Department: Head
Editor: Name, xxxx@email

Bridging the Cybersecurity Skills Gap: Knowledge Framework Comparative Study

Zaina Dkaidek[ORCID: 0009-0000-6865-4201], **Awais Rashid**[ORCID: 0000-0002-0109-1341]
University of Bristol, UK

***Abstract*—Organizations worldwide face challenges in recruiting personnel with the necessary cybersecurity knowledge due to a global skills shortage. This article analyzes four knowledge frameworks — CyBOK, CSEC2017, NICE, and CST to guide educators, curriculum designers, professionals, and students in selecting the best framework for their needs.**

Introduction

The shortage of cybersecurity professionals is a pressing concern with the (ISC)2 Cybersecurity Workforce Study revealing a staggering global deficit of 4 million workers. This shortage is a multi-faceted issue, largely attributable to the scarcity of experienced personnel and lack of standardized terminology [1]. Consequently, the public, academic, and private sectors in various countries and regions have developed cybersecurity knowledge frameworks to establish a standardized language, guide educational curricula, and define workforce skills.

We explore four frameworks: the Cyber Security Body of Knowledge (CyBOK), CSEC2017 Curricular guidance by the Joint Task Force on Cybersecurity Education, National Initiative for Cybersecurity Education (NICE), and European Joint Research Centre European Cybersecurity Taxonomy (CST). These were chosen as CyBOK and CSEC2017, although respectively originating from the United Kingdom and the United States, strive to be comprehensive and globally focused, whereas NICE and CST are well established within their regions — the United States and European Union (EU) — and address more region-specific needs. Another key framework is ENISA's European Cybersecurity Skills Framework (ECSF). We decided to focus on CST instead of the ECSF as it is used for mapping competencies, hence providing a different focus from the ECSF (which is more akin to NICE in a European context).

While these frameworks share common goals, they reflect the respective priorities of the entities that developed them. CyBOK offers foundational and scientific knowledge, CSEC2017 guides global academic curricula, NICE maps workforce skills, and CST captures EU research and technology competencies. In this article, we compare these frameworks using six themes (see *Table 1*).

Published by the IEEE Computer Society

We chose the theme of *global implementation* to examine whether these frameworks can be effectively utilized beyond their countries of origin. The remaining themes were derived by collating features extracted from previous research [2, 3, 4] and the stated objectives of CyBOK, CSEC2017, NICE, and CST.

Table 1. Theme descriptions

Themes	Description
Skill set categorization	The skill sets for specific job roles are clearly defined.
Foundational knowledge	The needed topics for a fundamental and holistic comprehension of the cybersecurity domain are mapped out.
Interdisciplinarity	There is an understanding of cybersecurity's multidisciplinary nature and its need to cover various disciplines across the technical, socio-technical and policy/regulatory domains.
Guides curricula	Curriculum designers are provided guidance when creating comprehensive cybersecurity education and training programs across various levels.
Timeliness	Core concepts that are relevant to the current cybersecurity landscape and consider the field's dynamic nature are defined [2].
Global implementation	Cybersecurity curricula guidance is implementable across institutions globally.

This comparative analysis aims to elucidate each framework's strengths, limitations, and ideal use cases while considering factors like content, timeliness, and potential for global implementation. Ultimately, we seek to guide users — educators, curriculum designers, professionals, and students in the cybersecurity field — in choosing the most suitable framework based on their specific needs and objectives.

Several studies, including van Oorschot's [5], have delved into the landscape of cybersecurity knowledge frameworks, emphasizing their role in shaping education and curricula. In contrast, our analysis focuses on identifying disparities or gaps among these frameworks based on predefined themes. Therefore, this article serves as a guide to cybersecurity knowledge frameworks, helping stakeholders to navigate the landscape and providing the necessary insights to select or combine frameworks optimally based on their needs, with the ultimate goal of improving the preparedness of cybersecurity professionals.

Overview of Knowledge Frameworks

The four knowledge frameworks aim to guide stakeholders on the knowledge and skills requisite for a cybersecurity career. They function as a reference to ensure that cybersecurity training programs are comprehensive and current, and they also assist organizations in identifying necessary cybersecurity-related job roles and responsibilities. We provide an overview of the four frameworks next, with *Table 2* summarizing their update cycles and major use cases to date.

