Cybersecurity Education Showdown: A Comparative Analysis of K-12 Education Systems in the United States, the European Union and China

Berenice Fernández Nieto[1,2,†], Daisy Romanini[1,3,*,†] and Yuhui Zhu[1,4,†]

[1]*IMT Scuola Alti Studi Lucca, Piazza San Francesco, 19 - 55100, Lucca LU, Italy*
[2]*Università degli Studi di Bari "Aldo Moro", Piazza Umberto I, 1 - 70121, Bari BA, Italy*
[3]*Istituto di Informatica e Telematica CNR, Via Giuseppe Moruzzi, 1 - 56124, Pisa PI, Italy*
[4]*Istituto TeCiP, Scuola Superiore Sant'Anna, Via Giuseppe Moruzzi, 1 - 56124, Pisa PI, Italy*

Abstract

Cybersecurity has become a critical aspect of modern life, essential for safeguarding infrastructure, maintaining data integrity, and addressing a growing array of threats. As cyberhygiene and cybersecurity literacy emerge as indispensable skills, K-12 education plays a pivotal role in cultivating a cybersecurity culture while simultaneously preparing the next generation of professionals. To delve into this role, our study conducts a comparative analysis of K-12 cybersecurity education in the United States, the European Union (with a focus on Germany, Estonia, France, and especially Italy), and the People's Republic of China, highlighting their legal frameworks, funding mechanisms, and initiatives aimed at raising public awareness. The findings provide insights into the strengths and gaps in global efforts to integrate cybersecurity into education, offering guidance for policymakers and educators seeking to advance this crucial field. In particular, this work underscores the importance of balancing centralized policies with localized flexibility to create inclusive, adaptative, and dynamic cybersecurity education ecosystems.

Keywords

Cybersecurity, K12 Education, Cybersecurity Literacy, K12 Cybersecurity Education, Cyberhygiene

1. Introduction

The global deficit of cybersecurity professionals has become an increasingly urgent challenge for governments and industries worldwide. In 2022, the cybersecurity workforce gap reached 4 million professionals globally, with North America, Europe, and Asia-Pacific experiencing significant increases in demand [1]. Projections by the World Economic Forum estimate a shortfall of 85 million workers by 2030, potentially leading to $8.5 trillion in unrealized revenue [2]. To address these challenges, K-12 education has emerged as a key strategy for fostering cybersecurity literacy and cultivating future talent.

Although its importance is widely recognized, K-12 cybersecurity education faces significant challenges, including insufficient teaching materials, inadequate teacher training, and limited curricula tailored to diverse student populations [3]. Internationally, programs such as Canada's Cybersecurity 120 and Singapore's Cyber Wellness initiative illustrate progress, but systemic barriers persist, especially in integrating essential skills like password security and social media safety [4].

Equity and inclusion further complicate the landscape. Women represent only 25% of the global cybersecurity workforce, with significant underrepresentation among marginalized communities [5]. This underrepresentation is especially concerning given that empirical studies suggest that workforce

Joint National Conference on Cybersecurity (ITASEC & SERICS 2025), February 03-8, 2025, Bologna, IT

[*] Corresponding author.

[†] The authors are listed alphabetically, and all contributed equally to this work.

berenice.fernandeznieto@imtlucca.it (B. F. Nieto); daisy.romanini@imtlucca.it (D. Romanini); yuhui.zhu@imtlucca.it (Y. Zhu)
https://www.imtlucca.it/it/berenice.fernandeznieto (B. F. Nieto); https://www.imt.it/it/daisy.romanini (D. Romanini); https://www.imtlucca.it/it/yuhui.zhu (Y. Zhu)
0009-0007-0468-5050 (B. F. Nieto); 0009-0006-2271-1438 (D. Romanini); 0000-0003-1116-4679 (Y. Zhu)

diversity enhances problem-solving and fosters innovation, underscoring the importance of inclusive education initiatives [6]. Despite this evidence, progress has been slow and uneven, highlighting the need for more comprehensive policies and targeted interventions to bridge these gaps and build a more diverse and resilient cybersecurity workforce. Nonetheless, it is essential to acknowledge initiatives that are progressively facilitating equality and equity in the sector, such as Women in CyberSecurity (WiCyS) [7], Girls Who Code [8], Cyberjutsu Girls Academy [9], Leading Cyber Ladies [10], Latinas in Cyber (LAIC) [11] and Women in Security and Privacy (WISP) [12], among others.

Against this background, this study examines K-12 cybersecurity education in the United States, the European Union (particularly Italy), and the People's Republic of China, exploring their regulatory frameworks, funding mechanisms, and awareness-raising strategies. These actors were chosen for their technological influence, economic power, and distinct educational approaches.

2. United States of America context

Over the last decade, the United States government has increased its financial support for K-12 cybersecurity education, aiming to cultivate a knowledgeable and proficient workforce in the field [13]. However, significant obstacles remain. A study conducted in 2021 identified several challenges that hinder teachers from effectively implementing cybersecurity education. These include inadequate teaching materials and age-appropriate curricula for students across various grade levels, particularly for underserved and underrepresented demographics [13].

Additionally, disparities in economic resources and program availability across schools lead to unequal educational opportunities for students. While some students benefit from diverse educational programs, access to cybersecurity education remains uneven and infrequent for many others [14]. The fragmented nature of decision-making—spread across national, state, district, and school levels—further exacerbates these disparities. Key educational matters, including learning standards, compulsory education requirements, curriculum design, and teacher certification, are subject to considerable local variation [15]. As an attempt to address these challenges, the NICE Framework was released in March 2024 [16]. The framework aims to establish a common language to categorize and describe cybersecurity work and serves as a tool to familiarize students with cybersecurity concepts, support career exploration, chart paths for future learning, and guide the development of K-12 cybersecurity-specific content [17].

2.1. Regulatory framework

Cybersecurity education in the U.S. is supported by the Every Student Succeeds Act (ESSA), which aims to enhance academic achievement and digital literacy for all students [18]. In 2012, the Department of Homeland Security launched the Cybersecurity Education and Training Assistance Program (CETAP) [19], designed to cultivate cybersecurity talent and improve nationwide cyber literacy through K-12 education programs.

CETAP's oversight was later transferred to the Cyber Defense Education and Training (CDET) under the Cybersecurity & Infrastructure Security Agency (CISA) [19]. On the other hand, Cyber.org, in partnership with CETAP, has become a leader in K-12 cybersecurity education. Through this collaboration, Cyber.org offers comprehensive programs that now reach students across all 50 states, fostering the next generation of cybersecurity professionals [19].

