouraging to see how countries like the United Kingdom, Spain, and Saudi Arabia are investing in educating their populations about cybersecurity. These ongoing efforts reflect an understanding of the importance of training and awareness in combating cyber threats.

The United Kingdom is in a constant search to create cybersecurity programs for its university students, with three articles in chronological order from 2020, 2021 and 2022, either with courses for university students, as well as training modules, that agree with the 2020 Global Cybersecurity Index (IGC) since in this criterion it was determined that Northern Ireland and the United Kingdom, for the year 2020, obtained the highest classification in this area (according to our study, since 2020, no articles on this particular topic by Northern Ireland); However, the United Kingdom is the number one country on the European continent, and the second according to the international classification of the 2020 Global Cybersecurity Index, which is constantly working to ensure that its nation fights against network vulnerabilities.

Spain appears in the Top three in the IGC, and in fourth place internationally, with a maximum score of 20 for the capacity development pillar, the article dated 2022 would respond to the continuity in its efforts to teach its population about cybersecurity.

Of the Arab States, Saudi Arabia tops the list, finding itself in the number one position in its region and the Top two in the global ranking of the IGC, about the two articles found in the year 2022, would affirm its continuous work in the time regarding this pillar since the classification obtained was 20, considered an area of relative strength.

Portugal is ranked 8th in the European regional classification, but, after the evaluation of compliance with the five pillars, it obtained the lowest grade regarding capacity development with 18.34, being an area of possible growth, note that it could improve since the article found is from 2021.

Slovenia appears in 34th place in the regional classification of Europe, regarding capacity development it obtained a grade of 17.50, a grade that could improve in the next edition of the IGC, since the two articles found are dated 2021 and 2022 the same would happen. with the Czech Republic being in 35th place in the regional classification of Europe, consequently, the grade obtained in this pillar, being the lowest in its evaluation, obtained a 9.14 according to IGC. The two articles found are dated from 2021 and 2022.

In America, the United States is the only one that is among the results with three articles from the years 2020, 2021, and 2022, ranking in the Top one in the regional and world classification of the IGC, obtaining a perfect score in all the pillars analyzed.

In Africa, Ghana is in the Top 3 of the IGC classification, in the present search an article from 2020 was found. However, the score obtained is 15.44, the lowest compared to the other pillars, it is important to highlight the need to continue moving forward over time. South Africa appears in eighth place in the ICG classification, but they did not respond to the questionnaire sent by the IUT, so the data was obtained by an ICG team, consequently, it is not possible to affirm that the information on the international standards described. they obtained a grade of 15.37; Only one article was found for this country from the year 2021.

C. Sources of knowledge, topics, and vulnerable Populations in cybersecurity policies

Of the pillars established by the IGC, in relation to technical and cooperation measures, it has been found that Europe has very good results for the protection of children online, since 89% of countries apply laws related to this point, Of the 26 articles found, 15 are European, three of them belong to the Top 2 of the General Index in Cybersecurity, United Kingdom, where the two pillars can be located, using workshops for the protection of online children as well as the establishment of national programs and national strategies in cybersecurity.

The Netherlands appears in 16th place in the global classification of the IGC, however, this country was not able to respond to the survey sent, which could have changed its position in the table, since it has three articles in this review that reflect the pillars corresponding technicians and cooperatives in the development of cybersecurity measures in their country. Czech Republic, also with three articles, related to cybersecurity