Cyber Security Body of Knowledge (CyBOK)

CyBOK is a comprehensive guide to foundational cybersecurity knowledge, developed and regularly updated since 2017 by a college of more than 115 international experts. Funded by the United Kingdom's National Cyber Security Program, CyBOK comprises 21 knowledge areas (KAs) divided into five groups. It aims to strengthen academic and professional training within the cybersecurity domain [6].

CSEC2017 Joint Task Force on Cybersecurity Education

Established in 2017 by the Joint Task Force (JTF)— a collaboration among the ACM, IEEE CS, AIS SIGSEC, and IFIP WG 11.8 — CSEC2017 guides global academic institutions seeking to devise cybersecurity degree curricula. It comprises eight KAs and 55 knowledge units, each incorporating multiple topics [7].

National Initiative for Cybersecurity Education (NICE)

NICE, a collaboration between the government, industry, and academia, is led by the U.S. Department of Commerce's National Institute of Standards and Technology (NIST). Focused on cybersecurity education, training, and workforce development, the framework encompasses seven categories with 33 specialty areas representing focused work or functions within cybersecurity [8].

European Joint Research Centre European Cybersecurity Taxonomy (CST)

Developed in 2019 by the European Commission, CST aims to unify cybersecurity definitions, terminologies, and domains. It serves

as a resource to map cybersecurity skills across EU countries. The initiative is a 3D taxonomy comprising "Research Domains," "Sectors," and "Technologies and Use Cases" [9].

Knowledge Framework Comparison

Contrasting the four frameworks on the basis of our six themes *(Table 3)*, we observe that there is no one-size-fits-all cybersecurity knowledge framework. Each framework's relevance heavily depends on the specific requirements and objectives of the user. We discuss the relative strengths and limitations of each framework next before presenting potential means for stakeholders to identify the framework that best meets their needs.

Skill Set Categorization

Understanding the skill sets required for different cybersecurity roles is vital. It equips educators to design relevant and effective training programs while allowing employers to recruit personnel with the necessary skills. CyBOK and CSEC2017 mainly focus on foundational knowledge and guiding academic curricula but can also be used to determine required cybersecurity skill sets.

CyBOK offers a framework for contrasting the depth and focus of different cybersecurity programs, assisting employers in identifying the KAs needed for specific roles and which courses or training programs may impart such knowledge. This feature has been utilized to develop certification programs in the United Kingdom, against which undergraduate and postgraduate degree programs can demonstrate their breadth and depth to particular CyBOK KAs [10]. One example of CyBOK being applied in a practical setting is through the UK Cyber Security Council — a newly formed professional body for the sector — which maps its specialisms to CyBOK for professional qualifications, enabling a rigorous knowledge-based under-pinning for the profession.

CSEC2017 overlaps significantly with NICE but is more academically oriented. While it does not capture the cybersecurity skill sets required in specific sectors, its extensive coverage of cybersecurity subdomains can aid employers in determining the necessary skill sets for personnel recruitment.

NICE offers an extensive mapping of the cybersecurity skills necessary for various job roles. This industry-oriented approach guides educational institutions and firms in supporting, training, and developing suitable professionals. NICE's practicality is evidenced by several professional-level courses and certifications aligning with the framework's specialty areas (cf. *Table 2*), which in turn enables better strategic workforce planning and hiring, thereby improving an organization's cybersecurity posture.

CST includes two professional-oriented dimensions: "Sectors" and "Technologies and Use Cases," which focus on cybersecurity industries and applications. These dimensions aim to identify the types of knowledge and skills generally needed for each industry and its specific technologies and use cases. However, according to the taxonomy's creators, the "Research Domains" are universally applicable across all sectors and technologies or use cases. Conversely, NICE goes a step further by providing a detailed list of specific skills required for each job role. As a result, CST is less comprehensive than NICE when it comes to delineating the skill sets needed for particular positions. However, as can be seen in *Table 2*, CST was instrumental in mapping EU cybersecurity capacities, which is crucial when determining the skills required within the field.