The National Initiative for Cybersecurity Education (NICE) serves as a central actor in advancing cybersecurity education. Through its 2020 strategic plan, NICE outlined five key goals aimed at career discovery, workforce diversity, talent management, framework expansion, and research on effective cybersecurity practices [20]. In 2023, NICE further solidified its role by publishing the Competency Areas, which detail essential competencies and their application in managing cybersecurity risks [21]. Other initiatives, such as Project REACH, Project Access, and CyberPatriot, also contribute significantly to the field.

Building on these efforts to standardize and enhance cybersecurity education, the K-12 Cybersecurity Learning Standards were published in August 2021. Developed by Cyber.org and its partners, these standards aim to support educators at the state and district levels by providing a clear framework based on three core themes: Computing Systems, Digital Citizenship, and Security [22].

Alongside these standards, CyberPatriot, an initiative led by the Air & Space Forces Association, aims to inspire student interest in cybersecurity within the broader STEM fields [23]. CyberPatriot operates through a range of initiatives, including competitions, camps, and an alumni network, while also awarding the CyberPatriot Center of Excellence (COE) designation to institutions that demonstrate excellence in cybersecurity education [24]

Finally, Senate Resolution 247 (2023) officially designated June (in 2023, nowadays is October) as Cybersecurity Education Month, encouraging nationwide efforts to raise cybersecurity awareness and strengthen educational and legislative support [25].

All these efforts and initiatives, including CETAP, NICE, and Cyber.org, are aligned with federal directives and grant-funded programs aimed at strengthening national cybersecurity talent and enhancing the capabilities of the future workforce. While they operate independently, they collectively contribute to action plans that support K-12 cybersecurity education across the United States.

2.2. Funding Mechanisms

Various sources, including federal grants, legislative initiatives, and pilot programs, fund K-12 cybersecurity education efforts. For example, CISA uses federal grants to meet the objectives of its strategic plan[1]. On the other hand, instruments like the Cybersecurity Opportunity Act award grants to higher education institutions that enroll vulnerable and minority students, provide resources to establish or expand cybersecurity programs, and foster partnerships between public and private institutions [27].

Furthermore, the H.R. 6868 - Cybersecurity Grants for Schools Act of 2022 provides financial assistance to state and local schools for cybersecurity education programs and initiatives, as well as support for non-profit organizations [28]. Similarly, the U.S. National Science Foundation has allocated funds to organizations such as the University of Missouri system to promote cybersecurity awareness among K-12 teachers, middle and high school students, and nearby colleges [29].

On the other hand, General educational initiatives from the Department of Education, such as the Student Support and Academic Enrichment Program, assist states, local education agencies, schools, and communities in *1)* providing all students with access to comprehensive education, *2)* improving learning environments, and *3)* enhancing the use of technology to promote academic achievement and digital literacy [30].

Other initiatives supported by diverse entities include the Keesler Air Force Base, Mississippi State University, and the National Security Agency's GenCyber program, which offers a camp for local K-12 teachers to promote cybersecurity awareness for both educators and students [31].

Other players, such as Amazon, have developed comprehensive programs that support students from early childhood to professional careers, focusing on training IT professionals, particularly in underserved and underrepresented communities [32].

2.3. Awareness Raising Strategy

Cybersecurity education awareness efforts are shaped by the Cybersecurity Enhancement Act of 2014, which established the NICE Program Office under the National Institute of Standards and Technology (NIST) [33, 34]. The Act assigns the NIST director, in coordination with federal agencies, industry, educational institutions, and other stakeholders, responsible for leading national cybersecurity awareness and education initiatives. Key efforts include: *1)* Making cybersecurity best practices accessible to individuals, SMEs, educational institutions, and local governments; *2)* Raising public awareness of cybersecurity, cyber safety, and cyber ethics; and *3)* Forecasting the Federal government's cybersecurity workforce needs and supporting recruitment, training, and retention strategies, among others [33, 34].

[1] 1) Understand how attacks occur — and how to stop them, 2) Drive implementation of measurably effective cybersecurity investments, 3) Provide cybersecurity capabilities and services that fill gaps and help measure progress, and 4) Contribute to efforts to build a national cyber workforce [26]

As mentioned above, NICE is a fundamental element in cybersecurity education awareness, and it is responsible for promoting an integrated ecosystem for education, training, and workforce development [34]. Beyond NICE, the CyberPatriot serves as a key effort to encourage K-12 students to explore careers in STEM fields. This national program includes activities such as the National Youth Cyber Defense Competition, the CyberPatriot Alumni Network, AFA Cybercamps, and the CyberPatriot Elementary School Cyber Education Initiative (ESCEI) [35]. It also offers educational resources like *"Sarah the Cyber Hero"* and *"Ben the Cyber Defender"*, alongside initiatives like CyberGenerations and the Senior Citizen's Cyber Safety Initiative, which provide free workshops, and the Tech Caregiver Program, complementing CyberGenerations [35].

Further enhancing cybersecurity awareness, the Stop.Think.Connect. initiative engages a coalition of private companies, non-profits, and government entities, led by the Anti-Phishing Working Group (APWG) and National Cyber Security Alliance (NCSA) [36]. Its goals include increasing cybersecurity awareness, disseminating strategies to improve online security, expanding knowledge on shared responsibility, and involving the public, private sector, and local governments in educational efforts [36]. The initiative also provides a Toolkit, which includes materials tailored for diverse audiences, ranging from K-12 students to senior citizens and law enforcement officials [37].

Expanding on these awareness-raising efforts, recent initiatives continue to broaden the scope and impact of cybersecurity education. In 2024, the Cyber Education Alliance, led by Girls Who Code, launched the Get Cyber Smart campaign during National Cybersecurity Awareness Month. This initiative targets K-12 students with interactive games, lesson plans, career exploration, and educational videos [38]. The private sector also contributes to cybersecurity education, with partnerships like Microsoft's collaboration with Cyber.org through the Technology Education and Literacy in Schools (TEALS) program. TEALS provides professional support and training to teachers and volunteers, helping to implement cybersecurity curricula in high schools nationwide [39].

3. European Union context

As the importance of information and communication technologies (ICT) in daily life continues to grow, influencing personal and educational domains across all age groups, the European Union (EU) is increasingly prioritizing the development of technological skills. The EU Skills Agenda for Sustainable Competitiveness, Social Fairness, and Resilience highlights how the COVID-19 pandemic accelerated the digital shift, making online learning commonplace [40].

However, the rise in online activity comes with inherent risks. The EU Kids Online survey, covering 25 101 children aged 9–16 across 19 European countries, reported that 11% experienced data abuse, highlighting a lack of online security awareness [41]. In Italy, 84% of children aged 9–17 use the internet daily, with 97% of adolescents aged 15–17 having access [42].