awareness, one of them was concerned with analyzing campaigns, another with measuring what experts say and the last one with knowing what students know, each one collaborated in reinforce the two aforementioned pillars, according to the global classification of this country in the ICG it is in position 68 and the European region 35, being one of the mentioned articles from the year 2020, and two from 2022, it can be said that they have been working to improve their situation concerning the technical and cooperative pillars, which would have favorable consequences in their future position in the next Global Cybersecurity Index. In Slovenia, the aim is also to find out from the aforementioned pillars whether the programs used in their country are useful when verifying what European students have learned, whether in secondary school or other educational establishments, therefore, in the global score made by each pillar the technical measures they obtained was the lowest score with 11.38 and 12.11 in cooperative measures, over the other pillars evaluated, which would make sense with the publications found in the year 2022, seeking a positively different classification for the next evaluation. Finland, which is in 22nd place in the ICG global ranking, and 14th in the regional ranking, is concerned about the population's knowledge of their Internet and computer skills and must worry a little more about establishing organizational measures., such as security agencies, therefore, is an area of possible growth having obtained a low score of 14.33. In Norway, much emphasis is placed on the technical means that must intervene so that cybersecurity in their country can develop, since the article uses a model that, through a structure, for the benefit of computer science professions.

Belgium occupies 19th place in the global cybersecurity ranking and 12th in the European region. The article found the response to the user's knowledge of the Internet, which would keep the capacity development pillar relevant. However, the highest score for this country is in the organizational measures, with 16.25, although no articles have been found that raise this pillar, we trust that they have planned to continue working on this for the next Global Cybersecurity index [61].

Austria occupies 29th place in the GCI, and 17th in the regional classification, with a low score regarding the pillar of cooperative measures at 17.70; The article found responses to discursive frameworks that can contribute to the rhetoric of cybersecurity.

Jordan is ranked 71st in the global cybersecurity ranking and 10th in the regional classification of Arab states, with its lowest score in technical measures at 10.74 points; The article seeks (like Austria) a legal framework for cybersecurity (specifically for its awareness) responding to the pillar of legal measures, but not, about technical measures.

Saudi Arabia obtained its only low score in the pillar of technical measures with 19.54. In this regard, the article investigates and evaluates what tools are scarce among university students to start improving in cybersecurity.

Kyrgyzstan is ranked 92nd in the IGC global ranking, and 7th in the CIS region; The article responds to the need to know the level of capacity development (in which it obtained a score of 1.87) of university education in said country, unfortunately, this would only be an answer about the other four pillars in which this The country has not correctly developed measures to contribute to cybersecurity, since, out of 100 as the maximum score, its score is 49.64.

Thailand is ranked 44th in the IGC global ranking, and 9th in the Asia-Pacific regional ranking; The article responds to the same thing as indicated by its peers, knowing the degree of awareness in cybersecurity, by the development of capabilities of its country and the pillars under analysis, however, the low mark was obtained in the pillar of technical measures.

The United States is number one in the global and regional classification of the ICG, so it is expected to find four articles that simultaneously respond to the five pillars previously stated, even in chronological years, from 2020 to 2022., having in common the application of thematic models to learn about cybersecurity, as well as the study of programs, subjects, and courses on the same topic.

Nigeria is in 47th place in the ICG global classification and 4th place in the regional results for African countries. The article responds precisely to the pillar in which they obtained a low score of 12.21, capacity development.

Australia is ranked 12th in the ICG global ranking, and 5th in the Asia-Pacific regional ranking; The identified article seeks to learn about the types of cybersecurity awareness, thus reinforcing the capacity development pillar in which they obtained a score of 20; However, it has been an opportunity for improvement in the organizational measures with a score of 18.98.

D. Final aspects of the discussion

There are many significant articles regarding America (United States) and Europe (United Kingdom), in which previous national plans are developed regarding infrastructure, programs, participation, and minimum standards for cybersecurity. For its part, the Inter-American Development Bank (2020)[10] issued the report Cybersecurity 2020 [61]: risks, advances, and the way forward in Latin America and the Caribbean, in which they developed the Cybersecurity Capacity Maturity Model for Nations (CMM, for its acronym in English); defining five dimensions such as (i) cybersecurity policies and strategies, (ii) Cyberculture and society, (iii) Cybersecurity education, training, and skills, (iv) legal and regulatory frameworks and (v) standards, organizations and technologies. They even attach a report for each country, which identifies the progress of the proposed indicators, until 2020. Unfortunately, in this review, no article on the object of study has been identified, that would even respond to the indicated report itself, well, The work carried out by the countries that make up Latin America and the Caribbean is low, and although it is recognized that some of these already have national cybersecurity strategies, research results in this regard have not yet been published, despite that the report has existed since 2020.