Foundational Knowledge

In the context of foundational knowledge, these frameworks should provide educators with a guide to ensure that students understand the cybersecurity domain comprehensively. CyBOK is designed to provide a comprehensive guide to foundational cybersecurity knowledge. It is divided into KAs that provide curriculum designers with foundational materials and sources. CyBOK's KAs cover numerous cybersecurity topics, including human, organizational, and regulatory aspects, attacks and defenses, systems security, infrastructure security, and software and platform security. By focusing on foundational knowledge, CyBOK aims to provide a holistic understanding of the cybersecurity domain, which is essential for educators and students to map out a coherent path of progression through the discipline.

CSEC2017 covers traditional cybersecurity

Table 2. Framework updates and use-cases

Framework	Updates	Major Use-Cases
CyBOK	**2019**: CyBOK version 1.0.0 with 19 KAs is launched. **2021**: CyBOK version 1.1.0 is released with two new KAs: applied cryptography and formal methods for security.	• This is part of the UK government's professionalization strategy for cybersecurity. • This underpins the certification scheme by NCSC for undergraduate and postgraduate degree programs in the United Kingdom [10]. • This forms the basis of the specialisms defined by the UK Cyber Security Council (a new professional body).
CSEC2017	**2017**: CSEC2017 launched. **2020**: Cyber2yr2020, an expansion of CSEC2017 but for associate degrees (two-year programs), launched.	• Several educational institutions in the US utilize CSEC2017 to guide their curricula for relevant subjects. • The expanded version of the framework, Cyber2yr2020, is being utilized by programs in a number of community colleges in the United States.
NICE	**2020**: Draft revision released. **2020**: NIST SP 800-181 Revision 1, the Workforce Framework for Cybersecurity released. **2021**: Draft NISTIR 8355, NICE Framework Competencies announced. **2023**: New proposed Work Role on Insider Threat.	• Several education programs, such as those targeting Pre-K-12 students, align their courses with the NICE framework work roles. • Several professional-level courses align with the framework's specialty areas such as the courses available in the NICCS Education and Training catalog. • Certifications such as CertNexus, based on the NICE framework, provide organizations with a way to identify cybersecurity skill gaps within their teams or to certify their expertise.
CST	**2019**: Formal proposal for CST published. **2021**: CST updated.	• This is the basis for the mapping of EU cybersecurity capacities, which supported the proposal for establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres, a legislative initiative under negotiation between the European Parliament and Council.

academic research sub-domains and conveys fundamental principles. It provides an extensive overview of foundational knowledge by covering topics such as cryptography, network security, and software security to ensure that students understand the theoretical underpinnings of cybersecurity and develop the critical thinking skills needed to tackle the field's complex challenges.

NICE, as a skills framework, is more career focused, and students learn the essential skill sets for their careers. Consequently, NICE does not provide an extensive compilation of foundational cybersecurity KAs. Instead, it encourages employees and students to learn job-specific skills. This focus makes NICE more prescriptive than the other frameworks, but it ensures that learners acquire the skills needed to succeed in their roles.

CST's creators aimed to build a cybersecurity realm of knowledge that includes competencies, definitions, and concepts from both traditional academic cybersecurity and beyond. By incorporating these core KAs, CST ensures that learners gain a fundamental understanding of the cybersecurity domain. However, CST's primary focus is on mapping sector-specific competencies across the EU to aid in classifying and analyzing potential European projects and policy initiatives rather than providing lists of foundational knowledge.

Interdisciplinarity

The complex nature of cyber threats and the need for multifaceted solutions require an interdisciplinary approach to cybersecurity, involving expertise and knowledge from various fields, including technical fields such as computer science and electronics engineering and nontechnical areas like psychology, law, sociology, criminology, and economics. CyBOK and CSEC2017 both cover a broad range of technical topics such as cryptography, network security, and software