In response, the EU has prioritized cybersecurity education. The Digital Education Action Plan (2021–2027) aims to integrate digital skills, including cybersecurity awareness, into school curricula [43]. Collaboration among authorities is crucial to equipping educators with resources and training to meet these goals. Cybersecurity awareness across disciplines helps students protect themselves and respond to threats [44].

Different EU member states demonstrate unique approaches:

- Germany: The IT Security in Schools (*IT-Sicherheit in der Schule*) program incorporates cybersecurity education through federal-state cooperation.
- Estonia: Cybersecurity is integrated at all school levels within its advanced digital infrastructure.
- France: The Ministry of National Education and ANSSI (*Agence Nationale de la Sécurité des Systèmes d'Information*), along with private-sector support, enhance cybersecurity education.
- Italy: Public-private collaborations bolster cybersecurity awareness and practical skill development.

The following section examines EU cybersecurity education policies, highlighting member states' initiatives, with a focus on Italy's contributions.

3.1. Regulatory framework

The EU's cybersecurity strategy is primarily guided by the Digital Education Action Plan and the Cybersecurity Act. These emphasize digital literacy, including cybersecurity, to prepare students for safe online participation [43, 45].

The European Union Agency for Cybersecurity (ENISA) supports member states through resources like the "CyberEducation Platform" to raise awareness among children [46]. Cybersecurity education combines technical, human and societal elements, helping professionals address challenges while considering ethical implications [47].

National initiatives reflect diverse implementations:

- Germany: Integrates cybersecurity in schools through its IT Security Act and tailored state programs [48, 49].
- Estonia: Offers cybersecurity resources like the "e-School" platform and emphasizes data protection and ethics [50].
- France: ANSSI's "CyberEdu" and the Digital Plan for Education (*Plan de Numérique pour l'Éducation*) provide K-12 modules and resources [51, 52].

Italy's cybersecurity strategy is led by key institutions: the Inter-Ministerial Committee for Cybersecurity (*Comitato Interministeriale per la Cybersicurezza*- CIC), the Department of Information Security (*Dipartimento delle informazioni per la sicurezza* - DIS) and the National Cybersecurity Agency (*Agenzia per la Cybersicurezza Nazionale* - ACN). The CIC, chaired by the Prime Minister, oversees the National Strategic Framework for Cybersecurity, coordinating efforts to protect national security. The DIS provides strategic intelligence, while the ACN, established in 2021, ensures compliance with national and EU cybersecurity policies, such as the NIS2 Directive, which mandates real-time incident reporting and tighter regulations for critical sectors[53, 54].

Aligned with the EU's Digital Education Action Plan and the NIS2 Directive, Italy prioritizes digital literacy and cybersecurity awareness in its national curriculum, starting with K-12 education. The ACN supports these efforts to foster a digitally resilient society [55].

Italy's cybersecurity education framework integrates the National Cybersecurity Strategy and the National Plan for Digital Schools (PNSD), emphasizing digital literacy across all school levels [56]. Initiatives include "Bringing Logical and Computational Thinking to the whole Primary School," offering 10 annual hours of lessons in primary schools. Voluntary programs, such as the "Programme for the Future" and competitions like "IT and Social Responsibility," further promote digital skills, with implementation varying regionally [57].

3.2. Funding Mechanisms

EU funding through Digital Europe and Horizon Europe supports cybersecurity education, allocating € 7.5 billion to digital transformation [58]. Member states receive additional resources:

- Germany: Programs like *DigitalPakt Schule* enhance schools' digital infrastructure through industry partnerships with companies like Siemens and SAP [59].
- Estonia: EU grants support platforms such as "e-School" [60].
- France: The Ministry of National Education collaborates with private companies like Orange Cyberdefense to fund training and campaigns [61].

Italy combines national and EU funding. The National Plan for Recovery and Resilience (PNRR) allocates € 6.23 billion to develop digital skills, including cybersecurity education. The country also benefits from funding through Horizon Europe and Digital Europe, supporting initiatives to improve digital literacy and address emerging cyber threats [62]. Partnerships with companies like Cisco and Google provide certifications and workshops to enhance learning [63][64].

3.3. Awareness Raising Strategy

The EU promotes cybersecurity awareness through European Cybersecurity Month (ECSM), which focuses on online security and data privacy citecybersecmonth. ENISA also leads initiatives like the European Cyber Security Challenge (ECSC) and Team Europe, fostering global collaboration and talent development [65]. Serious games such as "Targeted Attack" and "Cybersecurity Lab" simulate real-world challenges to build skills [66, 67].

National initiatives include:

- Germany: *IT-Sicherheit in der Schule* program organizes workshops and competitions [68].
- Estonia: Digital curriculum resources teach cyber hygiene and security [69, 70].
- France: ANSSI's "CyberEdu" and industry partnerships enhance education and competitions [71].

In Italy, Ludoteca del Registro .it uses certified games and tools to teach online security. Initiatives like Cyber Park and the Super Cyber Kids project target primary and middle school students [72, 42]. Challenges include limited educator knowledge, engagement difficulties, and voluntary program participation [73].

Programs like "Be Internet Awesome" by Google and Cisco's Networking Academy raise awareness of cybersecurity careers [74, 75]. "The Big Game", an initiative by the Italian Cybersecurity National Lab (CINI), integrates gamification into training and competitions to address workforce gaps and enhance Italy's cybersecurity ecosystem [65]. Key components include: *1)* CyberChallenge.IT: Italy's first cybersecurity training program for students aged 16–24, *2)* OliCyber.IT: Aimed at high school students, this program encourages technical engagement through competitions, *3)* CyberTrials: A training initiative for high-school girls to address the gender gap in cybersecurity, *4)* TeamItaly: The national cybersecurity team competing in international challenges like ECSC, *5)* CyberHighSchools: A network of schools integrating intermediate cybersecurity education.

4. People's Republic of China context

China's cybersecurity education effectively leverages existing regulatory tools, the education system, and public awareness campaigns. The implementation process demonstrates a strong preference for administrative command-based measures.

4.1. Regulatory framework

The root of the People's Republic of China cybersecurity regulation is the *Cybersecurity Law*, which was enacted by the National People's Congress of People's Republic of China in November 2016 [76, 77]. While this law mostly aims at the technical and administrative side of the national interest of cybersecurity, it also emphasizes the importance of cybersecurity education as a supporting and promotion approach. The law specifically designates entities responsible for advancing cybersecurity education, public awareness, and societal engagement.