V. CONCLUSIONS

Cybersecurity has emerged as a global concern that transcends the development status of countries, with national authorities worldwide recognizing its significance. Efforts to assess the level of cybersecurity knowledge among populations indicate a shared commitment to capacity development. However, cyberattacks persist as a threat beyond individual

users' protection skills, prompting intensive research on cybersecurity policies, particularly in countries like the United Kingdom and the United States

Various sources of knowledge, including courses, seminars, Internet access, and work experiences, address essential topics such as cybersecurity skills, privacy, and online behavior. Nevertheless, the scarcity of technical measures, as reflected in low scores on the Global Cybersecurity Index, highlights the need for further investigation into countries with unfavorable rankings.

While vulnerable populations, such as basic education students, require attention, the lack of training programs tailored to this demographic underscores an area for future exploration. Establishing global policies and regulatory frameworks for centralized cybersecurity risk management is crucial to mitigate cyber threats. This includes comprehensive training programs encompassing students, professionals, and the public, offering modules that equip them with the knowledge and skills to identify and respond to potential threats.

The cooperation of 193 surveyed countries has been instrumental in advancing cybersecurity efforts, yet greater initiative is expected, particularly from Latin American nations, where a lack of publications on cybersecurity themes and pillars was observed despite their inclusion in the Global Cybersecurity Index.

In summary, while significant progress is observed in the implementation of cybersecurity policies and programs worldwide, there are still challenges to overcome and areas where additional improvements can be made. The analysis provides valuable insight into the current state of cybersecurity at the international level and underscores the importance of continued work in this critical area to ensure data protection and online security for all.

REFERENCES

[1] Organization of American States, "Cybersecurity Education Future Planning through Workforce Development," 2020. Accessed: Aug. 24, 2023. [Online]. Available: https://www.oas.org/es/sms/cicte/docs/White-Paper-Cybersecurity-Education.pdf

[2] Interpol, "Cybercrime," Interpol. Accessed: May 12, 2023. [Online]. Available: https://www.interpol.int/es/Delitos/Ciberdelincuencia

[3] M. Goodman, *Future Crimes: How Our Radical Dependence on Technology Threatens Us All*. Canada: Penguin Random House, 2015. Accessed: Apr. 30, 2024. [Online]. Available: https://www.abebooks.com/Future-Crimes-Radical-Dependence-Technology-Threatens/31472462095/bd

[4] I. Álvarez, "Constitución y Derecho del Ciberespacio," in *Nuevos Retos de la Ciberseguridad en un Contexto Cambiante*, España: Aranzadi, 2019, pp. 21–46.

[5] Conal Iker, *Ciberseguridad y Derecho penal*, 1st ed. España: Aranzadi, 2022.

[6] Tejerina Ofelia, "Ciberataques enjambre, responsabilidad sincronizada," in *Nuevos retos de la ciberseguridad en un Contexto Cambiante*, España: Aranzadi, 2019, pp. 163–179.

[7] Organization of American States, "NIST, Cybersecurity, Framework," Organization of American States. Accessed: Aug. 24, 2023. [Online]. Available: https://www.oas.org/es/ssm/publications.asp?IE=00T78

[8] García Yolanda, "España era séptima en el Índice Global de Ciberseguridad en 2018," Newtral. Accessed: May 01, 2024. [Online]. Available: https://www.newtral.es/indice-global-ciberseguridad-espana/20220530/

[9] Y. B. Riega Viru, M. E. Ninaquispe Soto, and J. L. Salas Riega, "Cybercrime: A systematic review of the literature," in *Proceedings of the 20th LACCEI International Multi-Conference for Engineering, Education and Technology: "Education, Research and Leadership in Post-pandemic Engineering: Resilient, Inclusive and Sustainable Actions,"* Latin American and Caribbean Consortium of Engineering Institutions, 2022. doi: 10.18687/LACCEI2022.1.1.576.