Table 3. Framework comparison based on themes

Themes	CyBOK	CSEC2017	NICE	CST
Skill Set Categorization	Guides professional training by supplying the foundational knowledge needed to work within the cybersecurity sector.	Provides curricula guidance concerning fundamental cybersecurity subdomains to help prepare students for the workforce.	Industry-oriented and delivers detailed guidance regarding the skill set needed for a specific career.	Maps cybersecurity skills across different industries and captures European sectorial competencies.
Foundational Knowledge	Provides a comprehensive guide to foundational cybersecurity knowledge.	Extensively covers traditional cybersecurity academic research subdomains.	Details the skills needed for a specific job.	Defines foundational cybersecurity knowledge, concepts and definitions.
Interdisciplinarity	Provides broad coverage of different topics, particularly the more technical ones.	Provides broad coverage of different topics, particularly the more technical ones.	Encourages students and employees to gain the skill set for their specific careers.	The "Research Domains" dimension provides good coverage of the operational subdomains but lacks in the technical subjects.
Guides the Creation of Curricula	Offers foundational knowledge to build curricula and compare programs across various educational levels, including secondary, undergraduate, postgraduate, and professional development.	This is a qualification-based knowledge framework that helps education and training programs specify what content is required for cybersecurity education programs.	Addresses general cybersecurity awareness, formal education (post-secondary education), professional training, and workforce structure.	Supplies basic cybersecurity concepts and EU competencies to guide academic curricula.
Timeliness	Provides established foundational cybersecurity concepts and regularly updated to incorporate new KAs that reflect the current state of knowledge and emerging needs.	This is a solid foundational knowledge base of traditional cybersecurity subdomains.	Details required skills for the current United States labor market.	Captures foundational cybersecurity knowledge, concepts and definitions; it is also flexible and modified to keep pace with the rapidly changing domain.
Potential Global Implementation	Focuses on foundational knowledge allowing for global implementation.	Developed for global implementation.	Reflects the U.S. cybersecurity landscape.	Built around the European landscape and competencies.

security as well as nontechnical areas like human, organizational, and regulatory factors.

NICE does not cover some critical cybersecurity areas, like the physical layer, cyberphysical systems, hardware security, human factors, and web and mobile security. Nonetheless, the "Specialty Areas" within the NICE framework cover a range of technical and nontechnical fields, including software development, legal advice and advocacy, incident response, and digital forensics.

CST underlines the importance of protecting individuals and society by viewing cybersecurity through education, policies, privacy, and cultural perspectives. However, the technical areas covered in the "Research Domains" dimension are relatively limited compared to CyBOK and CSEC2017.

Guides Curricula

To shape and cultivate cybersecurity curricula effectively, a framework must facilitate a shared understanding among all stakeholders and ensure a uniform language for cybersecurity education, training, and workforce development. This is crucial in harmonizing skill development with cybersecurity demands, bridging the divide between academia and industry.

CyBOK offers a comprehensive guide to developing a multidisciplinary cybersecurity curriculum. It provides foundational knowledge and a common framework that compares programs across different educational levels, such as sec-

ondary, undergraduate, postgraduate, and professional development. Unlike CSEC2017, which adheres to a strict curriculum guide, CyBOK enables flexibility in the depth of knowledge required for each topic. Moreover, the successful practical implementation of CyBOK is evident in its use as a certification framework for various university-level programs at a national level through the National Cyber Security Centre (NCSC) certification program [10]. Furthermore, CyBOK's Mapping Framework, available on its website, aids curriculum designers in aligning their degree content with the framework, which has been applied to a multitude of professional certification programs.

CSEC2017 is a qualification-based knowledge framework that outlines the discipline's boundaries and the essential dimensions of education curricula. It can guide designers of an entire curriculum or course syllabus at the postsecondary level. It provides consistency and stability while being flexible to a program's needs, grounded in fundamental principles. This framework has been proven to be usable in practice with several educational institutions, including George Washington University, El Paso Community College, and Consumnes River College, which utilize it to guide their curricula for relevant subjects.

NICE emphasizes general cybersecurity awareness, formal education, professional training, and workforce structure. This framework eases the process for curriculum designers collaborating with the private sector to develop courses based on industry needs by providing a common lexicon. A standard language reduces the difficulty for curricula designers to work with the private sector when deciding on courses based on industry needs. Several programs (as shown in *Table 2*), align their courses with the NICE framework work roles. Nonetheless, although NICE has had several successful implementations in guiding curricula, its primary aim is to provide specific skill sets for individual job roles, which could leave graduates lacking in broader cybersecurity competencies.