While the Cybersecurity Law establishes an abstract framework for cybersecurity education, its effective implementation relies heavily on collaboration between various government departments at the national and local levels. Given that cybersecurity education encompasses both technical issues and broader educational concerns, two key subsystems within the national and local governments, *Cyberspace Administration of China* [78] and *Ministry of Education* [79], are primarily responsible for its execution. *Local governments* are also tasked with developing tailored plans to fulfill the unique conditions of respective regions.

The design and implementation of K0-K12 curricula are guided by a unique national standard that ensures consistency across the country. In this context, cybersecurity—a relatively new and emerging field—has also been integrated into the educational framework.

The *National Curriculum* [80] consists of compulsory guidelines that are uniformly implemented across the country as the core of China's national education system. These guidelines outline the objectives, content, and basic teaching requirements for each subject, offering clear and standardized guidance for schools at all educational levels. It also establishes a quality standard for textbooks used in the cybersecurity education process. While publishing houses and provinces have the autonomy to organize and author textbooks tailored to specific regional or educational needs, all these textbooks are subject to revision and approval by the MoE.

As part of the curriculum reforms introduced in 2017 and 2022, *Information Technology* was officially designated as a national subject for both high school and compulsory education [81, 82]. In the first debut of information technology as a national subject, cybersecurity issues were incorporated across multiple topics and integrated into sub-modules designed to align with the varying cognitive levels of students at different stages of education.

The core content of the subject begins with basic digital literacy for K1 students and progresses to more practical digital skills for high school students. Alongside this progression, relevant cybersecurity topics are addressed in parallel, aiming to foster a deeper understanding of the digital world. As a national subject that is theoretically mandatory for all students, it provides a holistic framework that allows students to understand the cybersecurity challenges present in the digital landscape. Moreover, it ensures that even students who do not pursue careers in technical fields acquire critical knowledge that is essential for responsible citizenship in an increasingly digital society.

Unlike the compulsory and common high school education system, vocational high school education in China is structured around a profession-based framework, similar to colleges and universities. In 2021, cybersecurity was officially included in the *Catalogue of Vocational Education Professions* [83]. While there is no standardized curriculum for vocational high schools, the Ministry of Education oversees the qualification of textbooks primarily through a unified review process [84]. This open policy has encouraged professors and researchers from higher education institutions to contribute to the development of more effective textbooks and learning materials.

4.2. Funding Mechanisms

While there have been numerous funding initiatives for cybersecurity education aiming at the higher education level, as of 2024, there is still no national-level funding for primary and secondary education.

Some local governments with abundant financial resources are proactive in funding educational research activities. Several schools have also sought government funding for cybersecurity education under this framework. For example, Haian Chengnan Experimental Primary School initiated a research project focused on exploring the paradigm of cybersecurity education at the primary school level [85]. This research is funded by the Education Bureau of Nantong Municipality, although the grant amount has not been disclosed.

Besides this grant, very few similar instances can be found in the publicly available government announcements. Although Information Technology has been incorporated into the national curriculum in recent years, it is still considered a supplementary subject and often overlooked in educational research and entrance examinations (*Zhongkao* and *Gaokao*). Also, since secondary school graduates are generally not considered skilled labor forces, existing programs primarily focus on basic cybersecurity hygiene literacy, as the education system expects any technical aspects of cybersecurity to be addressed at the higher education level for those pursuing careers in this field.

4.3. Awareness Raising Strategy

The primary focus of the awareness-raising strategy in mainland China is on promoting cyber hygiene and safe online practices. At the same time, there are initiatives aimed at sparking students' interest in the technical aspects of cybersecurity, helping to prepare them for potential professional careers in the field.

Similar to initiatives in Europe and the United States, CAC has launched *National Cybersecurity Week* annually since 2014 [86, 87]. This event aims to raise public awareness of cybersecurity issues. While its primary focus is not directly on K0-K12 students, schools are still required to participate as key execution units by preparing special lectures related to cybersecurity. Additionally, local governments and businesses work closely with the education system to increase social awareness by offering resources that schools may otherwise lack. For example, *Haidian District* is an administrative area in *Beijing*, renowned for being home to many of China's top-tier universities and leading IT industries. Leveraging its top-tier intellectual resources within mainland China, during the 2024 edition of National Cybersecurity Week, the district organized a series of interactive cybersecurity lectures [88]. In collaboration with the Ministry of Industry and Information Technology, Haidian Education Science Research Institute, and local schools, these lectures covered a wide range of technical issues affecting privacy and information security in daily life, addressing common cyber threats such as QR code scams and weak passwords. The initiative, which engaged over 1,500 students, aimed to enhance their awareness of cybersecurity risks while equipping them with practical knowledge to navigate the digital world safely. Through this collaborative effort, Haidian District is making significant strides in fostering digital literacy and promoting cybersecurity best practices among its younger population. *Shenzhen* also organized similar activities by hosting "study tours" in collaboration with local companies [89].

Outside of major cities with thriving digital economies and advanced practices, limitations in teaching resources and research capabilities often make it challenging to conduct in-depth cybersecurity lectures. As a result, awareness-raising campaigns in these areas are typically conducted in collaboration with local law enforcement and schools, primarily focusing on cyber hygiene-related issues such as internet addiction, misinformation, and telecom fraud [90, 91].

Some provincial governments have also developed a series of cybersecurity competitions by leveraging the resources of local universities and research institutes. The *Qiangwang Bei (Cup)* [92, 93] is a Capture the Flag (CTF) competition organized by Henan Province in partnership with CAC and the PLA Information Engineering University. While the competition primarily targets professional hacker teams with advanced qualifications, it also features a special session aimed at identifying and nurturing young talent interested in pursuing careers in cybersecurity [94]. Sichuan Province also hosted a similar competition, leveraging the resources of the School of Cyber Science and Engineering at Sichuan University [95, 96]. This competition is connected with "Youth Program" [97], an early-entrance admission program, which aims to select high school students with exceptional cybersecurity talents outside of the regular college entrance examination (Gaokao). This program allows students to enter university without the requirement of completing three years of high school education. In addition, Beijing University of Posts and Telecommunications organized comparable events modeled after the *International Olympiad in Informatics (IOI)* framework [98]. However, this initiative was eventually discontinued after 2019.

Although China has established a multi-level, customizable strategy for cybersecurity awareness at both the national and local levels, its implementation remains inconsistent.

National-level awareness initiatives tend to be well-executed, as they are planned and evaluated by both national and local administrative bodies, with funding and oversight ensured. However, local-level efforts often face significant challenges, including a lack of dedicated funding, limited awareness, absence of independent evaluation mechanisms, insufficient long-term activity planning, and shortages of expert resources. As a result, these initiatives risk being unsustainable in the long run.