[10] Inter-American Development Bank and Organization of American State, "Reporte Ciberseguridad 2020: riesgos, avances y el camino a seguir en América Latina y el Caribe," Inter-American Development Bank, Washington, Jul. 2020. doi: 10.18235/0002513.

[11] M. J. Page *et al.*, "The PRISMA 2020 statement: an updated guideline for reporting systematic reviews," *BMJ*, p. n71, Mar. 2021, doi: 10.1136/bmj.n71.

[12] J. Maguire and R. English, "Opportunities to Fail: Using Peer-review to support Assessment Literacy in Cyber Security," in *Proceedings of the 21st Koli Calling International Conference on Computing Education Research*, New York, NY, USA: ACM, Nov. 2021, pp. 1–2. doi: 10.1145/3488042.3489967.

[13] A. Calderaro and A. J. S. Craig, "Transnational governance of cybersecurity: policy challenges and global inequalities in cyber capacity building," *Third World Q*, vol. 41, no. 6, pp. 917–938, Jun. 2020, doi: 10.1080/01436597.2020.1729729.

[14] I. Brass and J. H. Sowell, "Adaptive governance for the Internet of Things: Coping with emerging security risks," *Regul Gov*, vol. 15, no. 4, pp. 1092–1110, Oct. 2021, doi: 10.1111/rego.12343.

[15] J. O. Willers, "Seeding the cloud: Consultancy services in the nascent field of cyber capacity building," *Public Adm*, vol. 100, no. 3, pp. 538–553, Sep. 2022, doi: 10.1111/padm.12773.

[16] A. Mishra, Y. I. Alzoubi, A. Q. Gill, and M. J. Anwar, "Cybersecurity Enterprises Policies: A Comparative Study," *Sensors*, vol. 22, no. 2, p. 538, Jan. 2022, doi: 10.3390/s22020538.

[17] O. Rebro, A. Gladysheva, M. Suchkov, and A. Sushentsov, "The Notion of 'Digital Sovereignty' in Modern World Politics," *International Trends / Mezhdunarodnye protsessy*, vol. 19, no. 4, pp. 47–67, 2021, doi: 10.17994/IT.2021.19.4.67.6.

[18] M. Karpiuk, "Organisation of the National System of Cybersecurity: Selected Issues," *Studia Iuridica Lublinensia*, vol. 30, no. 2, p. 233, Jun. 2021, doi: 10.17951/sil.2021.30.2.233-244.

[19] C. Calliess and A. Baumgarten, "Cybersecurity in the EU The Example of the Financial Sector: A Legal Perspective," *German Law Journal*, vol. 21, no. 6, pp. 1149–1179, Sep. 2020, doi: 10.1017/glj.2020.67.

[20] S. AlDaajeh, H. Saleous, S. Alrabaee, E. Barka, F. Breitinger, and K.-K. Raymond Choo, "The role of national cybersecurity strategies on the improvement of cybersecurity education," *Comput Secur*, vol. 119, p. 102754, Aug. 2022, doi: 10.1016/j.cose.2022.102754.

[21] International Telecommunication Union, "Global Cybersecurity Agenda (GCA)," International Telecommunication Union. Accessed: Aug. 25, 2023. [Online]. Available: https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx

[22] T. Crick, J. H. Davenport, P. Hanna, A. Irons, and T. Prickett, "Overcoming the Challenges of Teaching Cybersecurity in UK Computer Science Degree Programmes," in *2020 IEEE Frontiers in Education Conference (FIE)*, IEEE, Oct. 2020, pp. 1–9. doi: 10.1109/FIE44824.2020.9274033.