CST's alignment of definitions, terminologies, and domains with established EU cybersecurity centers and competencies can guide academic curricula effectively. By having students, instructors, and curricula designers map the "Research Domains" to the "Sectors" and "Technologies and Use Cases," one can better plan the courses that need to be available or taken to ensure that future personnel have the cybersecurity skills and knowledge required for a specific sector or application. Nonetheless, the issue with the approach taken by NICE and CST is that students and professionals gain only a narrow view of cybersecurity by focusing on a particular career or sector regarding education. Cybersecurity involves a multiplicity of disciplines, and if personnel do not have a holistic understanding of the domain, it will be more challenging to combat potential cybersecurity problems.

Timeliness

Assessing the timeliness of cybersecurity frameworks is challenging as the discipline continues to evolve as new technologies and threats emerge. Therefore, this article established its timeliness perspective from the definition of Parekh et al. [2]. They explain that a cybersecurity framework is considered timely if it can identify core concepts within the current technology landscape. To elaborate on the timeliness of the different frameworks, it is essential to note that technological change in cybersecurity is rapid and constant. As a result, frameworks that are not updated regularly can become outdated quickly and may not reflect the current state of knowledge and emerging needs.

CyBOK was last updated in 2021. It has an open change proposal process that enables the community to propose changes to existing KAs or propose new ones to reflect the present state of knowledge in the domain. The CyBOK Executive Board regularly reviews proposals for updates, ensuring that the framework stays up to date with the field's latest trends and developments.

The framework designers then plan to implement these updates regularly. This approach ensures that the framework can help identify relevant core concepts within current technology, making it a timely and relevant resource for cybersecurity education and training.

In contrast, CSEC2017 may not be as timely in keeping pace with the fast-evolving technology developments. CSEC2017, for example, provides a solid foundational knowledge base, but its relatively fixed nature may not update consistently to

keep up with rapidly changing technology trends. It is not scheduled for regular updates but was expected to be reviewed within five years of the publication dates to ensure that it remains relevant. We did not find any public information indicating if the review had taken place, nor did we find any reports on the outcomes of such a review.

NICE, on the other hand, stays current with the skills required by the U.S. cybersecurity workforce. NICE was last updated in 2023, and its updates are based on the cybersecurity workforce's needs and priorities.

CST offers a foundational knowledge base, concepts, and definitions, which can be modified and adapted to keep up with the rapidly changing cybersecurity domain. This adaptability allows for the integration of newly emerging KAs and technology trends when required. CST was last updated in 2021 and is planned to be reviewed and updated regularly to reflect changes in the cybersecurity landscape. However, specific update timelines have not been defined.

Global Implementation

The capacity to implement a cybersecurity framework globally is crucial as cyber threats are not confined to specific geographic regions. CyBOK's flexibility and adaptability make it suitable for global implementation. It provides a common language and a shared understanding of cybersecurity, enabling the development of multi-disciplinary curricula tailored to different countries' education systems. Also, the CyBOK project involved an international team of experts and was designed to be adaptable to other education systems worldwide. At the same time, the mapping framework provides resources for curriculum designers to map their degree contents, making it easier to execute in other regions.

Similarly, CSEC2017 was designed to guide cybersecurity curricula globally and provides a qualification-based knowledge framework that can be implemented across different countries. The framework's creators organize community engagement activities to gather insights from experts globally. Even during the key milestones in the CSEC2017 development process, activities such as a global stakeholder survey and international workshops were conducted. As global community engagement was a priority when developing CSEC2017, it can be adaptable to different education systems worldwide.

On the other hand, NICE's emphasis on skill sets is more specific to the U.S. cybersecurity landscape and may not be easily incorporated into other countries' education systems. For example, it does not capture the particular idiosyncrasies of the European outlook regarding the identified sectors as well as the law and regulation context. At the same time, CST is centered around the European landscape and competencies. Therefore, while NICE and CST may be suitable for their respective regions, they may have limitations in global applicability. However, NICE and CST can serve as a precedent for other countries.

Guidance and Recommendations

Guidance for users

The comparison of the strengths of each framework, such as their global implementation potential and timeliness, can be used by users to identify the most fitting framework for their needs. In this regard, we distill a heat map (*Figure 1*) that highlights the strengths and limitations of each framework along the six thematic categories. For instance, CyBOK excels in *foundational knowledge*, *guides curricula*, and *global implementation*. This makes it particularly effective for developing academic and professional courses, including those beyond its country of origin. In contrast, CSEC2017 also shows robustness in *foundational knowledge*, *guides curricula*, and *global implementation*, aligning with its purpose of shaping academic curricula worldwide. However, it is limited in terms of *timeliness*, given its less frequent updates. In the ever-evolving field of cybersecurity, where new technologies and threats constantly emerge, frequent updates are essential.

NICE is particularly beneficial for individuals pursuing specific cybersecurity career paths, offering detailed insights into the skills required for various job roles. While CyBOK is less detailed in this aspect, its emphasis on *foundational knowledge* is vital for organizations seeking to understand the skills necessary from their workforce as a whole to secure their networks. Furthermore, though NICE scores high in *guides curricula*, its approach differs from CyBOK and CSEC2017,

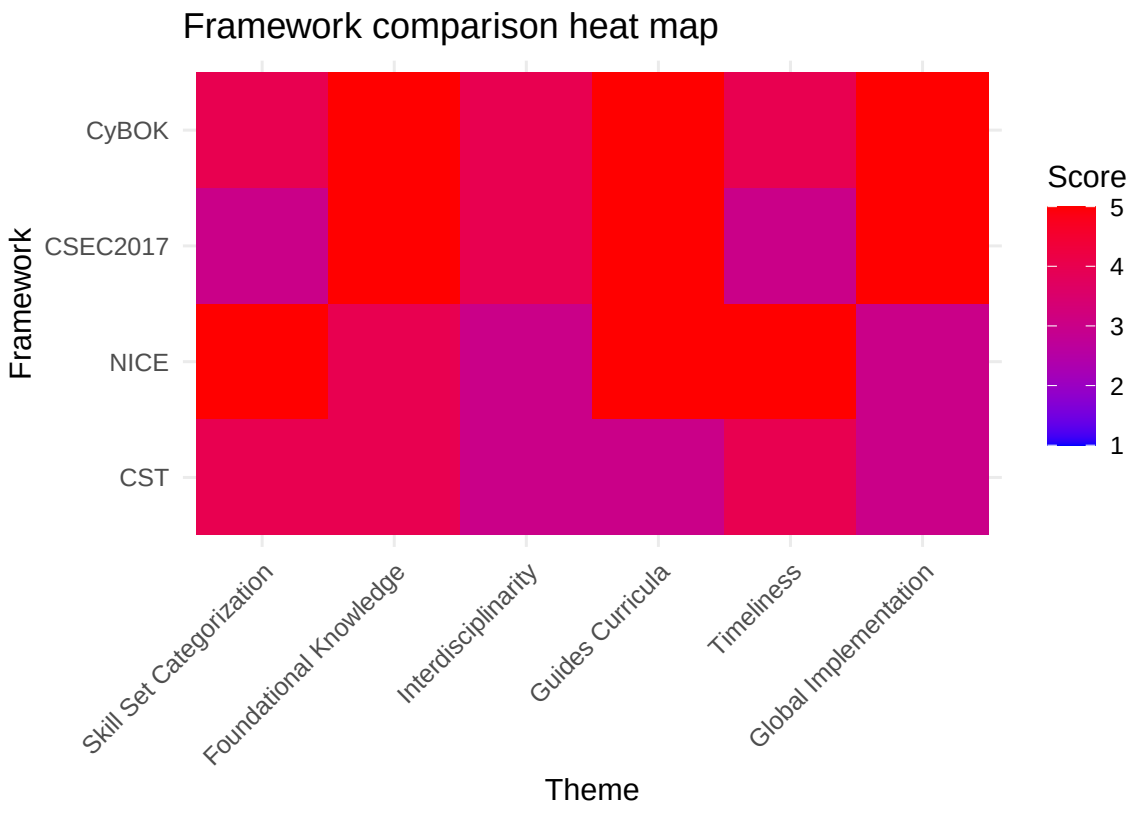

Figure 1. Heat map comparing how each framework follows the themes

being more prescriptive. Nonetheless, this does not diminish its efficacy in curriculum guidance, especially for courses and students focusing on specialization.

CST's objectives are not fully encapsulated by these themes. Its comprehensive nature is geared toward mapping sector-specific cybersecurity skills in Europe and identifying skill gaps. CST is strong in *foundational knowledge*, establishing a standardized cybersecurity lexicon. Also, its focus on *skill set categorization* is noteworthy as it aims to address European cybersecurity skill and knowledge gaps.

Recommendations

Our overarching recommendation for current and future framework designers is to provide comprehensive information about their frameworks' strengths, usage guidelines, goals, and target audience. This includes being transparent about their framework's limitations and acknowledging the existence of other frameworks that may better serve certain needs. Providing comprehensive information about each framework will not only enhance its usability but also contribute to the growth of cybersecurity education and workforce training globally.

Moreover, research should strive to quantify the benefits of each framework, align them with specific cybersecurity areas, and provide clarity on the value each framework brings. Designers should also be more explicit about their frameworks' goals, strengths, limitations, and ideal use cases to increase their utility. A single framework cannot meet every need, but multiple frameworks can complement each other. Comparisons such as ours or future indexes could serve as valuable resources to facilitate this integration.

The cybersecurity workforce gap is a recurring and pressing concern globally. Multiple efforts, such as the four frameworks above, are being made to address this issue. The benefits of these efforts will only be maximized through a clearer understanding of their respective

strengths, limitations, and complementarity. The comparison provided in this article serves as a stepping stone towards a more targeted application of each framework depending on sector, application, or user needs.

Acknowledgement

This work was supported by CyBOK, funded by the United Kingdom's National Cyber Security Programme.

References

1. (ISC)², "(ISC)2 cybersecurity workforce study: How the economy, skills gap and artificial intelligence are challenging the global cybersecurity workforce," Report, 2023. [Online]. Available: https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2_Cybersecurity_Workforce_Study_2023.pdf?rev=28b46de71ce24e6ab7705f6e3da8637e
2. G. Parekh, D. Delatte, G. L. Herman, L. Oliva, D. Phatak, T. Scheponik, and A. T. Sharman, "Identifying core concepts of cybersecurity: Results of two delphi processes," *IEEE Transactions on Education*, vol. 61, no. 1, pp. 11–20, 2018.
3. S. Cooper, C. Nickell, L. C. Pérez, B. Oldfield, J. Brynielsson, A. G. Gökce, E. K. Hawthorne, K. J. Klee, A. Lawrence, and S. Wetzel, "Towards information assurance (ia) curricular guidelines," in *Proceedings of the 2010 ITiCSE Working Group Reports*, ser. ITiCSE-WGR '10. New York, NY, USA: Association for Computing Machinery, 2010, p. 49–64. [Online]. Available: https://doi.org/10.1145/1971681.1971686
4. W. Wei, A. Mann, K. Sha, and T. A. Yang, "Design and implementation of a multi-facet hierarchical cybersecurity education framework," in *2016 IEEE Conference on Intelligence and Security Informatics (ISI)*. IEEE, 2016, pp. 273–278.
5. P. C. van Oorschot, "Coevolution of security's body of knowledge and curricula," *IEEE Security & Privacy*, vol. 19, no. 5, pp. 83–89, 2021.
6. CyBOK, "Knowledgebase – cybok v1.1," 2021. [Online]. Available: https://www.cybok.org/knowledgebase1_1/
7. "Cybersecurity curricular guidelines: Csec2017," 2017. [Online]. Available: https://cybered.hosting.acm.org/wp/
8. NIST, "Nice framework resource center," 2020. [Online]. Available: https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center
9. JRC, "European cybersecurity taxonomy," 2019. [Online]. Available: https://joint-research-centre.ec.europa.eu/jrc-news/european-cybersecurity-taxonomy-2019-11-28_en
10. L. Nautiyal, A. Rashid, J. Hallett, B. Shreeve, K. Michael, E. Chris, and H. Catherine, "The united kingdom's cyber security degree certification program: a cyber security body of knowledge case study," *IEEE Security & Privacy*, vol. 20, no. 1, pp. 87–95, 2022.