5. Comparative Analysis

The global efforts to integrate cybersecurity education reveal both strengths and gaps across different regions. In the United States, the emphasis on collaboration between the private sector, nonprofits, and federal initiatives (together with the NICE framework) is fostering innovation in cybersecurity education while simultaneously broadening the range of pedagogical resources for educators. However, the absence of a uniform national curriculum and unequal availability of resources among schools has led to disparities in access, particularly across diverse states. In contrast, the European Union demonstrates a strong and unified commitment through the Digital Education Action Plan and robust funding mechanisms like Horizon Europe. While member states such as Germany, Estonia, and France have shown notable progress in integrating cybersecurity into curricula, implementation remains uneven across the region due to varying local priorities and capacities. Italy's integration of cybersecurity education within national frameworks like the National Cybersecurity Strategy is notable. However, regional disparities and reliance on voluntary programs still pose challenges. Meanwhile, China's approach stands out for its standardized, government-driven model, ensuring broad access to cybersecurity education through a unified national curriculum. However, the top-down structure may limit flexibility and adaptability to rapidly evolving cybersecurity threats and regional needs.

These findings underscore the need for a balanced approach, one that combines structured national policies with localized adaptability. Effective cybersecurity education should integrate standardized frameworks with mechanisms that allow regional and institutional innovation, ensuring inclusivity and responsiveness to emerging challenges. A global strategy that fosters both consistency and adaptability is key to equipping future generations with the necessary skills to navigate an increasingly complex digital world.

6. Conclusion

Integrating cybersecurity education into K-12 curricula is crucial to addressing the growing workforce gap and fostering a culture of digital literacy. Our comparative analysis of cybersecurity education systems in the United States, the European Union, and China highlights various approaches shaped by governance structures, funding mechanisms, and awareness strategies. In the United States, a fragmented system (driven by nonprofit and private sector collaboration) has spurred innovation, but also exacerbated resource disparities. The European Union's centralized framework, supported by strong funding initiatives, has facilitated progress, though local implementation challenges persist. Meanwhile, China's government-led model ensures broad access but may lack the flexibility needed to respond to evolving cyber threats.

This study contributes to the literature by examining how regulatory frameworks, funding strategies, and awareness initiatives influence the effectiveness of K-12 cybersecurity education. The findings underscore the need for adaptable national curriculum guidelines that establish a consistent foundation while allowing localized adjustments to meet specific needs. Equally important is sustained investment in educator training, resource accessibility, and cross-sector partnerships to support effective cybersecurity education across diverse contexts.

Future research should focus on improving localized education efforts, reducing regional disparities, and promoting curriculum innovation. In addition, more research on effective evaluation metrics and funding models is needed to ensure that cybersecurity education remains accessible and adaptable to the rapidly evolving digital landscape. Addressing these challenges will be the key to equipping the next generation with the skills necessary to navigate an increasingly complex cyber environment.

CRediT Author Statement

Berenice Fernandez Nieto: Visualization, Investigation, Writing - Original draft, Writing - Review & Editing. **Daisy Romanini**: Conceptualization, Investigation, Writing - Original draft, Writing - Review & Editing. **Yuhui Zhu**: Resources, Investigation, Writing - Original draft, Writing - Review & Editing.

Acknowledgments

This work was partially supported by SERICS (PE00000014) under the MUR National Recovery and Resilience Plan funded by the European Union - NextGenerationEU; Project EMERALD (Grant agreement No. 101120688) under the EU's Horizon Europe Innovation program; and Project PNRR (DM 351/2022 I.3.4).

The authors sincerely thank Professor Paolo Prinetto for his guidance and lifelong commitment to advancing cybersecurity, and Dr. Sonia Montegiove for her dedication to promoting the inclusion of women in this field.

No competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Declaration on Generative AI

During the preparation of this work, the authors used ChatGPT-4o for grammar and spelling checking. After using this tool, the authors reviewed and edited the content as needed and take full responsibility for the publication's content.

References

[1] ISC2, How the economy, skills gap and artificial intelligence are challenging the global cybersecurity workforce 2023, 2023. URL: https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2_Cybersecurity_Workforce_Study_2023.pdf?rev=28b46de71ce24e6ab7705f6e3da8637e, accessed: 2024-11-14.

[2] W. E. Forum, Cybersecurity industry has an urgent talent shortage. here's how to plug the gap, 2024. URL: https://www.weforum.org/stories/2024/04/cybersecurity-industry-talent-shortage-new-report/, accessed: 2024-11-14.

[3] W. Chen, Y. He, X. Tian, W. He, Exploring cybersecurity education at the k-12 level, in: E. Langran, D. Rutledge (Eds.), Proceedings of SITE Interactive Conference, Association for the Advancement of Computing in Education, 2021, pp. 108–114. URL: https://www.learntechlib.org/primary/p/220175/.

[4] A. Ibrahim, et al., A systematic review of k-12 cybersecurity education around the world, IEEE Access 12 (2024) 59726–59738. URL: https://doi.org/10.1109/ACCESS.2024.3393425. doi:10.1109/ACCESS.2024.3393425.

[5] European Cyber Security Organisation, Gender diversity in cybersecurity, 2022. URL: https://ecs-org.eu/ecso-uploads/2022/10/622f59b70f039.pdf.

[6] G. Javidi, E. Sheybani, K-12 cybersecurity education, research, and outreach, in: 2018 IEEE Frontiers in Education Conference (FIE), 2018, pp. 1–5. doi:10.1109/FIE.2018.8659021.

[7] W. in CyberSecurity (WiCyS), Wicys - women in cybersecurity, 2025. URL: https://www.wicys.org/, accessed: 2025-02-10.

[8] G. W. Code, Girls who code, n.d. URL: https://girlswhocode.com/, accessed: 2025-02-10.

[9] C. G. Academy, Cyberjutsu girls academy | stem workshops for girls - women's society of cyberjutsu, 2017. URL: https://womenscyberjutsu.org/mpage/CGA_Home, accessed: 2025-02-10.

[10] L. C. Ladies, Leading cyber ladies, n.d. Accessed: 2025-02-10.

[11] L. in Cyber (LAIC), Latinas in cyber, 2022. Accessed: 2025-02-10.

[12] W. in Security, Privacy, Women in security and privacy, n.d. URL: https://www.wisporg.com, accessed: 2025-02-10.

[13] W. Chen, Y. He, X. Tian, W. He, Exploring cybersecurity education at the k-12 level, in: Proceedings of the Society for Information Technology & Teacher Education International Conference, 2021, pp. 108–114. URL: https://www.learntechlib.org/primary/p/220175/.