[23] I. Ievgeniia Kuzminykh, M. Yevdokymenko, O. Yeremenko, and O. Lemeshko, "Increasing Teacher Competence in Cybersecurity Using the EU Security Frameworks," *International Journal of Modern Education and Computer Science*, vol. 13, no. 6, pp. 60–68, Dec. 2021, doi: 10.5815/ijmecs.2021.06.06.

[24] J. Hajny, S. Ricci, E. Piesarskas, O. Levillain, L. Galletta, and R. De Nicola, "Framework, Tools and Good Practices for Cybersecurity Curricula," *IEEE Access*, vol. 9, pp. 94723–94747, 2021, doi: 10.1109/ACCESS.2021.3093952.

[25] M. Antunes, C. Silva, and F. Marques, "An Integrated Cybernetic Awareness Strategy to Assess Cybersecurity Attitudes and Behaviours in School Context," *Applied Sciences*, vol. 11, no. 23, p. 11269, Nov. 2021, doi: 10.3390/app112311269.

[26] B. Jerman Blažič and A. Jerman Blažič, "Cybersecurity Skills among European High-School Students: A New Approach in the Design of Sustainable Educational Development in Cybersecurity," *Sustainability*, vol. 14, no. 8, p. 4763, Apr. 2022, doi: 10.3390/su14084763.

[27] T. Srivatanakul and F. Annansingh, "Incorporating active learning activities to the design and development of an undergraduate software and

web security course," *Journal of Computers in Education*, vol. 9, no. 1, pp. 25–50, Mar. 2022, doi: 10.1007/s40692-021-00194-9.

[28] S. McCullough, S. Abudu, E. Onwubuariri, and I. Baggili, "Another brick in the wall: An exploratory analysis of digital forensics programs in the United States," *Forensic Science International: Digital Investigation*, vol. 37, p. 301187, Jul. 2021, doi: 10.1016/j.fsidi.2021.301187.

[29] L. Wang, J. Yang, and P.-J. Wan, "Educational modules and research surveys on critical cybersecurity topics," *Int J Distrib Sens Netw*, vol. 16, no. 9, p. 155014772095467, Sep. 2020, doi: 10.1177/1550147720954678.

[30] A. da Veiga *et al.*, "A Reference Point for Designing a Cybersecurity Curriculum for Universities," 2021, pp. 46–62. doi: 10.1007/978-3-030-81111-2_5.

[31] I. Wiafe, F. N. Koranteng, E. N. Obeng, N. Assyne, A. Wiafe, and S. R. Gulliver, "Artificial Intelligence for Cybersecurity: A Systematic Mapping of Literature," *IEEE Access*, vol. 8, pp. 146598–146612, 2020, doi: 10.1109/ACCESS.2020.3013145.

[32] A. Alammari, O. Sohaib, and S. Younes, "Developing and evaluating cybersecurity competencies for students in computing programs," *PeerJ Comput Sci*, vol. 8, p. e827, Jan. 2022, doi: 10.7717/peerj-cs.827.

[33] M. A. Alqahtani, "Factors Affecting Cybersecurity Awareness among University Students," *Applied Sciences*, vol. 12, no. 5, p. 2589, Mar. 2022, doi: 10.3390/app12052589.

[34] K. Dočkalová Burská, V. Rusňák, and R. Ošlejšek, "Data-driven insight into the puzzle-based cybersecurity training," *Comput Graph*, vol. 102, pp. 441–451, Feb. 2022, doi: 10.1016/j.cag.2021.09.011.

[35] F. Ben Salamah, M. A. Palomino, M. Papadaki, and S. Furnell, "The Importance of the Job Role in Social Media Cybersecurity Training," in *2022 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, IEEE, Jun. 2022, pp. 454–462. doi: 10.1109/EuroSPW55150.2022.00054.