[14] Ed Week Research Center, The state of cybersecurity education in k-12 schools, 2020. URL: https://cyber.org/sites/default/files/2020-06/The%20State%20of%20Cybersecurity%20Education%20in%20K-12%20Schools.pdf.

[15] J. Gal-Ezer, C. Stephenson, A tale of two countries: Successes and challenges in k-12 computer science education in israel and the united states, ACM Transactions on Computing Education 14 (2014) 8:1–8:18. URL: https://doi.org/10.1145/2602483. doi:10.1145/2602483.

[16] National Initiative for Cybersecurity Careers and Studies, Workforce framework for cybersecurity (nice framework) | niccs, 2024. URL: https://niccs.cisa.gov/workforce-development/nice-framework, accessed: [insert access date here].

[17] National Institute of Standards and Technology, NICE Framework K12 Frequently Asked Questions, 2024. URL: https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center/about/faq/k12-faq.

[18] Every student succeeds act, https://www.congress.gov/114/plaws/publ95/PLAW-114publ95.pdf, 2015. 20 U.S.C.

[19] Cybersecurity & Infrastructure Security Agency, Cybersecurity education and training assistance program, 2023. URL: https://niccs.cisa.gov/sites/default/files/documents/CDET_Fact%20Sheet_CETAP_020223.pdf?trackDocs=CDET_Fact%20Sheet_CETAP_020223.pdf, accessed: 2024-11-14.

[20] NICE, NICE strategic plan, 2021. URL: https://www.nist.gov/document/nice-implementation-plan-2021.

[21] K. Wetzel, NICE Framework Competency Areas:: Preparing a Job-Ready Workforce, NIST IR 8355, National Institute of Standards and Technology, 2023. URL: https://doi.org/10.6028/NIST.IR.8355.

[22] Cyber Innovation Center & CYBER.ORG, K-12 cybersecurity learning standards, 2021. URL: https://cyber.org/sites/default/files/2021-10/K-12%20Cybersecurity%20Learning%20Standards_1.0.pdf, accessed: 2024-11-14.

[23] CyberPatriot, Centers of excellence, 2013. URL: https://www.uscyberpatriot.org/Pages/About/Centers-of-Excellence.aspx.

[24] CyberPatriot, Cyberpatriot i, 2023. URL: https://www.uscyberpatriot.org/Pages/Competition/Season%20History/CyberPatriot-I.aspx.

[25] US Congress, Senate resolution 247–designating june 2023 as national cybersecurity education month; congressional record vol. 169, no. 103, 2023. URL: https://www.congress.gov/congressional-record/volume-169/issue-103/senate-section/article/S2074-1?q=%7B%22search%22%3A%5B%22s.+res.+247%22%5D%7D&s=1&r=1.

[26] Cybersecurity and Infrastructure Security Agency, Cisa cybersecurity strategic plan fy2024-2026, 2023. URL: https://www.cisa.gov/sites/default/files/2023-08/FY2024-2026_Cybersecurity_Strategic_Plan.pdf, accessed: 2024-11-14.

[27] U.S. Congress, S.2305 - cybersecurity opportunity act, 117th congress (2021-2022), 2022. URL: https://www.congress.gov/bill/117th-congress/senate-bill/2305/text, accessed: 2024-11-14.

[28] U.S. Congress, H.r.6868 - cybersecurity grants for schools act of 2022, 2022. URL: https://www.congress.gov/bill/117th-congress/house-bill/6868/text?q=%7B%22search%22%3A%5B%22Cybersecurity+Grants+for+Schools+Act+of+2022%22%2C%22Cybersecurity%22%2C%22Grants%22%2C%22for%22%2C%22Schools%22%2C%22Act%22%2C%22of%22%2C%222022%22%5D%7D&r=1&s=1, accessed: 2024-11-14.

[29] U.S. National Science Foundation, Cybercorps sfs renewal: Federal and university training union for research and education on security (futures), n.d. URL: https://nsf.gov/awardsearch/showAward?AWD_ID=1946619, accessed: 2024-11-14.

[30] U.S. Department of Education, Student support and academic enrichment program (title iv, part a), 2024. URL: http://www.ed.gov/grants-and-programs/formula-grants/school-improvement/student-support-and-academic-enrichment-program, accessed: 2024-11-14.

[31] A. Education, T. Command, Gencyber: Keesler, msu empowers local k-12 teachers through cyber initiative, 2024. URL: https://www.aetc.af.mil/News/Article-Display/Article/3810229/gencyber-keesler-msu-empowers-local-k-12-teachers-through-cyber-initiative/, accessed: 2024-11-14.

[32] A. F. Engineer, Amazon future engineer, 2024. URL: https://www.amazonfutureengineer.com/, accessed: 2024-11-14.

[33] U.S. Congress, Public law no. 113-274 (12/18/2014), 2024. URL: https://www.congress.gov/bill/

113th-congress/senate-bill/1353/text, accessed: 2024-11-14.

[34] National Institute of Standards and Technology, About, 2024. URL: https://www.nist.gov/itl/applied-cybersecurity/nice/about, accessed: 2024-11-14.

[35] Air & Space Forces Association, What is cyberpatriot?, 2013. URL: https://www.uscyberpatriot.org/Pages/About/What-is-CyberPatriot.aspx, accessed: 2024-11-15.

[36] Stop Think Connect, About stop. think. connect., n.d. URL: https://www.stopthinkconnect.org/about, accessed: 2024-11-15.

[37] U.S. Department of Homeland Security (DHS), Stop.think.connect., 2013. URL: https://www.nist.gov/system/files/documents/2017/01/19/d1_trk1_dorville_stop_think_connect_2.pdf, accessed: 2024-11-15.

[38] E. Stokes, #GetCyberSmart: Girls Who Code and Partners Unveil Cybersecurity Resources for K-12 Students, 2024. URL: https://www.edtechinnovationhub.com/news/girls-who-code-launches-cyber-education-campaign, accessed: 2024-11-15.

[39] CYBER.ORG, Cyber.org joins microsoft's teals program as its first partner to deliver free cybersecurity curriculum, 2022. URL: https://cyber.org/news/cyberorg-joins-microsofts-teals-program-its-first-partner-deliver-free-cybersecurity, accessed: 2024-11-15.

[40] European Commission, Commission presents European Skills Agenda for sustainable competitiveness, social fairness and resilience, https://ec.europa.eu/social/main.jsp?langId=en&catId=89&furtherNews=yes&newsId=9723, 2020.

[41] London School of Economics and Political Science, EU kids online 2020, https://www.lse.ac.uk/media-and-communications/research/research-projects/eu-kids-online/eu-kids-online-2020, 2020.

[42] G. Bassi, S. Fabbri, A. Vaccarelli, Cybersecurity Education: A Gamification Approach, https://conference.pixel-online.net/library_scheda.php?id_abs=6126, 2023.

[43] European Commission, Digital education action plan 2021-2027, <a href="{">{</a>https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX, 2020.

[44] G. Langner, J. Andriessen, G. Quirchmayr, S. Furnell, V. Scarano, T. J. Tokola, Poster: The Need for a Collaborative Approach to Cyber Security Education, in: 2021 IEEE European Symposium on Security and Privacy (EuroS&P), 2021, pp. 719–721. doi:10.1109/EuroSP51992.2021.00058.

[45] European Parliament and Council, Regulation (EU) 2019/881 on information and communications technology cybersecurity certification (Cybersecurity Act), <a href="{">{</a>https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex, 2019.

[46] European Union Agency for Cybersecurity, ENISA CyberEducation platform, https://www.enisa.europa.eu/topics/education/cyberedu/#/, 2024.

[47] M. Bishop, D. Burley, S. Buck, J. J. Ekstrom, L. Futcher, D. Gibson, E. K. Hawthorne, S. Kaza, Y. Levy, H. Mattord, A. Parrish, Cybersecurity Curricular Guidelines, in: M. Bishop, L. Futcher, N. Miloslavskaya, M. Theocharidou (Eds.), Information Security Education for a Global Digital Society, IFIP Advances in Information and Communication Technology, Springer International Publishing, Cham, 2017, pp. 3–13. doi:10.1007/978-3-319-58553-6_1.

[48] Bundesamt für Sicherheit in der Informationstechnik, Cybersicherheit in der Schule, in Bildungseinrichtungen und zuhause, https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Sicher-im-digitalen-Schulalltag/digitaler-schulalltag_node.html, 2023.

[49] Federal Ministry for Economic Affairs and Energy of Germany, Germany - digital strategy 2025, https://digital-skills-jobs.europa.eu/en/actions/national-initiatives/national-strategies/germany-digital-strategy-2025, 2021.

[50] Estonian Ministry of Education and Research, Estonia: A snapshot of digital skills, https://digital-skills-jobs.europa.eu/en/latest/briefs/estonia-snapshot-digital-skills, 2023.

[51] Ministère de l'Éducation nationale, Stratégie du numérique pour l'éducation 2023-2027, https://www.education.gouv.fr/strategie-du-numerique-pour-l-education-2023-2027-344263, 2024.

[52] Agence Nationale de la Sécurité des Systèmes d'Information, La formation initiale en cybersécurité,

https://cyber.gouv.fr/formation-initiale-en-cybersecurite, 2024.

[53] V. Viscardi, The Influence of National Cultures on Cybersecurity Strategies: A Comparative Case Studies analysis of the UK and Italy's Cybersecurity Postures, https://dspace.cuni.cz/handle/20.500.11956/177255, 2020-09-16, 2020.

[54] L. Martino, The Italian Cybersecurity Ecosystem, in: L. Martino (Ed.), Cybersecurity in Italy: Governance, Policies and Ecosystem, Springer International Publishing, Cham, 2024, pp. 11–29. doi:10.1007/978-3-031-64396-5_2.

[55] Italian National Cybersecurity Agency, National cybersecurity strategy, https://www.acn.gov.it/portale/en/strategia-nazionale-di-cybersicurezza, 2022.

[56] Ministero dell'Istruzione e del Merito, Piano nazionale scuola digitale, https://www.mim.gov.it/scuola-digitale, 2018.

[57] E. Biolo, IT literacy in primary school education system: A comparative study of Finland, French-speaking Switzerland and Italy, https://www.theseus.fi/bitstream/handle/10024/857004/Biolo_Eleonora.pdf?sequence=2&isAllowed=y, 2024.

[58] European Commission, The digital europe programme, https://digital-strategy.ec.europa.eu/en/activities/digital-programme, 2024.

[59] Bundesministerium für Bildung und Forschung, Die finanzen im DigitalPakt schule, https://www.digitalpaktschule.de/de/die-finanzen-im-digitalpakt-schule-1763.html, 2024.

[60] E-Estonia, What is e-education?, https://e-estonia.com/what-is-e-education/, 2024.

[61] Ministère de l'Éducation nationale, L'éducation à la cybersécurité, https://www.education.gouv.fr/l-education-la-cybersecurite-380421, 2024.

[62] European Research Executive Agency, Increased cybersecurity, https://rea.ec.europa.eu/funding-and-grants/horizon-europe-cluster-3-civil-security-society/increased-cybersecurity_en, 2024.

[63] Dipartimento per la Trasformazione Digitale, Le misure del PNRR per la transizione digitale, https://padigitale2026.gov.it/misure/, 2024.

[64] Camera dei Deputati, Memoria di cisco systems italy sulla difesa cibernetica italiana, https://documenti.camera.it/leg19/documentiAcquisiti/COM04/Indagine/leg19.com04.Indagine.Memoria.PUBBLICO.ideGes.29853.23-05-2024-11-17-27.203.pdf, 2024.

[65] G. Ferraro, N. Maunero, S. Montegiove, P. Prinetto, The Big Game: The Italian Avenue of Attack to Cybersecurity Skill Shortage, in: M. Hinchey, B. Steffen (Eds.), The Combined Power of Research, Education, and Dissemination: Essays Dedicated to Tiziana Margaria on the Occasion of Her 60th Birthday, Springer Nature Switzerland, Cham, 2025, pp. 19–34. doi:10.1007/978-3-031-73887-6_2.

[66] B. J. Blažič, Changing the landscape of cybersecurity education in the EU: Will the new approach produce the required cybersecurity skills?, Education and Information Technologies 27 (2022) 3011–3036. doi:10.1007/s10639-021-10704-y.

[67] B. Jerman Blažič, A. Jerman Blažič, Cybersecurity Skills among European High-School Students: A New Approach in the Design of Sustainable Educational Development in Cybersecurity, Sustainability 14 (2022) 4763. doi:10.3390/su14084763.

[68] Bundesamt für Sicherheit in der Informationstechnik, Awareness, https://www.bsi.bund.de/dok/13768350, 2024.

[69] Estonian Education and Youth Board, E-School, https://e-estoniax.com/solution/e-school/, 2024.

[70] Ministry of Education and Research of Estonia, Cyber security education in Estonia: From kindergarten to NATO Cyber Defence Centre, https://www.educationestonia.org/cyber-security-education-in-estonia/, 2024.

[71] Agence Nationale de la Sécurité des Systèmes d'Information, CyberEdu: La cybersécurité pour toutes les formations en informatique, https://cyber.gouv.fr/cyberedu-la-cybersecurite-pour-toutes-les-formations-en-informatique, 2024.

[72] G. Bassi, S. Fabbri, A. Franceschi, Teaching Cybersecurity: The Evaluation of Nabbovaldo and Blackmail from Space, in: G. Fulantelli, D. Burgos, G. Casalino, M. Cimitile, G. Lo Bosco, D. Taibi (Eds.), Higher Education Learning Methodologies and Technologies Online, Communications

in Computer and Information Science, Springer Nature Switzerland, Cham, 2023, pp. 136–147. doi:10.1007/978-3-031-29800-4_11.

[73] F. Manganello, P. Callaghan, G. Città, P. Denaro, J. Earp, C. Fante, D. Ifenthaler, C. Kirna, L. J. Laszlo, I. Matteucci, S. Perna, N. Plintz, A. Vaccarelli, M. Gentile, SuperCyberKids: Enhancing Cybersecurity Education in K-12 Through Digital Game-Based Learning, in: G. Casalino, R. Di Fuccio, G. Fulantelli, P. Raviolo, P. C. Rivoltella, D. Taibi, G. A. Toto (Eds.), Higher Education Learning Methodologies and Technologies Online, Springer Nature Switzerland, Cham, 2024, pp. 323–334. doi:10.1007/978-3-031-67351-1_22.

[74] Google, Vivi Intenet al meglio - Il programma sulla sicurezza online, https://beinternetawesome.withgoogle.com/it_it/, 2024.

[75] Cisco Systems, Networking Academy - Scuola digitale, https://www.scuoladigitalecisco.it/networking-academy/, 2024.

[76] Cybersecurity Law of PRC, https://www.cac.gov.cn/2016-11/07/c_1119867116.htm, 2016.

[77] Cybersecurity Law of the People's Republic of China, Wikipedia (2024). https://en.wikipedia.org/w/index.php?title=Cybersecurity_Law_of_the_People%27s_Republic_of_China&oldid=1233739940.

[78] Homepage of Cyberspace Administration of China, https://www.cac.gov.cn/index.htm, ????.

[79] Homepage of Ministry of Education, PRC, http://www.moe.gov.cn/, ????.

[80] Nord Anglia Education, The Chinese Curriculum, https://www.nordangliaeducation.com/academic-excellence/curricula-guide/chinese-curriculum, ????

[81] Ministry of Education of PRC, Information Technology Curriculum Standards for Compulsory Education (2022 Edition), Beijing Normal University Publishing Group, 2022. http://www.moe.gov.cn/srcsite/A26/s8001/202204/t20220420_619921.html.

[82] Ministry of Education of PRC, Information Technology Curriculum Standards for Regular High Schools (2017 Edition, Revised 2020), People's Education Press, 2020. http://www.moe.gov.cn/srcsite/A26/s8001/202006/t20200603_462199.html.

[83] Ministry of Education of PRC, Catalogue of Vocational Education Professions (2021)., http://www.moe.gov.cn/srcsite/A07/moe_953/202103/t20210319_521135.html, 2021.

[84] Ministry of Education of PRC, The First Batch of "14th Five-Year Plan" National Vocational Education Textbooks List., http://www.moe.gov.cn/srcsite/A07/moe_953/202306/t20230629_1066321.html, 2023.

[85] Hai'an Chengnan Experimental Primary School, Nantong, The "14th Five-Year Plan" of Nantong Educational Science (Educational Technology Project) - Research on the Project-based Practice of Cyber Security Education in Primary Schools, https://mp.weixin.qq.com/s/HDu6KvTN7Xg-kqUlIpiqfw, 2024.

[86] Cyberspace Administration of China, Homepage of National Cybersecurity Week, 2024 Edition, https://www.cac.gov.cn/gzzt/ztzl/zt/waz/A0920011111index_1.htm, 2024.

[87] National Cybersecurity Week (in Chinese), Wikipedia (2024). https://zh.wikipedia.org/w/index.php?title=%E5%9B%BD%E5%AE%B6%E7%BD%91%E7%BB%9C%E5%AE%89%E5%85%A8%E5%AE%A3%E4%BC%A0%E5%91%A8&oldid=84195861.

[88] Education Commission of Haidian District, Beijing, Haidian District, Interactive Lectures on Cybresecurity Education, https://www.bjhdedu.cn/xw/jwdt/202409/t20240920_73761.html, 2024.

[89] Shenzhen Information Industry Association, The 2024 Yantian District Youth Cybersecurity Study Tour, http://www.sziia.org/contentPage.html?news=yjdt&num=3&key=yjdt3&id=2&newid=7741, 2024.

[90] Xinhua News Agency, Cybersecurity Week in School Campuses, http://csj.news.cn/20240912/c05d3526e6c648b2a32a995c36351115/c.html, 2024.

[91] Xinhua News Agency, Guizhou Channel, Cybersecurity Week in School Campuses (Guizhou Province), http://gz.news.cn/20240912/4d1385ddb25147398d454aadc1544193/c.html, 2024.

[92] Qiangwang Bei Homepage, https://www.qiangwangbei.com/, ????

[93] Cyberspace Administration of China, The Eigth Edition of Qiangwang Bei Cybersecurity Competition, https://www.cac.gov.cn/2024-10/15/c_1730681394145224.htm, 2024.

[94] Administration Commitee of Zhengzhou High-Tech Industrial Development Zone, Qiangwang Bei: Registration Notice for Youth Special Session, https://www.zzgx.gov.cn/qndt/8809446.jhtml, 2024.

[95] Government of Chenghua District, Chengdu, The 4th Geek Youth Challenge successfully concluded, https://www.chenghua.gov.cn/chqrmzf/c143758/2024-08/27/content_c654a329671242ada1a99fca8d0148e7.shtml, 2024.

[96] Chengdu Cybersecurity Series Events, Geek Youth Challenge Homepage, https://www.cdccs.cn/#/geekYouth, 2024.

[97] Chengdu Foriegn Language School (Xinjin District), Second-year high school student Zhiqi Xia has been admitted in advance to the Cybersecurity Youth Program at Sichuan University, https://mp.weixin.qq.com/s/amVtSkXS1S0Yu6R4J9sb_w, 2024.

[98] School of Cyberspace Security, Beijing University of Posts and Telecommunications, The 2nd National Cyber Security Technology Competition for Middle School Students was successfully held, https://scss.bupt.edu.cn/info/1153/2803.htm, 2019.