[36] J. Mendivil Caldentey, B. Sanz Urquijo, and M. Gutierrez Almazor, "Formación y concienciación en ciberseguridad basada en competencias: una revisión sistemática de literatura," *Pixel-Bit, Revista de Medios y Educación*, no. 63, pp. 197–225, 2022, doi: 10.12795/pixelbit.91640.

[37] P. R. J. Trim and Y.-I. Lee, "The Global Cyber Security Model: Counteracting Cyber Attacks through a Resilient Partnership Arrangement," *Big Data and Cognitive Computing*, vol. 5, no. 3, p. 32, Jul. 2021, doi: 10.3390/bdcc5030032.

[38] J. Nicholson, J. Terry, H. Beckett, and P. Kumar, "Understanding Young People's Experiences of Cybersecurity," in *Proceedings of the 2021 European Symposium on Usable Security*, New York, NY, USA: ACM, Oct. 2021, pp. 200–210. doi: 10.1145/3481357.3481520.

[39] K. Michalakopoulou, A. Nikitas, E. T. Njoya, and J. Johnes, "Innovation in the legal service industry: Examining the roles of human and social capital, and knowledge and technology transfer," *The International Journal of Entrepreneurship and Innovation*, p. 146575032211196, Aug. 2022, doi: 10.1177/14657503221119667.

[40] T. van Steen, E. Norris, K. Atha, and A. Joinson, "What (if any) behaviour change techniques do government-led cybersecurity awareness campaigns use?," *J Cybersecur*, vol. 6, no. 1, Jan. 2020, doi: 10.1093/cybsec/tyaa019.

[41] S. Barth, M. D. T. de Jong, and M. Junger, "Lost in privacy? Online privacy from a cybersecurity expert perspective," *Telematics and Informatics*, vol. 68, p. 101782, Mar. 2022, doi: 10.1016/j.tele.2022.101782.

[42] J. W. A. Witsenboer, K. Sijtsma, and F. Scheele, "Measuring cyber secure behavior of elementary and high school students in the Netherlands," *Comput Educ*, vol. 186, p. 104536, Sep. 2022, doi: 10.1016/j.compedu.2022.104536.

[43] V. Švábenský, J. Vykopal, and P. Čeleda, "What Are Cybersecurity Education Papers About?," in *Proceedings of the 51st ACM Technical Symposium on Computer Science Education*, New York, NY, USA: ACM, Feb. 2020, pp. 2–8. doi: 10.1145/3328778.3366816.

[44] V. Švábenský *et al.*, "Evaluating Two Approaches to Assessing Student Progress in Cybersecurity Exercises," in *Proceedings of the 53rd ACM Technical Symposium on Computer Science Education*, New York, NY, USA: ACM, Feb. 2022, pp. 787–793. doi: 10.1145/3478431.3499414.

[45] V. Švábenský, J. Vykopal, and P. Čeleda, "What Are Cybersecurity Education Papers About?," in *Proceedings of the 51st ACM Technical Symposium on Computer Science Education*, New York, NY, USA: ACM, Feb. 2020, pp. 2–8. doi: 10.1145/3328778.3366816.

[46] B. J. Blažič, "Changing the landscape of cybersecurity education in the EU: Will the new approach produce the required cybersecurity skills?," *Educ Inf Technol (Dordr)*, vol. 27, no. 3, pp. 3011–3036, Apr. 2022, doi: 10.1007/s10639-021-10704-y.

[47] M. Kyytsönen, J. Ikonen, A.-M. Aalto, and T. Vehko, "The self-assessed information security skills of the Finnish population: A regression analysis," *Comput Secur*, vol. 118, p. 102732, Jul. 2022, doi: 10.1016/j.cose.2022.102732.

[48] S. Bromander *et al.*, "Investigating Sharing of Cyber Threat Intelligence and Proposing A New Data Model for Enabling Automation in Knowledge Representation and Exchange," *Digital Threats: Research and Practice*, vol. 3, no. 1, pp. 1–22, Mar. 2022, doi: 10.1145/3458027.

[49] L. De Kimpe, M. Walrave, P. Verdegem, and K. Ponnet, "What we think we know about cybersecurity: an investigation of the relationship between perceived knowledge, internet trust, and protection motivation in a cybercrime context," *Behaviour & Information Technology*, vol. 41, no. 8, pp. 1796–1808, Jun. 2022, doi: 10.1080/0144929X.2021.1905066.

[50] N. Klimburg-Witjes and A. Wentland, "Hacking Humans? Social Engineering and the Construction of the 'Deficient User' in Cybersecurity Discourses," *Sci Technol Human Values*, vol. 46, no. 6, pp. 1316–1339, Nov. 2021, doi: 10.1177/0162243921992844.

[51] M. Khader, M. Karam, and H. Fares, "Cybersecurity Awareness Framework for Academia," *Information*, vol. 12, no. 10, p. 417, Oct. 2021, doi: 10.3390/info12100417.

[52] T. Alharbi and A. Tassaddiq, "Assessment of Cybersecurity Awareness among Students of Majmaah University," *Big Data and Cognitive Computing*, vol. 5, no. 2, p. 23, May 2021, doi: 10.3390/bdcc5020023.

[53] M. E. Erendor and M. Yildirim, "Cybersecurity Awareness in Online Education: A Case Study Analysis," *IEEE Access*, vol. 10, pp. 52319–52335, 2022, doi: 10.1109/ACCESS.2022.3171829.

[54] W. C. H. Hong, C. Chi, J. Liu, Y. Zhang, V. N.-L. Lei, and X. Xu, "The influence of social education level on cybersecurity awareness and behaviour: a comparative study of university students and working graduates," *Educ Inf Technol (Dordr)*, vol. 28, no. 1, pp. 439–470, Jan. 2023, doi: 10.1007/s10639-022-11121-5.

[55] J. Sleeman, T. Finin, and M. Halem, "Temporal Understanding of Cybersecurity Threats," in *2020 IEEE 6th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing, (HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS)*, IEEE, May 2020, pp. 115–121. doi: 10.1109/BigDataSecurity-HPSC-IDS49724.2020.00030.

[56] C. Sample, S. Ming Loo, C. Justice, E. Taylor, and C. Hampton, "Cyber-Informed: Bridging Cybersecurity and Other Disciplines," in *Proceedings of the 19th European Conference on Cyber Warfare*, ACPI, Jun. 2020. doi: 10.34190/EWS.20.092.

[57] H. M. Jawad and S. Tout, "Gamifying Computer Science Education for Z Generation," *Information*, vol. 12, no. 11, p. 453, Nov. 2021, doi: 10.3390/info12110453.

[58] R. Lasisi, M. Menia, Z. Farr, and C. Jones, "Exploration of AI-enabled Contents for Undergraduate Cyber Security Programs," *The International FLAIRS Conference Proceedings*, vol. 35, May 2022, doi: 10.32473/flairs.v35i.130615.

[59] A. A. Garba, M. M. Siraj, and S. H. Othman, "An assessment of cybersecurity awareness level among Northeastern University students in Nigeria," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 12, no. 1, p. 572, Feb. 2022, doi: 10.11591/ijece.v12i1.pp572-584.

[60] S. Akter, M. R. Uddin, S. Sajib, W. J. T. Lee, K. Michael, and M. A. Hossain, "Reconceptualizing cybersecurity awareness capability in the data-driven digital economy," *Ann Oper Res*, Aug. 2022, doi: 10.1007/s10479-022-04844-8.

[61] International Telecommunication Union, "Global Cybersecurity Index 2020," London, 2020. Accessed: Aug. 24, 2023. [Online]. Available: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf