ITUPublications

International Telecommunication Union
Development Sector

A systems approach to understanding national cybersecurity education capacity

OAS More rights for more people

ITU

A systems approach to understanding national cybersecurity education capacity

OAS More rights for more people

Acknowledgements

The 'A Systems Approach to Understanding National Cybersecurity Education Capacity' research paper has been developed through the joint effort of the International Telecommunication Union (ITU) and the Organization of American States (OAS) and is shared with the global community to assist countries in their efforts to build secure, sustainable, and resilient digital societies.

Disclaimer

The designations employed and the presentation of the material in this publication do not imply the expression of any opinion whatsoever on the part of ITU or OAS concerning the legal status of any country, territory, city or area or of its authorities, or concerning the delimitation of its frontiers or boundaries. The mention of specific companies or of certain manufacturers' products does not imply that they are endorsed or recommended by ITU or OAS in preference to others of a similar nature that are not mentioned. Errors and omissions excepted, the names of proprietary products are distinguished by initial capital letters.

All reasonable precautions have been taken by ITU or OAS to verify the information contained in this publication. However, the published material is being distributed without warranty of any kind, either expressed or implied. The responsibility for the interpretation and use of the material lies with the reader. The opinions, findings and conclusions expressed in this publication do not necessarily reflect the views of OAS, or ITU or its membership.

ISBN

978-92-61-39031-0 (Electronic version)
978-92-61-39041-9 (EPUB version)
978-92-61-39051-8 (MOBI version)

Please consider the environment before printing this report.

Table of contents

List of boxes, figures and tables

Boxes

Figures

Tables

Foreword

The International Telecommunication Union (ITU) has a long-standing history of collaboration with the Organization of American States (OAS) on digital transformation initiatives. Both ITU and OAS prioritize a human-centric approach to digital transformation, recognizing that sustainable and resilient ICTs depend on people equipped with the necessary skills and knowledge to manage and operate technology.

This framework, designed to help countries understand and navigate their unique cybersecurity ecosystems, emerged from the recognition of the need for a more comprehensive approach to cybersecurity capacity development. By fostering a deeper understanding of the cybersecurity education ecosystem, this approach aims to balance immediate workforce gaps with long-term requirements, ensuring sustained cybersecurity resilience.

We hope this paper will serve as a significant step forward in helping countries adopt a holistic approach to cybersecurity capacity development. By leveraging this framework, countries can make strategic investments in their cybersecurity workforce, fostering collaboration between governments and stakeholders to bridge skills deficits and optimize resource allocation.

Dr Cosmas Luckyson Zavazava
Director of the Telecommunication Development Bureau
International Telecommunication Union

A Systems Approach to Understanding National Cybersecurity Education Capacity

PURPOSE AND INTENDED AUDIENCE

To close the global cybersecurity workforce gap and continue institutionalizing an approach to a structured process for a cybersecurity workforce, it is important to further develop national cybersecurity education capacity in all countries around the world. This research paper looks at existing research in national cybersecurity education capacity and explores the application of a 'systems approach' to guide future cybersecurity education capacity development, using systems thinking tools to build a holistic understanding of the national cybersecurity education capacity landscape. This research paper is aimed at stakeholders working across government, private sector, academia, and civil society that are interested in how a systems approach can improve the understanding of national cybersecurity education landscapes and guide the design and implementation of future capacity development interventions, with particular application to low-and-middle income countries. Informed by secondary sources, this paper intends to initiate a broader discussion and further research on the benefits and applications of a systems approach to cybersecurity education capacity development.

LITERATURE REVIEW

SUPPLY-SIDE CHALLENGES

- Lack of awareness and aspiration for cybersecurity careers and unclear career pathways.
- Underutilization of full labor market potential, with women underrepresented in cybersecurity education programs.
- Need to increase the availability and accessibility of a range of cybersecurity education and training pathways.
- Need for greater alignment of cybersecurity education competencies with industry needs.
- Difficulties encountered for education offerings to keep up to date due to rapid pace of change in cybersecurity.
- Lack of educator expertise and resources to deliver cybersecurity education at scale.
- Lack of capacity to address cybersecurity education in the context of competing national development priorities.

DEMAND-SIDE CHALLENGES

- Demand for cybersecurity competencies is rapidly growing and outpacing supply, not just for building a cybersecurity workforce, but for building a cybersecure society.
- Cybersecurity workforce requirements vary by country context, with different needs, environments, cultures, and resources influencing cybersecurity education.
- Need for greater clarity in defining and communicating cybersecurity industry requirements for labor.
- High entry-level requirements for cybersecurity roles make it difficult for aspiring cybersecurity professionals to enter the cybersecurity workforce.
- Employers' underinvestment in the necessary resources and ongoing training of cybersecurity workforce.

A review of five leading frameworks for assessing national cybersecurity capacity identified five components of national cybersecurity education capacity: including School Curricula and Programs, Tertiary Education and Research, Training and Certification, Awareness and Culture, and Administration and Governance.

SYSTEMS APPROACH TO NATIONAL CYBERSECURITY EDUCATION CAPACITY BUILDING

Adaptations of a select set of tools to the problem of low national cybersecurity education capacity are presented to explore their utility in building a holistic understanding of the system.

A **Problem Tree** provides a high-level visual representation of some of the causes and effects of the problem of low levels of cybersecurity education capacity.

The **Stakeholder Analysis** provides an indicative list of stakeholders and maps their varying levels of interest and roles in national cybersecurity education capacity

The **Systems Concept** provides a a high-level representation of national cybersecurity education capacity as a system. The system concept takes into consideration the five components of national cybersecurity education capacity identified in this paper and situates them within the context of the overall system environment, illustrating potential interrelationships between the system components.

RECOMMENDATIONS, NEXT STEPS, AND FUTURE RESEARCH

Recommendations include guidance for countries to inform their approach to building national cybersecurity education capacity as well as a checklist of short-to-medium and medium-to-long term interventions that countries can consider as part of future capacity building efforts. **Next steps** to build on this work, as well as areas for **future research** are proposed.

1 Introduction

Background

Cybersecurity continues to be a key challenge to the ongoing stability, safety, and productivity of the global economy. In 2020, the World Economic Forum *"concluded that, while progress has been made in improving cybersecurity across the ecosystem, the increased complexity, pace, scale and interdependence shown by our forward look at technological trends will overwhelm many current defenses. Without interventions now, it will be difficult to maintain the integrity of and trust in the emerging technology on which future global growth depends."*[1]

Despite advancements in cybersecurity education and other capacity development activities, a persistent disparity of low supply and high demand exists in the global cybersecurity workforce. Supply and demand pressures have been exasperated by the unprecedented disruptions to organizations, technologies, and communities following the COVID-19 pandemic, and the rapid transition to remote work, the heightened dependence on digital technologies, and the increased digital footprints of most countries. In addition, the geo-political landscape, ongoing economic digital transformation efforts, and uncertainties around emerging technologies such as AI have all contributed to an evolving digital risk and threat environment that places pressure on the resiliency and efficacy of cybersecurity workforces.[2] The International Information System Security Certification Consortium, Inc. (ISC2) estimated in 2022 that the global cybersecurity workforce had reached 4.7 million people and that the world needed a further 3.4 million cybersecurity professionals to cope with the growing number of threats and challenges.[3]

Cybersecurity workforce challenges are more acute in low- and middle-income countries where limited resources are stretched across a range of policy priorities, and it is therefore critical to use and deploy available resources efficiently and build on existing capacity as part of the broader development context.

Given the size of the cybersecurity challenge and need for effective investment, there is an opportunity for education and broader digital literacy efforts to play a key role in mainstreaming cybersecurity in national and global development contexts. This can help to facilitate the achievement of the 2030 Agenda for Sustainable Development and provide a driving force for Sustainable Development Goal 4 on quality education[4] by equipping both young people and adults with the knowledge, and technical and vocational skills, to thrive in an increasingly digitalized world.[5]

---

1 World Economic Forum. (2020). Future Series: Cybersecurity, emerging technology and systemic risk. http://www3.weforum.org/docs/WEF_Future_Series_Cybersecurity_emerging_technology_and_systemic_risk_2020.pdf

2 World Economic Forum. (2022). Global Cybersecurity Outlook 2022 – Insight Report. https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2022.pdf

3 (ISC)² Cybersecurity Workforce Study 2022 https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2-Cybersecurity-Workforce-Study-2022.pdf

4 United Nations. (2023). SDG 4 Quality Education. https://sdgs.un.org/goals/goal4

5 UNICEF. (2021). Digital Literacy in Education Systems Across ASEAN. https://www.unicef.org/eap/media/7766/file/Digital%20Literacy%20in%20Education%20Systems%20Across%20ASEAN%20Cover.pdf

Report structure

To reduce the global cybersecurity workforce deficit, it is important to further develop national cybersecurity education capacity in all countries around the world. This study looks at existing research in national cybersecurity education capacity and explores the application of a 'systems approach' to guide future cybersecurity education capacity development. A systems approach, explored in section 3, seeks to address complex policy challenges by using a holistic design methodology, which considers how individual elements work together and how they are impacted in context.[6] This study explores the application of a systems approach to guide future cybersecurity education capacity development by:

- identifying and describing current research on the challenges and characteristics of national cybersecurity education capacity;
- exploring how a systems approach can support the understanding and development of cybersecurity capacity;
- adapting systems thinking tools for consideration in the conceptualization of national cybersecurity education capacity as a system; and
- outlining recommendations for national cybersecurity education capacity building.

Policy-makers need to understand the cybersecurity education ecosystem before they can address critical needs and remove barriers to cybersecurity education. Building on the work of the Global Forum on Cyber Expertise (GFCE) Working Group D[7], this study outlines a cybersecurity education capacity systems concept.

Intended audience

This study is aimed at stakeholders working across government, private sector, academia, and civil society who are interested in how a systems approach can improve the understanding of national cybersecurity education landscapes and guide the design and implementation of future capacity development, with particular application to low- and middle-income countries. It is hoped that the contents of this study will initiate broader discussions and further research by Member States on the benefits and applications of a systems approach to cybersecurity education capacity development.

Scope

The analysis of cybersecurity capacity must reflect the diversity of conditions, composition, and priorities of capacity and workforce development goals to determine the suitability of a systems approach to varying national contexts. Although this study highlights the complexity and the importance of understanding the interrelationship of components across national cybersecurity education capacity systems, it is not intended to be a comprehensive analysis of such systems. It is hoped, however, that by exploring the application of a systems approach, stakeholders can draw on these ideas and concepts as part of their efforts to understand and strengthen national cybersecurity education capacity.

---

6 OECD. (2017). Systems Approaches to Public Sector Challenges. https://www.oecd.org/publications/systems-approaches-to-public-sector-challenges-9789264279865-en.htm

7 GFCE Working Group D: Cyber Security Culture and Skills. (2019). White Paper: Task Force on Cybersecurity Professional Training and Development. https://cybilportal.org/wp-content/uploads/2020/02/GFCE-WG-D-White-Paper-Task-Force-on-Cybersecurity-Professional-Training-and-Development.pdf

2 Review of cybersecurity education capacity

This section presents an overview and provides the scope and key elements of existing national cybersecurity education capacity research including academic journals, frameworks and guides, policy and industry papers, and websites. The criteria for the selection of these resources included:

- recency: publication in the last eight years (2016 to 2023);
- diversity of publication type: ensuring diversity of source type by including nine academic journal articles, seven frameworks and guides, and thirteen policy/industry papers, and one research centre website;
- diversity of author: representation of both government and non-government authors;
- diversity of geography, which included authors from Africa, the Americas, Asia-Pacific, and Europe regions.

2.1 Defining key terms

For the purpose of this study, this section defines key terms to serve as reference points for the topics explored.

Cybersecurity can be described as *"the collection of tools, policies, guidelines, risk management approaches, actions, trainings, best practices, assurance and technologies that can be used to improve the capability and capacity to protect the availability, integrity and confidentiality of assets in the connected infrastructures pertaining to government, private organizations and citizens; these assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and data in the cyber-environment."*[8]

This comprehensive and broad reaching perspective of cybersecurity is aligned to Parrish et al (2018), who define the field of cybersecurity education as a meta-discipline that incorporates ideas and constructs from a range of disciplines including aspects of law, policy, human factors, ethics, and risk management.[9] The selection of this definition acknowledges cybersecurity as a holistic concept and effectively captures the complexity of cybersecurity and its diverse elements.

National cybersecurity capacity

National cybersecurity capacity can be considered as a broad measurement of the extent to which a country has established resilience to cyber risks and threats across government, the private sector, and civil society. According to the Cybersecurity Capacity Maturity Model for Nations (CMM),[10] cybersecurity is comprised of five dimensions which, together, constitute national cybersecurity capacity:

- developing cybersecurity policy and strategy;
- encouraging responsible cybersecurity culture within society;

---

8 The International Telecommunication Union, The World Bank, Commonwealth Secretariat, the Commonwealth Telecommunications Organisation, NATO Cooperative Cyber Defence Centre of Excellence. (2018) Guide to Developing a National Cybersecurity Strategy – Strategic engagement in cybersecurity

9 Parrish, A., Impagliazzo, J., Raj, R. K., Santos, H., Asghar, M. R., Jøsang, A., ... & Stavrou, E. (2018). Global perspectives on cybersecurity education for 2030: a case for a meta-discipline. In Proceedings Companion of the 23rd Annual ACM Conference on Innovation and Technology in Computer Science Education

10 Global Cyber Security Capacity Centre. (2023). Assessing National Cybersecurity Capacity. https://gcscc.ox.ac.uk/cmm-dimensions-and-factors

- building cybersecurity knowledge and capabilities;
- creating effective legal and regulatory frameworks; and
- controlling risks through standards and technologies.

National cybersecurity capacity building

According to the European Commission, cybersecurity capacity building includes *"all types of activities (e.g. human resources development, institutional reform or organizational adaptations) that safeguard and promote the safe, secure and open use of cyberspace."*[11]

Exploring this idea further, Pawlak & Barmpaliou state that *"cybersecurity capacity building has been described as increasing resilience against cybersecurity threats through the implementation of different policies, including the development of NCS and CSIRTs, as well as education and awareness initiatives (Calderaro & Craig, 2020). In this way, cybersecurity capacity building includes three main dimensions: developing individual capacities, strengthening institutional structures, and designing policy frameworks."*[12]

Elsewhere, Collett notes that *"international cybersecurity capacity building emerged in the mid- 2000s as a mechanism for countries and organisations to assist each other, across borders, in protecting the safe, secure and open use of the digital environment."* Collett further states that such mechanisms should focus less on donor-beneficiary frameworks and more on multidirectional, multistakeholder partnerships where the global public, private, and civil society sectors can work together to help countries build cybersecurity capacity.[13]

Cybersecurity education capacity

The role of education is a key part of overall efforts to strengthen national cybersecurity capacity and it can be defined as "*the administration and governance of cybersecurity education programmes and initiatives, and their accessibility and suitability across society, including awareness-raising, formal and informal learning, vocational and professional training pathways, and the building of knowledge and capabilities through research and development."*[14]

National cybersecurity education capacity building

Building on the definitions above, national cybersecurity education capacity building can be defined as "*all types of activities with the aim of increasing the ability of a nation to develop cybersecurity knowledge, skills and abilities across society."*

Knowledge, skills, abilities and competencies

In the context of national cybersecurity education capacity building, definitions of knowledge, skills, abilities, and competencies are based on those provided in the national initiative for

---

[11] European Commission. (2018). Operational Guidance for the EU international cooperation on cyber capacity building. https://www.iss.europa.eu/content/operational-guidance-eu%E2%80%99s-international-cooperation-cyber-capacity-building

[12] Patryk Pawlak & Panagiota-Nayia Barmpaliou, 2017. "Politics of cybersecurity capacity building: conundrum and opportunity," Journal of Cyber Policy, Taylor & Francis Journals, vol. 2(1), pages 123-144, January.

[13] Collett, R. (2021). Understanding cybersecurity capacity building and its relationship to norms and confidence building measures. Journal of Cyber Policy, 6:3, 298-317, https://doi.org/10.1080/23738871.2021.1948582

[14] Adapted from Global Cyber Security Capacity Centre. (2023). Assessing National Cybersecurity Capacity. https://gcscc.ox.ac.uk/cmm-dimensions-and-factors

cybersecurity education (NICE) cybersecurity workforce framework.[15] Knowledge, skills, and abilities are the attributes required to perform work roles or practices that are generally demonstrated through relevant experience, education, or training:

- knowledge is a body of information applied directly to the performance of a function;
- skill is often defined as an observable competence to perform a learned act;
- ability is the competence to perform an observable behaviour or a behaviour that results in an observable product or outcome;
- competencies are defined as the potential to use knowledge, skills, abilities, behaviours, and personal characteristics to successfully perform tasks, specific functions or practices, or operate in a given role or position.

2.2 Building education capacity

This section outlines key considerations when building national cybersecurity education capacity and presents the complexity and multi-faceted nature of capacity building as well as the challenges typically experienced by countries when addressing low capacity. It includes an overview of maturity and readiness indicators drawn from leading cybersecurity capacity assessment frameworks, what a country needs to consider, and the typical stages in the capacity building process.

[15] National initiative for cybersecurity education (NICE) cybersecurity workforce framework. NIST special publication, 800(2017)

Women in the cybersecurity workforce

Although there is a growing effort to address the lack of women in the cybersecurity workforce, there remains a significant gender gap in the cybersecurity sector. According to ISC2, women hold only 25 per cent of cybersecurity jobs globally,[1] with an expected increase to 30 per cent by 2025 and 35 per cent by 2031.[2] This gap is even more pronounced in top cybersecurity positions, with only 17 per cent of chief information security officer roles being filled by women.

The gender gap is caused by various factors, including intersectional discrimination, lack of awareness, and insufficient encouragement for girls to consider cybersecurity as a career option. Gender stereotypes are also a significant obstacle, with STEM careers often being viewed as unappealing to women. In addition, women working in the cybersecurity industry face unique challenges, including a lack of career growth opportunities, sparse recognition from their colleagues, managers and company leadership, and a lack of gender-inclusive policies.[3]

Tackling the gender gap in cybersecurity requires a comprehensive and multi-faceted approach that takes into account the intersectional discrimination that women face in this field. Focusing solely on statistics is not enough; there is a need to recognize the complex set of challenges that women encounter in their personal and professional lives. To address this issue, some strategies that can be implemented include collaborating with schools to create programmes targeted at girls and adolescents to improve their understanding of STEM careers, training teachers on how to encourage girls to excel in these fields, promoting cybersecurity clubs for women in schools, introducing female role models to students, and offering more scholarships, internships, and upskilling opportunities for women to join and succeed in cybersecurity roles.

It is also important to create an inclusive culture that prevents women from being forced out of the industry. Instead of asking women to conform to a male-dominated cybersecurity industry, the industry itself needs to change and become more welcoming to women.[4] This has been a long-standing issue that needs to be addressed to make progress towards a more equitable and diverse industry. An example of an initiative to close the workforce gap is the ITU Women in Cyber initiative, which has worked to inspire, educate, and connect women through talks, trainings, and mentorships. *Her CyberTracks* supports women in policy roles to ensure that that they have the necessary skills and knowledge to engage in cyber policy. These efforts at the international organizational level complement local initiatives, seeking to support women in diving into cybersecurity careers. By leveraging the success of the Women in Cyber Mentorship Programme, *Her CyberTracks* provides specialized, targeted training, maintaining the essential mentorship and role modeling aspects.

---

1 (ISC)² Cybersecurity Workforce Study 2022 https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2-Cybersecurity-Workforce-Study-2022.pdf

2 Osborne, Charlie. (2023) "Women to Hold 30 Percent of Cybersecurity Jobs Globally by 2023" Cybercrime Magazine. https://cybersecurityventures.com/women-in-cybersecurity-report-2023/

3 WiCyS. (2023). 2023 State of Inclusion of Women in Cybersecurity – Executive Summary. https://www.wicys.org/wp-content/uploads/2023/03/Executive-Summary-The-State-of-Inclusion-of-Women-in-Cybersecurity.pdf

4 Association for Civil Rights. (2019). The desertion of women in the computer industry: the case of cybersecurity. https://adc.org.ar/wp-content/uploads/2019/06/051-A-la-desercion-de-las-mujeres-en-la-industria-informatica-04-2019.pdf

Current challenges

Despite the progress made over the past decade, national cybersecurity education capacity building is still an emerging field and there is a need for further evidence of what works best in practice and how the global community can assist low- and middle-income countries in building a cybersecurity workforce and cybersecure society.

An understanding of the key challenges faced in building national cybersecurity education capacity can help to support the design and implementation of capacity building measures. This includes the demand-side[16] factors (national and organizational need for cybersecurity knowledge, skills, and abilities) and supply-side[17] factors (awareness, education, and training of the cybersecurity workforce and population) that need to be addressed and aligned in order to drive holistic improvements, as detailed in Table.1

[16] **Demand-side challenges drawn from:**
Radunović, & Rüfenacht. (2016). Report on cybersecurity competence building trends in OECD countries. https://www.diplomacy.edu/resource/cybersecurity-competence-building-trends/; Aspen Cybersecurity Group.(2018). Principles for Growing and Sustaining the Nation's Cybersecurity Workforce. https://www.aspeninstitute.org/wp-content/uploads/2018/11/Aspen-Cybersecurity-Group-Principles-for-Growing-and-Sustaining-the-Nations-Cybersecurity-Workforce-1.pdf; De Zan & Di Franco. (2019). Cybersecurity Skills Development in the EU. https://www.enisa.europa.eu/publications/the-status-of-cyber-security-education-in-the-european-union/@@download/fullReport; GFCE Working Group D. (2022). Developing Cyber Security as a Profession. https://thegfce.org/wp-content/uploads/2022/08/GFCE-Report-Developing-Cyber-Security-as-a-Profession-July-2022-1.pdf; AlDaajeh, S., Saleous, H., Alrabaee, S., Barka, E., Breitinger, F., & Choo, K. K. R. (2022). The role of national cybersecurity strategies on the improvement of cybersecurity education. Computers & Security, 119; Creese, S., Dutton, W. H., & Esteve-González, P. (2021). The social and cultural shaping of cybersecurity capacity building: a comparative study of nations and regions. Personal and ubiquitous computing, 25(5), 941-955. https://doi.org/10.1007/s00779-021-01569-6

[17] **Supply-side challenges drawn from:**
Aspen Cybersecurity Group. (2018). Principles for Growing and Sustaining the Nation's Cybersecurity Workforce https://assets.aspeninstitute.org/content/uploads/2018/11/Aspen-Cybersecurity-Group-Principles-for-Growing-and-Sustaining-the-Nations-Cybersecurity-Workforce-1.pdf; Catota, F. E., Morgan, M. G., & Sicker, D. C. (2019). Cybersecurity education in a developing nation: The Ecuadorian environment. Journal of Cybersecurity, 5(1); De Zan & Di Franco. (2019). Cybersecurity Skills Development in the EU. https://www.enisa.europa.eu/publications/the-status-of-cyber-security-education-in-the-european-union/@@download/fullReport; Rahman, N. A. A., Sairi, I. H., Zizi, N. A. M., & Khalid, F. (2020). The importance of cybersecurity education in school. International Journal of Information and Education Technology, 10(5), 378-382; Blažič, B.J. (2022). Changing the landscape of cybersecurity education in the EU: Will the new approach produce the required cybersecurity skills? Educ Inf Technol 27, 3011–3036 https://doi.org/10.1007/s10639-021-10704-y; J. Hajny, S. Ricci, E. Piesarskas, O. Levillain, L. Galletta and R. De Nicola. (2021). Framework, Tools and Good Practices for Cybersecurity Curricula. IEEE Access, vol. 9, pp. 94723-94747. https://doi.org/10.1109/ACCESS.2021.3093952; Shillair, R., Esteve-González, P., Dutton, W. H., Creese, S., Nagyfejeo, E., & von Solms, B. (2022). Cybersecurity education, awareness raising, and training initiatives: National level evidence-based results, challenges, and promise. Computers & Security, 119, https://doi.org/10.1016/j.cose.2022.102756

Table 1: Supply and demand challenges for cybersecurity education capacity

Examples of supply-side challenges	Examples of demand-side challenges
• Lack of awareness and aspiration for cybersecurity career pathways by students. • Lack of clarity of career roadmaps and progression pathways for prospective cybersecurity professionals. • Underutilization of full labour market potential for a cybersecurity workforce, with women severely underrepresented and a need to involve more minority groups in cybersecurity education programmes. • Need to increase the availability and accessibility of a range of cybersecurity education and training pathways including apprenticeships, tertiary, and re-training programmes. • Need for greater alignment of cybersecurity competencies developed through formal education programmes and curricula with industry expectations and needs. • Difficulties encountered for education offerings and curricula to keep up to date due to rapid pace of change in the cybersecurity field. • Lack of educator expertise and resources to deliver required cybersecurity education at scale at secondary and tertiary education levels. • Lack of awareness, limited resources, and governance capacity to address cybersecurity capacity in the context of competing national development priorities.	• Demand for cybersecurity competencies is rapidly growing and outpacing supply not just for building a cybersecurity workforce, but for building a cybersecure society. • Cybersecurity workforce requirements vary by country context, with different needs, environments, cultures, and resources influencing cybersecurity education design and availability. • Need for greater clarity and building capability for organisations to define and communicate cybersecurity industry requirements for labour and recognizing cybersecurity as its own profession rather than a sub-set of IT roles. • High entry-level requirements for cybersecurity roles make it difficult for aspiring cybersecurity professionals to enter the cybersecurity workforce. • Employers' underinvestment in the necessary resources and ongoing training of cybersecurity workforce.

Indicators of commitment, maturity and readiness

In order to address the supply and demand challenges *"there is an urgent need for a national cybersecurity education strategy that bolsters multiple initiatives as well as a multi-stakeholder space in which government, industry, and academia can actively work together to address national cybersecurity educational requirements."*[18]

The components and indicators of national cybersecurity education capacity need to be understood, and the following five leading frameworks outline some important indicators to measure and build capacity:

- **Global Cybersecurity Index (GCI)**[19] developed by ITU covers capacity building measures.
- **National Cyber Security Index (NCSI)**[20] developed by the e-Governance Academy Foundation, includes two indicators: cyber safety and security website, and education and professional development.

---

18 Catota, F. E., Morgan, M. G., & Sicker, D. C. (2019). Cybersecurity education in a developing nation: The Ecuadorian environment. Journal of Cybersecurity, 5(1)

19 ITU. (2018). Global Cybersecurity Index (GCI). https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

20 E-Governance Academy Foundation. (2020). National Cyber Security Index (NCSI). https://ncsi.ega.ee/

- **National Capabilities Assessment Framework (NCAF)**[21] developed by the European Union Agency for Cybersecurity (ENISA), covers capacity-building and awareness.
- **Cybersecurity Capacity Maturity Model for Nations (CMM)**[22] developed by the Global Cyber Security Capacity Centre (GCSCC) covers 'Building cybersecurity knowledge and capabilities'.
- **Cyber Readiness Index (CRI)**[23] developed by the Potomac Institute for Policy Studies covers investment in research and development (R&D).

A review of these five frameworks identified the following five main components:

- school curricula and programmes;
- tertiary education and research;
- training and certification;
- awareness and culture;
- administration and governance.

Each of these five components have specific indicators initiated and driven by stakeholders in the public, private, and civil society sectors.

School curricula and programmes

Elements of the school curricula and programmes component include:[24]

- incorporating cybersecurity and cyber safety as a part of the school curriculum;
- building aspirations for cybersecurity career paths including the introduction of games, competitions, informational talks, and technology demonstrations;
- identifying stakeholders at the school level beyond students, to include teachers, parents, administrators, and other relevant community members to engage in related initiatives;
- ensuring that primary and secondary schools have qualified cybersecurity teachers.

---

21 ENISA. (2020). National Capabilities Assessment Framework (NCAF). https://www.enisa.europa.eu/publications/national-capabilities-assessment-framework

22 Global Cyber Security Capacity Centre. (2021). Cybersecurity capacity maturity model for nations (CMM): Revised edition. https://gcscc.ox.ac.uk/files/cmm2021editiondocpdf

23 Potomac Institute. (2015). Cyber Readiness Index (CRI) 2.0. https://www.potomacinstitute.org/images/CRIndex2.0.pdf

24 **Cybersecurity education capacity features of the school curricula and programmes component drawn from:** Global Cyber Security Capacity Centre. (2021). Cybersecurity capacity maturity model for nations (CMM): Revised edition. https://gcscc.ox.ac.uk/files/cmm2021editiondocpdf; Bate, L, (2018). Cybersecurity Workforce Development: A Primer. New America, Florida International University.https://d1y8sb8igg2f8e.cloudfront.net/documents/Cybersecurity_Workforce_Development_A_Primer_2018-11-01_183611.pdf; ITU. (2018). Global Cybersecurity Index (GCI). https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf; Parrish, A., Impagliazzo, J., Raj, R. K., Santos, H., Asghar, M. R., Jøsang, A., ... & Stavrou, E. (2018, July). Global perspectives on cybersecurity education for 2030: a case for a meta-discipline. In Proceedings companion of the 23rd annual ACM conference on innovation and technology in computer science education (pp. 36-54); Catota, F. E., Morgan, M. G., & Sicker, D. C. (2019). Cybersecurity education in a developing nation: The Ecuadorian environment. Journal of Cybersecurity, 5(1); E-Governance Academy Foundation. (2020). National Cyber Security Index (NCSI). https://ncsi.ega.ee/; OAS. (2020). Cybersecurity Education. https://www.oas.org/es/sms/cicte/docs/White-Paper-Cybersecurity-Education.pdf

Tertiary education and research

Elements of the tertiary education and research component include:[25]

- offering cybersecurity as part of a suite of tertiary education programmes such as diplomas, bachelor degrees and masters, and PhD pathways, which should include specialist cybersecurity programmes and involve cybersecurity in other technical and non-technical subject areas such as computer science, engineering, business, finance, healthcare, law, and public policy;
- ensuring cybersecurity curricula keeps up to date with research and developments in the field;
- developing a national certification programme for the accreditation of cybersecurity programmes;
- offering alternative cybersecurity education pathways, including vocational colleges and trade-apprenticeships;
- encouraging tertiary education providers and industry to work together to ensure cybersecurity education programmes align with cybersecurity workforce needs and wherever possible incorporate work-based learning and work integrated learning as part of the curricula;
- ensuring the supply of cybersecurity subject area qualified academics at the tertiary level;
- encouraging industry and government experts to participate in cybersecurity education delivery;
- establishing cybersecurity research centres;
- establishing and encouraging formal and informal public-private partnerships that drive cybersecurity research and development programmes.

[25] **Cybersecurity education capacity features of the tertiary education and research component drawn from:** Potomac Institute. (2015). Cyber Readiness Index (CRI) 2.0. https://www.potomacinstitute.org/images/CRIndex2.0.pdf; Radunović, Vladimir, & Rüfenacht, David. (2016). Report on cybersecurity competence building trends in OECD countries. https://www.diplomacy.edu/resources/general/cybersecurity-competence-building-trends; Henry, Adam P. (2017). Mastering the Cyber Security Skills Crisis: Realigning Educational Outcomes to Industry Requirements https://unsw.adfa.edu.au/unsw-canberra-cyber/sites/accs/files/uploads/ACCS-Discussion-Paper-4-Web.pdf; Bate, L. (2018). Cybersecurity Workforce Development: A Primer. https://d1y8sb8igg2f8e.cloudfront.net/documents/Cybersecurity_Workforce_Development_A_Primer_2018-11-01_183611.pdf; ITU. (2018). Global Cybersecurity Index (GCI). https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf; The International Telecommunication Union, The World Bank, Commonwealth Secretariat, the Commonwealth Telecommunications Organisation, NATO Cooperative Cyber Defence Centre of Excellence. (2018) Guide to Developing a National Cybersecurity Strategy. Creative Commons Attribution 3.0 IGO; Catota, F. E., Morgan, M. G., & Sicker, D. C. (2019). Cybersecurity education in a developing nation: The Ecuadorian environment. Journal of Cybersecurity, 5(1); De Zan & Di Franco. (2019). Cybersecurity Skills Development in the EU. https://www.enisa.europa.eu/publications/the-status-of-cyber-security-education-in-the-european-union/@@download/fullReport; OAS. (2020). Cybersecurity Education. https://www.oas.org/es/sms/cicte/docs/White-Paper-Cybersecurity-Education.pdf

Work integrated learning[1, 2]

Work integrated learning (WIL) is an educational approach that integrates practical work experience as part of the curricula. This approach provides students with opportunities to turn theory into practice and gain real-world experience. This combination of academic study and practical experience helps students develop a broad range of skills and competencies as well as creating opportunities for mentorship and networking with industry. As cybersecurity is a rapidly evolving field where applied skills and up-to-date knowledge are highly valued, WIL can provide students with the opportunity to work with real cyber threats and security challenges, enabling them to develop vital problem-solving skills and an understanding of how to handle real-world cybersecurity incidents.

WIL can take a variety of forms including work placements, fieldwork, industry projects, and internships. For example, Western Sydney University in Australia offers a Bachelor of Cyber Security and Behaviour course where final year students complete 44 days as an intern in a cybersecurity related workplace. During this time students complete a range of related assessments such as a journal on what they have learnt, assignments based on their role, and feedback from supervisors. This experience provides the student with credit for the equivalent of four full subjects of study towards their certification.

1 Bridge, j & Twaddle, J. (2023). Scaling up work integrated learning in higher education. https://www.pwc.com.au/government/government-matters/work-integrated-learning-in-higher-education.html

2 Western Sydney University. (2023). Industry Placement Pathway. https://online.westernsydney.edu.au/online-courses/social-science/bachelor-cyber-security-behaviour/placement-pathway/

Training and certification

Elements of the training and certification component include:[26]

- availability and accessibility of a range of cybersecurity training courses including in technical and non-technical areas; for experts and non-experts; formal and informal learning and mentoring; and aimed at operational and executive levels;
- availability and accessibility of cybersecurity professional certifications;
- availability of cyber exercises and drills at the regional, national, sectoral, and organizational level;
- availability of cybersecurity mentorship programmes;
- existence of cybersecurity professional associations;
- existences of a register of certified cybersecurity professionals in the country.

26 **Cybersecurity Education Capacity features of the Training and Certification component drawn from:** Global Cyber Security Capacity Centre. (2021). Cybersecurity capacity maturity model for nations (CMM): Revised edition. https://gcscc.ox.ac.uk/files/cmm2021editiondocpdf ITU. (2018). Global Cybersecurity Index (GCI). https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf. The International Telecommunication Union, The World Bank, Commonwealth Secretariat, the Commonwealth Telecommunications Organisation, NATO Cooperative Cyber Defence Centre of Excellence. (2018) Guide to Developing a National Cybersecurity Strategy. Creative Commons Attribution 3.0 IGO; GFCE Working Group D. (2019). White Paper: Task Force on Cybersecurity Professional Training and Development. https://cybilportal.org/wp-content/uploads/2020/02/GFCE-WG-D-White-Paper-Task-Force-on-Cybersecurity-Professional-Training-and-Development.pdf; E-Governance Academy Foundation. (2020). National Cyber Security Index (NCSI). https://ncsi.ega.ee/

Awareness and culture

Elements of the awareness and culture component, include:[27]

- formal and informal cybersecurity awareness programmes that build a cybersecurity culture in government, industry, academia and civil society and which include elements such as the promotion of digital literacy and cyber safety skills, highlighting cybersecurity risks, developing cybersecure work practices, and encouraging participation in the cybersecurity workforce;
- targeted cybersecurity executive awareness programmes adapted for different sectors of the economy such as finance, telecommunications, critical infrastructure, and government agencies;
- availability and accessibility of an online portal and resources to provide cybersecurity information to the general public as well as government, industry, academia and civil society.

Administration and governance

Elements of the administration and governance component, include:[28]

- incorporating capacity and workforce development as part of national strategies and policies, including broad consultation with government, private sector, academia and civil society stakeholders;
- developing of a national cybersecurity education and research action plan;
- designating at least one government entity to oversee the implementation, monitoring and evaluation of the national cybersecurity education action plan;
- allocating government resources to fund cybersecurity education capacity development programmes;
- adopting a common taxonomy for government, industry, and academia to describe cybersecurity workforce requirements and share information, knowledge, skills, and abilities;

---

[27] **Cybersecurity Education Capacity features of the Awareness and Culture component drawn from:** Global Cyber Security Capacity Centre. (2021). Cybersecurity capacity maturity model for nations (CMM): Revised edition. https://gcscc.ox.ac.uk/files/cmm2021editiondocpdf. ITU. (2018). Global Cybersecurity Index (GCI). https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf. The International Telecommunication Union, The World Bank, Commonwealth Secretariat, the Commonwealth Telecommunications Organisation, NATO Cooperative Cyber Defence Centre of Excellence. (2018) Guide to Developing a National Cybersecurity Strategy. Creative Commons Attribution 3.0 IGO; Catota, F. E., Morgan, M. G., & Sicker, D. C. (2019). Cybersecurity education in a developing nation: The Ecuadorian environment. Journal of Cybersecurity, 5(1); OAS. (2020). Cybersecurity Education. https://www.oas.org/es/sms/cicte/docs/White-Paper-Cybersecurity-Education.pdf; Rahman, N. A. A., Sairi, I. H., Zizi, N. A. M., & Khalid, F. (2020). The importance of cybersecurity education in school. International Journal of Information and Education Technology, 10(5), 378-382.

[28] **Cybersecurity Education Capacity features of the Administration and Governance component drawn from:** Potomac Institute. (2015). Cyber Readiness Index (CRI) 2.0. https://www.potomacinstitute.org/images/CRIndex2.0.pdf; Global Cyber Security Capacity Centre. (2021). Cybersecurity capacity maturity model for nations (CMM): Revised edition. https://gcscc.ox.ac.uk/files/cmm2021editiondocpdf; Newhouse, W., Keith, S., Scribner, B., & Witte, G. (2017). National initiative for cybersecurity education (NICE) cybersecurity workforce framework. NIST special publication, 800(2017), 181; The International Telecommunication Union, The World Bank, Commonwealth Secretariat, the Commonwealth Telecommunications Organisation, NATO Cooperative Cyber Defence Centre of Excellence. (2018) Guide to Developing a National Cybersecurity Strategy – Strategic engagement in cybersecurity (p.13). Creative Commons Attribution 3.0 IGO; De Zan & Di Franco. (2019). Cybersecurity Skills Development in the EU. https://www.enisa.europa.eu/publications/the-status-of-cyber-security-education-in-the-european-union/@@download/fullReport; OAS. (2020). Cybersecurity Education. https://www.oas.org/es/sms/cicte/docs/White-Paper-Cybersecurity-Education.pdf

- ensuring regular engagement and cooperation between government, education providers and industry to align supply and demand requirements of the cybersecurity workforce.

These elements can be supported by the introduction of government funded incentive mechanisms such as:

- promotion of competitions and other initiatives that drive aspirations for cybersecurity careers;
- funding targeted programmes for underrepresented groups such as women to ensure the full inclusion of the available workforce;
- grants to encourage the transition to cybersecurity careers;
- grants to encourage the retention of the cybersecurity workforce within the country;
- cybersecurity education programme scholarships;
- cybersecurity R&D tax credits, grants and scholarships.

Building capacity

To effectively address the supply and demand challenges to build capacity, it is important to adopt a holistic approach when raising the level of maturity and readiness of existing cybersecurity education capacity (taking the various components into account). The European Commission[29] provides a framework for such an approach as part of the 'Operational Guidance for the EU's International Cooperation on Cyber Capacity Building' in which all cybersecurity capacity development efforts must be built across individual and organizational capacity, and the enabling environment (see Table 2).

Table 2: Levels of capacity

Individual capacity	Organizational capacity	Enabling environment
"Capacity building for individuals is the process of equipping them with the understanding, skills and access to information, knowledge and training to perform effectively."	*"Capacity building for an organization is focused on the elaboration of management structures, processes and procedures internally and managing relationships between different organizations and sectors (public, private and community)."*	*"Creating an enabling environment is about generating the right set of legal, regulatory, economic and societal changes that ultimately support organizations, institutions and agencies at all levels and in all sectors in enhancing their capacities."*

Stages of cybersecurity capacity building

The *Operational Guidance for the EU's International Cooperation on Cyber Capacity Building*[30] also defines the main stages of capacity building as part of its proposed Cyber Capacity Building Framework (CCBF). The checklist for cybersecurity capacity-building stages, detailed below and

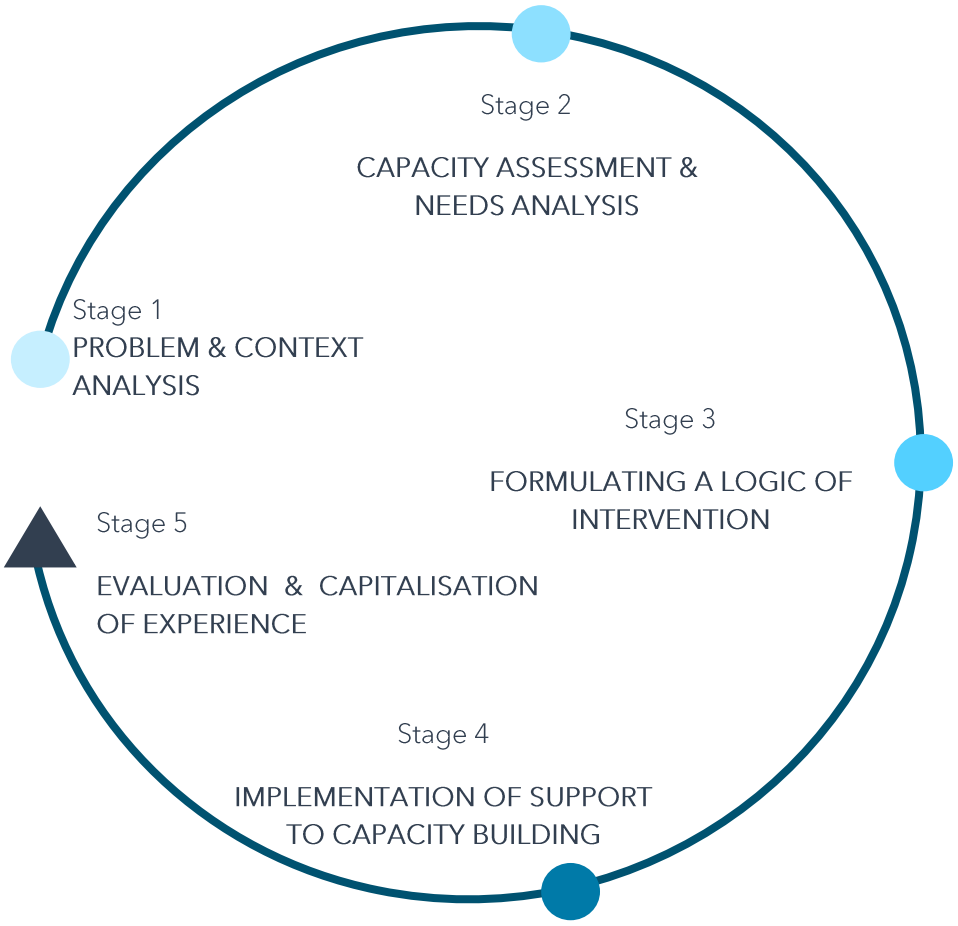
[29] European Commission. (2018). Operational Guidance for the EU's international cooperation on cyber capacity building. https://www.iss.europa.eu/content/operational-guidance-eu%E2%80%99s-international-cooperation-cyber-capacity-building

[30] European Commission. (2018). Operational Guidance for the EU's international cooperation on cyber capacity building. https://www.iss.europa.eu/content/operational-guidance-eu%E2%80%99s-international-cooperation-cyber-capacity-building

illustrated in Figure 1, provides a process that countries can apply in the preparatory stages to achieve their capacity building goals.

- **Problem and context analysis:** Understanding the problem to be addressed, the broader context and strategic drivers, and defining capacity building goals.
- **Capacity assessment and needs analysis:** Understanding existing capacities, resources available, and the identification of the gaps and priorities.
- **Formulating a logic of intervention:** Identifying specific agents of change, capacities to be strengthened, as well as any moderating factors that can impact success.
- **Implementation of support to capacity building:** Facilitating and monitoring the delivery of the intervention.
- **Evaluation and capitalization of experience:** Assessment of the achievement of the capacity building goals and lessons to support future actions.

Figure 1: Cybersecurity capacity building stages



Source: adapted from the EU operational guidance

3 Systems approach to education capacity building

3.1 The systems approach concept

The findings outlined in section 2 reveal the complex and multi-faceted issues when seeking to determine the state of maturity, address gaps, develop national cybersecurity capacity and build resilience in their cybersecurity ecosystem. This complexity, and the ever-changing environment, makes cybersecurity education a so-called 'wicked problem', one that requires a holistic and multi-level response given its critical function as a part of the solution. The challenges of national cybersecurity education capacity have been summarized by Bate[31] when describing experiences in the United States of America:

> *"There is no single underlying problem, but rather an interconnected and multifaceted array of issues that ties together K12 education, diversity and inclusion, higher education, industry certifications and competencies, military and intelligence recruitment, apprenticeship and work-based learning, veterans' employment, federal hiring practices, and much more."*

This section outlines the potential merits of applying a systems approach that seeks to address the complex policy challenges using a holistic approach, which includes understanding how individual elements work together, how elements are related, and how they are impacted by their environment. A systems approach requires a diverse range of perspectives to understand the various inputs, processes, and outputs of the system.[32]

Allen and Kilvington[33] identify four key components of a systems approach to address a 'wicked' problem. These components include:

1. **Multiple perspectives:** who are the key actors that are part of or impacted by the situation and how do their knowledge systems and views frame their perspectives and level of engagement with the issues?
2. **Interconnections:** how do the various elements of the system interconnect, what are the patterns of these connections and the nature and direction of these relationships?
3. **Boundaries:** what is the scope and scale of the system, and how do different actors consider definitions of and improvements to the problem being addressed?
4. **Influence:** what are the enablers and barriers within a system, what drives the system and what are the leverage points that offer the greatest potential for intervention to influence system outcomes?

---

31 Bate, L. (2018). Cybersecurity Workforce Development: A Primer. https://d1y8sb8igg2f8e.cloudfront.net/documents/Cybersecurity_Workforce_Development_A_Primer_2018-11-01_183611.pdf

32 OECD. (2017). Systems Approaches to Public Sector Challenges. https://www.oecd.org/publications/systems-approaches-to-public-sector-challenges-9789264279865-en.htm

33 Allen & Kilvington. (2018). Summary: An introduction to systems thinking and systemic design – concepts and tools (Presentation). Based on material for an introductory workshop. https://learningforsustainability.net/post/systemicdesign-intro/

A system, in this context, can be defined as:

> *"Elements joined together by dynamics that produce an effect, create a whole or influence other elements and systems…A system always exceeds the sum of its parts."* [1]

[1] OECD. (2017). Systems Approaches to Public Sector Challenges. https://www.oecd.org/publications/systems-approaches-to-public-sector-challenges-9789264279865-en.htm

As an example, a relatively simple system is a bicycle, which is a system that has several easily defined components including wheels, gears, pedals, brakes, and handlebars, that when working together allow the bicycle to move in a specific direction at variable speeds. If any part was modified, its ability to perform will be dependent on how it interacts with the other parts of the bicycle. The effectiveness of the bicycle as a system will also be influenced by the environment in which it is operating, such as a slippery snow-covered footpath, a sandy beach, or an indoor cycling track.

Whilst a bicycle is a system with easily defined components, there are more complex systems, such as global financial markets, environmental ecosystems, and national cybersecurity education capacity systems. Although these systems may be much harder to define than a bicycle, there is merit in breaking down such complex systems to a level of abstraction that allows for a deeper understanding of which components are important and how they might be interacting with each other to produce a given result. This is explained further by the Organization for Economic Co-operation and Development (OECD),[34] which identified education as a public sector challenge that could benefit from a systems approach:

> *"Education is also appropriate for systems approaches due to its contextual variance. Nearly every transaction in education is unique, and the objectives of each participant in the transaction are also unique (e.g. school leader with teacher, teacher with student, student with parent). This makes the system especially resistant to scaling solutions, or those that attempt to apply the same logic to every scenario. Education systems also have compounding and contradictory objectives, such as the inculcation of shared identity versus agency and independence for students. Systems approaches help to navigate this space where the optimal is often impossible."*

Why consider exploring a systems approach for national cybersecurity education capacity?

Given the importance and complex nature of national cybersecurity education capacity building and the limited resources available to governments, a systems approach offers the potential to assist governments and other relevant actors to optimize their response to this challenge. Establishing a holistic understanding of the key elements and boundaries of the national cybersecurity education capacity building system can help governments to identify existing and future actions that will drive positive change in the system. Furthermore, by identifying

[34] OECD. (2017). Systems Approaches to Public Sector Challenges. https://www.oecd.org/publications/systems-approaches-to-public-sector-challenges-9789264279865-en.htm

interrelationships between different elements, governments can begin to understand how actions and investments in one component of national cybersecurity education capacity may impact others, and whether the impact is likely to be positive or negative.[35]

Greater understanding of the national cybersecurity education capacity system can create a shift in policy approach. This can be achieved by recognizing that the individual elements of the system can act differently when in isolation or as a part of the wider system**.** This can help governments to provide a framework to identify key leverage or primary intervention points where targeted activity might help to optimize and nurture the capacity of the system. Such an approach has the potential to increase the efficacy of cybersecurity education capacity actions, optimize resource allocation, and drive long-term positive impacts and the achievement of policy goals over time.

The following section explores how applying a systems approach to a problem aligns with existing frameworks on national cybersecurity capacity building processes.

3.2 Systems approach to capacity building

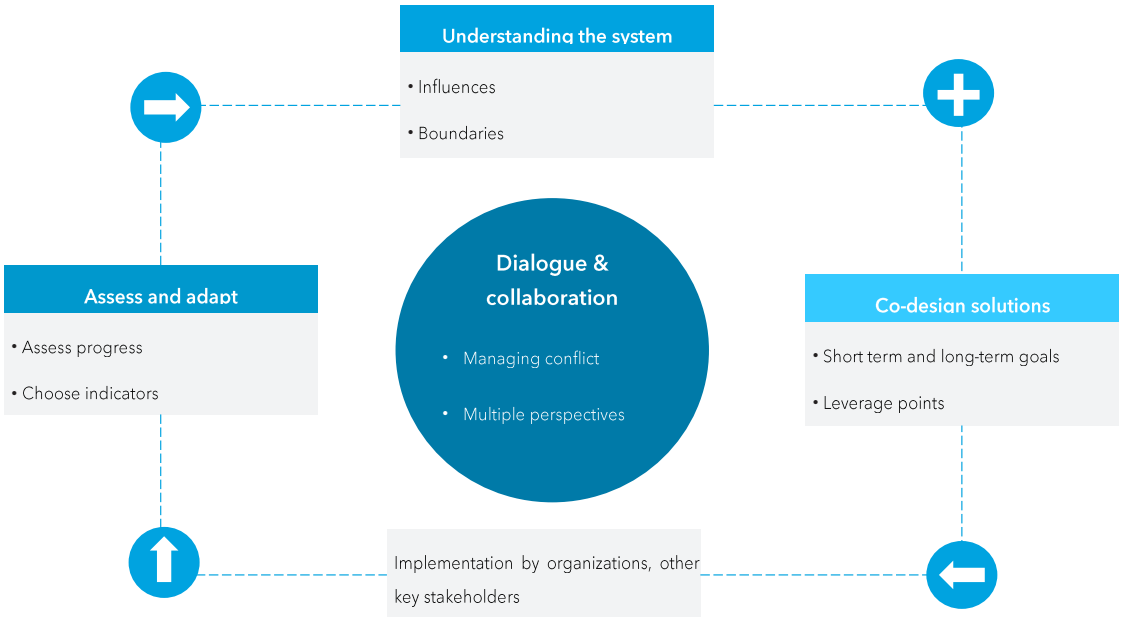
Consistent with capacity building in a project and programme management cycle,[36] a structured process can also be followed when applying a systems approach to a problem. This helps to define the components of a system and offer solutions. Allen and Kilvington[37] introduce this process through a systemic design cycle that consists of three functions: understand the system, co-design solutions, and assess and adapt. These functions should be underpinned by ongoing dialogue and collaboration between key system stakeholders. This systemic design cycle is illustrated in Figure 2.

[35] Learning for Sustainability. (2020). Systems Thinking. https://learningforsustainability.net/systems-thinking/

[36] European Commission. (2018). Operational Guidance for the EU's international cooperation on cyber capacity building. https://www.iss.europa.eu/content/operational-guidance-eu%E2%80%99s-international-cooperation-cyber-capacity-building

[37] Allen & Kilvington. (2018). Summary: An introduction to systems thinking and systemic design – concepts and tools (Presentation). Based on material for an introductory workshop. https://learningforsustainability.net/post/systemicdesign-intro/

Figure 2: Systemic design cycle



Source: adapted from allen and kilvington 'Key systems thinking components'

The systemic design cycle has parallels with the project and programme management cycle. Table 3 aligns these approaches for cybersecurity capacity building.

Table 3: Alignment of approaches

Stage	Cybersecurity capacity building in the project and programme management cycle	Systemic design cycle functions	
1	*Problem and context analysis*	Understanding the system	Dialogue and collaboration
2	*Capacity assessment and needs analysis*		
3	*Formulating a logic of intervention*	Co-design solutions	
4	*Implementation, including monitoring and reporting*	Implementation by organizations, other key stakeholders	
5	*Evaluation of the provided support*	Assess and adapt	

Mapping the systemic design cycle functions to cybersecurity capacity building in the project and programme management cycle, makes it easier to identify the types of systems thinking tools that might most benefit policy-makers and educators in their cybersecurity education

capacity building efforts. Examples of systemic design function tools[38, 39, 40] that may be useful as part of this process include:

- **Iceberg models** assist in understanding complex issues by looking beyond surface level events to understand the range of patterns, structures, and mental models influencing the situation being assessed.
- **Logic models** provide a visual representation of how an initiative is expected to perform by detailing the connections and flow between inputs, change mechanisms, outputs, outcomes, impacts and moderating factors.
- **PESTLE analysis** is a strategic framework to analyse the political, economic, social, technological, legal, and environmental (PESTLE) factors in which an intervention is being deployed.
- **Problem and objective tree** is a set of visual tools that can illustrate relationships and connections. A problem tree can assist in identifying the root causes of a problem and its consequences. An objective tree is a complementary tool which uses the causes and effects of the problem tree and reverses them to identify objectives and outcomes to solve the problem.
- **Stakeholder analysis or mapping** is used to identify and understand the range of individuals, groups and other entities that are likely to have an interest in, be affected by, or have the ability to influence the success of an initiative.
- **System concept mapping** is visualization tool to represent and allow for the analysis of complex systems through identifying and illustrating system components, relationships and feedback loops.

Three of these tools have been selected and applied to the problem of national cybersecurity education capacity in section 4: problem trees, stakeholder analysis, and systems concept mapping.

---

38 Allen & Kilvington. (2018). Summary: An introduction to systems thinking and systemic design – concepts and tools (Presentation). Based on material for an introductory workshop. https://learningforsustainability.net/post/systemicdesign-intro/

39 Social Value International. (2017). Maximise Your Impact: A guide for social entrepreneurs. https://socialvalueint.org/maximise-your-impact-guide

40 REWIRE Project. (2021). PESTLE analysis of Cybersecurity Education. https://digital-skills-jobs.europa.eu/en/inspiration/research/pestle-analysis-cybersecurity-education-2021

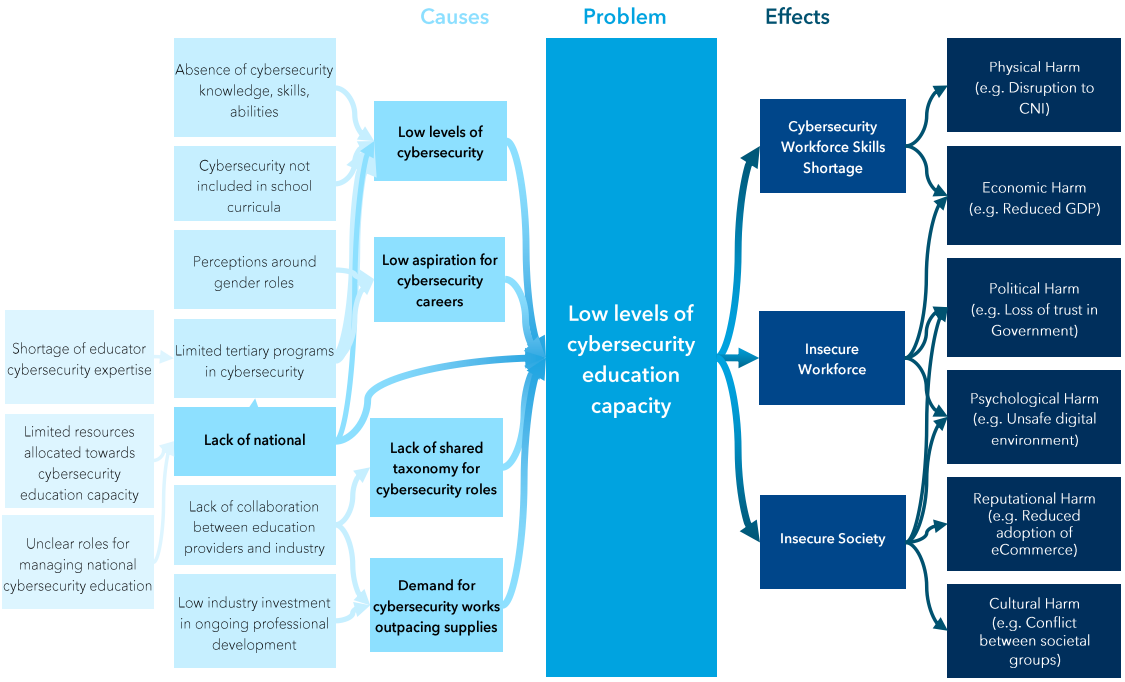
4 Understanding the cybersecurity education capacity system

There are a wide range of tools[41, 42] to help policy-makers and practitioners explore systems approaches to policy challenges. This section sets out how a select set of tools can be adapted to national cybersecurity education capacity and explores how they can be used to build a holistic understanding of the system. The application of these tools depends on the different national contexts in which they are used and this section introduces general concepts as the basis for future discussion. It is important to note that the tools presented here should be adapted to each country's policy goals and individual system characteristics.

4.1 Problem tree

The national cybersecurity education capacity system problem tree,[43] illustrated in Figure 3, is an example of a systems tool that leads to an understanding of the system by identifying the components and how they connect. For national cybersecurity education capacity building, the decision tree presents some of the causes and effects of low levels of cybersecurity education capacity.[44] It incorporates insights from the challenges identified in section 2 and shows how low levels of national cybersecurity education capacity can lead to negative effects.

Figure 3: National cybersecurity education capacity problem tree



Source: ITU

---

41 Allen & Kilvington. (2018). Summary: An introduction to systems thinking and systemic design – concepts and tools (Presentation). Based on material for an introductory workshop. https://learningforsustainability.net/post/systemicdesign-intro/

42 OECD, 2017, "Systems Approaches to Public Sector Challenges". OECD. (2017). Systems Approaches to Public Sector Challenges. https://www.oecd.org/publications/systems-approaches-to-public-sector-challenges-9789264279865-en.htm

43 Adapted from: Social Value UK. (2017). Maximise Your Impact – A Guide for Social Entrepreneurs. http://www.socialvalueuk.org/app/uploads/2017/10/MaximiseYourImpact.24.10.17.pdf

44 Cyber Harms in problem tree adapted from: Agrafiotis, I., Bada, M., Cornish, P., Creese, S., Goldsmith, M., Ignatuschtschenko, E., Upton, D. M. (2016). Cyber harm: concepts, taxonomy and measurement. Saïd Business School WP.

4.2 Stakeholder analysis

The stakeholder analysis tool assists in building a deeper understanding of national cybersecurity education capacity. As stakeholders are likely to have different perspectives, interests, and power over systems and how they work, it is important to gather multi-stakeholder perspectives to reach a holistic understanding of the system. Table 4 provides an indicative list of stakeholders with varying levels of interest and roles in national cybersecurity education capacity.

Table 4: National cybersecurity education stakeholders

Stakeholder	Type	Interests/roles in national cybersecurity education capacity
School students	Individual	• Students at primary and secondary education levels have the opportunity to engage in cybersecurity related academic and aspiration building learning and activities.
Tertiary students	Individual	• Students at tertiary level may be actively pursuing cybersecurity as a career path and look to obtain knowledge, skills, and abilities to enter the workforce. • Other students at this level may benefit from cybersecurity knowledge as part of their studies in areas other than cybersecurity e.g., computer science, engineering, business, finance, healthcare, law, and public policy.
Parents	Individual	• Parents of primary, secondary and tertiary level students will have varying levels of engagement in the academic achievement and career aspirations of their children and may influence decisions to pursue cybersecurity careers.
School teachers	Individual	• School teachers have a direct role in delivering cybersecurity related curricula and activities and can play a key role in the future education and career direction and development of their students.
Tertiary educators	Individual	• Tertiary educators have a direct role in delivering cybersecurity related curricula and activities and can play a key role in the future education and career direction and development of their students.
General public	Individual	• Individual members of the general public will require an understanding of cybersecurity and the tools to keep them safe online.
National governments	Government	• National governments set policy directions and resource allocations for the achievement of cybersecurity education and workforce development goals, as well as broader national security responsibilities to protect individual citizens, organizations, government systems and national infrastructure.

Table 4: National cybersecurity education stakeholders (continued)

Stakeholder	Type	Interests/roles in national cybersecurity education capacity
Government agencies	Government	• Government agencies administer allocated resources to achieve national cybersecurity workforce and national security policy goals. • Government agencies also contribute to demand for the cybersecurity workforce. • Government agencies develop and implement specific actions to achieve policy goals.
Private sector	Private	• The private sector drives demand for the cybersecurity workforce and typically leads the way in knowledge, skills, and ability requirements for the cybersecurity professionals. • The private sector invests resources to support their own workforce requirements and engagement with other stakeholders to achieve workforce goals. • The private sector has an interest in informing government policy development and implementation. • The private sector also often plays a leading role in cybersecurity education through academies and training programmes.
Civil society	Civil society	• Civil society also drives demand for the cybersecurity workforce. • Civil society has an interest in informing government policy development and implementation.
Research centres	Education	• Research centres support research and development and look for opportunities for commercialization of cybersecurity innovations. • Research centres help to identify opportunities and threats that may affect government, private sector, and civil society stakeholders and society.
Professional training providers	Education	• Professional training providers offer courses to support certification and professional development of the cybersecurity workforce and other training needs including both technical and non-technical training at both operational and executive levels. • Professional training providers have interests in government, private sector and civil society workforce needs. • Professional training providers have an interest in supporting government policy development and implementation.

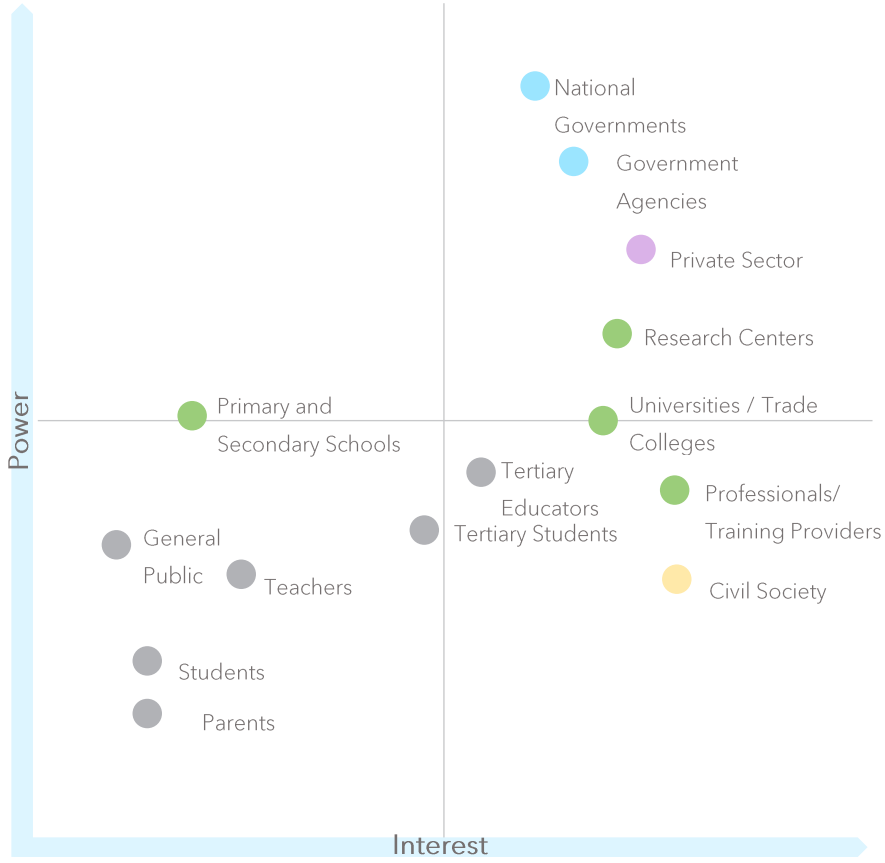
Table 4: National cybersecurity education stakeholders (continued)

Stakeholder	Type	Interests/roles in national cybersecurity education capacity
Universities and trade colleges	Education	• Universities and trade colleges offer formal programmes in cybersecurity and also have the opportunity to embed cybersecurity skills across a broad range of programme areas. • Universities and trade colleges have interests in government, private sector and civil society workforce needs. • Universities and trade colleges have interest in informing government policy development and implementation. • Universities and trade colleges work with schools, employers, and governments on promoting cybersecurity pathways. • Universities drive research and development in cybersecurity.
Primary and secondary schools	Education	• Primary and secondary schools facilitate opportunities to teach cybersecurity and related curriculum and run related activities. • Primary and secondary schools may work with trade colleges, universities, employers, and government to promote different career pathways.

Figure 4 maps the stakeholders listed in Table 4 based on estimated levels of interest and power regarding the building of national cybersecurity education capacity.[45] For the purpose of this exercise, 'Interest' considers to what degree each stakeholder is likely to be affected by changes in national cybersecurity education capacity, and how much they are interested or concerned. 'Power' considers the influence they may have over national cybersecurity education capacity building, and to what degree they can help to achieve, or block, the desired change.

[45] Stakeholder Mapping Adapted from: Social Value UK. (2017. Maximise Your Impact – A Guide for Social Entrepreneurs. http://www.socialvalueuk.org/app/uploads/2017/10/MaximiseYourImpact.24.10.17.pdf

Figure 4: National cybersecurity education capacity stakeholder map



4.3 System concept

Figure 5 provides a high-level representation of national cybersecurity education capacity as a system. The system concept takes into consideration the five components of national cybersecurity education capacity identified in section 2.2 and places them within the context of the overall system environment, illustrating potential links between system components. A key for the systems concept is provided in Table 5.

Table 5: Key to systems concept in Figure 5

Colour and shape	Description
Light blue box	The area within this box represents the national cybersecurity education capacity systems environment e.g. represents all the various cybersecurity and wider societal components of a country.
Grey box	This box contains the boundary of the national cybersecurity education capacity system.
Blue box	This box contains the outputs of the national cybersecurity education capacity system.

Table 5: Key to systems concept in Figure 5 (continued)

Colour and shape	Description
Dark blue box	This box contains the inputs of the national cybersecurity education capacity system.
Lighter blue box	This box contains the administration and governance component of national cybersecurity education capacity.
Yellow box	This box represents the awareness and culture component of national cybersecurity education capacity.
Green box	These three boxes represent the school curricula and programmes, tertiary education and research, and training and certification components of national cybersecurity education capacity. These three components have been grouped together as they represent opportunities for facilitating the direct transfer of cybersecurity knowledge, skills, and abilities.
Purple box	This box represents the active national cybersecurity workforce.
Light grey box	These boxes represent the proposed cybersecurity education capacity stages (CECS) that cybersecurity professionals move through as part of the education lifecycle, with the number and characteristics of stages likely to vary between countries.
Solid-black arrows	These arrows indicate the typical direction of travel through the various CECS.
Solid-coloured arrows 	These solid-coloured arrows indicate the potential existence and direction of relationships between system elements.
Dotted-coloured arrows 	These dotted coloured arrows indicate the direct engagement and potential transfer of knowledge, skills, and abilities, between components of national cybersecurity education capacity and individuals moving through each CECS.
Dotted-black arrows	The dotted black arrows indicate labour force movement from each CECS into the cybersecurity workforce.
Dark grey arrow	This arrow represents inputs into the system e.g., resources, people, technology etc.
Grey arrow	This arrow represents outputs produced by the system e.g. a reduction in cybersecurity harms and a more resilient cybersecure society.

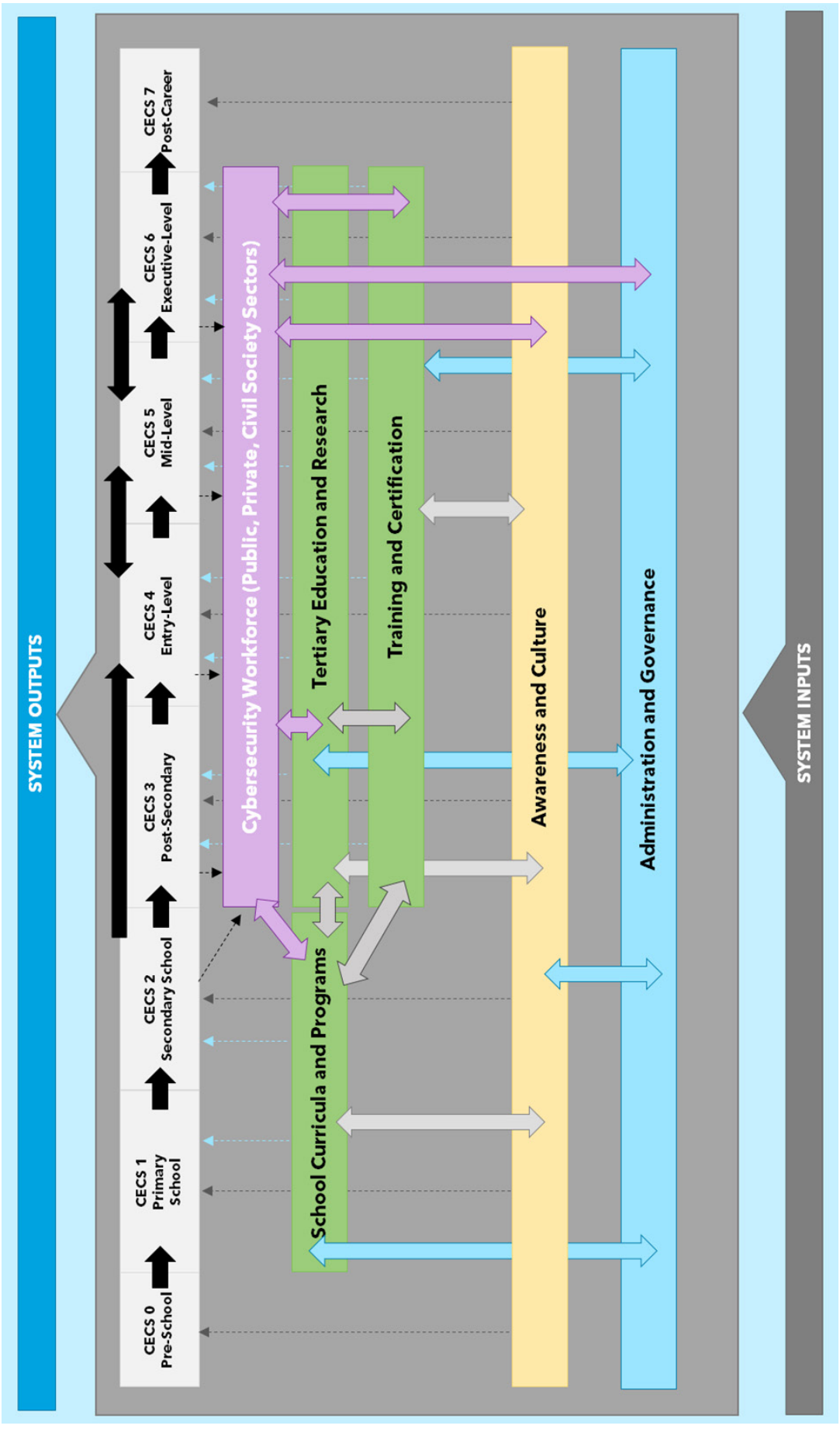
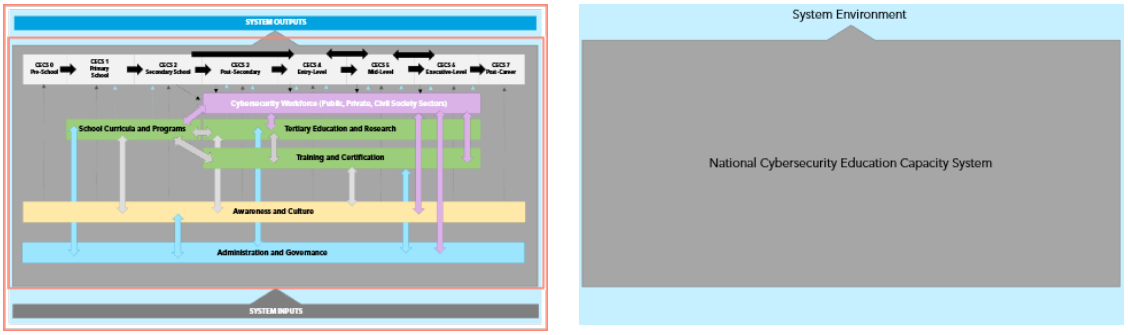


Figure 5: National cybersecurity education capacity system concept

Breaking down the systems concept diagram

Figure 6: National cybersecurity education capacity system and the system environment

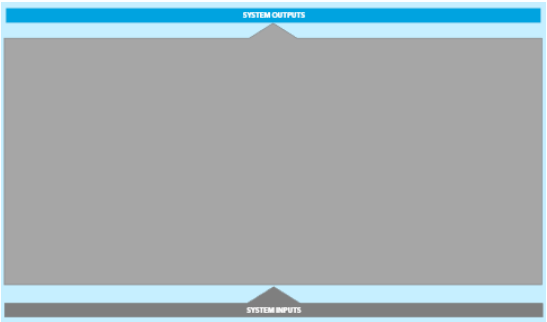


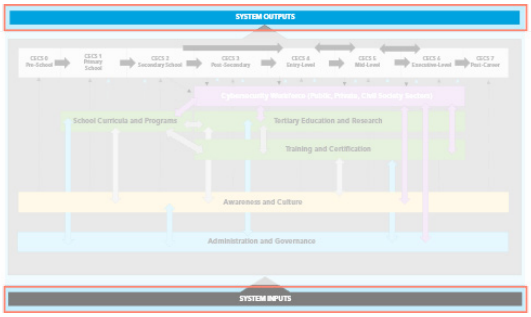
Source: ITU

The ***national cybersecurity education capacity system*** reflects all the components and elements that contribute to national cybersecurity education capacity including activities driven by the public and private sectors, civil society stakeholders and individuals. To ensure the accessibility and comprehension of the system, a high-level abstraction has been presented to allow countries to think about the overall components, interactions, and goals of a system. At this high-level of abstraction, system components include school curricula and programmes, tertiary education and research, training and certification, awareness and culture, administration and governance. In addition to these components, the system includes the cybersecurity workforce and the various cybersecurity education capacity stages (CECS) that interact with each other as well as the five components detailed above. It is these components and how they interact and influence each other that make up the national system. To understand and explore such a national system, it is important to create system boundaries to see how different inputs influence the internal functions of the system and examine how external influences stemming from the system environment impact its dynamics.

The ***system environment*** represents the context of the national cybersecurity education capacity system. This includes other areas of significance for national cybersecurity, and the broader range of priorities, challenges, and circumstances that create the conditions in which national cybersecurity education capacity functions. It is important to acknowledge the complex moderating factors that will impact national cybersecurity education, which exists in a broad national, regional, and global environment alongside a vast array of other systems each with their own complexity and impact on each other (e.g., financial system, climate change and environment, food security, transport, social and economic structures, and political systems).

System inputs and outputs





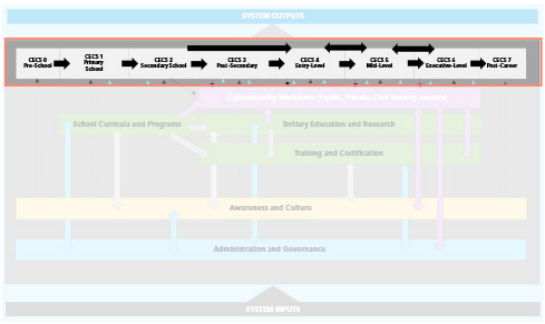
System inputs, represented by the dark grey arrow (), influence the operation and sustainability of a system. For a national cybersecurity education capacity system, inputs might include:

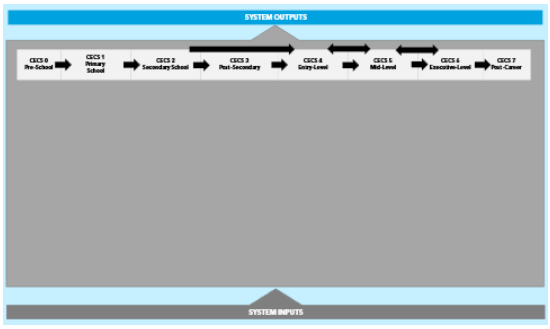
- financial and human resources to develop and expand the scale of cybersecurity education;
- technology to facilitate cybersecurity education, including support infrastructure, as well as hardware and software;
- curriculum and training resources that can be adapted and implemented to improve the effectiveness of cybersecurity education;
- knowledge and expertise from cybersecurity experts, practitioners, and systems analysis that can support the design and optimization of national cybersecurity education capacity;
- regional and global cybersecurity factors and other conditions such as changes to the cybersecurity threat landscape and cybersecurity education policies and priorities.

System outputs, represented by the grey arrow (), illustrate the product of the system inputs working together to produce outcomes and might include:

- improved sustainability and resilience of the cybersecurity workforce, cybersecure workforce, and cybersecure society, that reflect national priorities and requirements;
- mitigation of cybersecurity risks and harms;
- improved national cybersecurity capacity maturity;
- lessons and knowledge from research and analysis of the system that can provide feedback to improve future performance and optimize policy recommendations to enhance the system.

Cybersecurity education capacity stages





The systems concept introduces the stages of cybersecurity education capacity building as a customizable way to map the education lifecycle of cybersecurity professionals in any given country. The stages are intended to represent the path an individual would follow throughout their education and workforce journey from early childhood to retirement. By deconstructing the cybersecurity education capacity system into smaller, more manageable stages, the aim is to enhance understanding of effective actions needed to reach national cybersecurity education goals. Additionally, this approach is expected to shed light on the interplay of measures across each component of the cybersecurity education capacity system.

The solid-black arrows (⬆) represent the direction that individuals within the system travel between each stage. The direction and movement between each stage may be different for each country and should be customized to align to the typical experience of each country.

The dotted-black arrows (⇡) represent the typical timing of when people enter the cybersecurity workforce. This can be customized for each country to highlight when individuals are entering the cybersecurity workforce and where there may be gaps in the system.

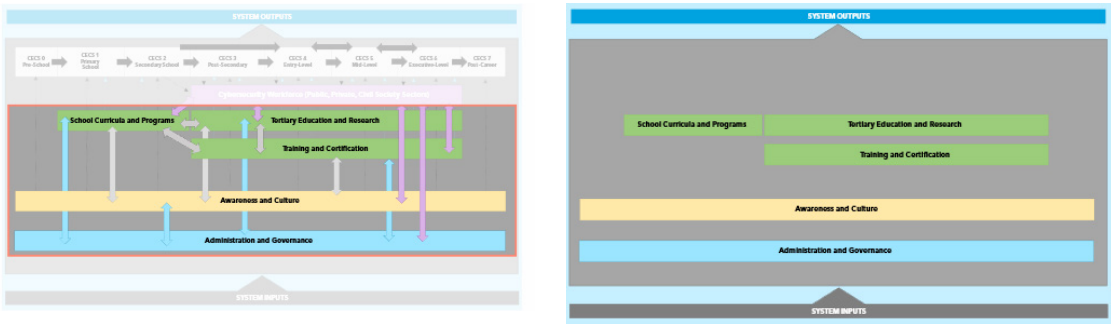
As an example, a country might define each CECS as follows:

- CECS 0 – Pre-school
- CECS 1 – Primary school
- CECS 2 – Secondary school
- CECS 3 – Post-secondary
- CECS 4 – Entry-level
- CECS 5 – Mid-level
- CECS 6 – Executive-level
- CECS 7 – Post-career

It should be noted that an individual at any stage can engage with any of the components of the national cybersecurity education capacity system. For example, a full-time university student at CECS 3 may study for a degree in cybersecurity (tertiary education and research component) at the same time as someone who is mid-career in CECS 5. As such, each stage is intended to represent the main study or employment focus of an individual at any given point.

When applying this systems concept to a specific country, the number and characteristics of each stage can be defined to align with existing constructs and contexts (e.g., existing school systems and commonly accepted career levels). Each stage could then be explored taking into account key stakeholders, policy success indicators, moderating factors, and existing actions and resource allocations. This is further explored in Table 6.

Figure 7: Key national cybersecurity education capacity system components



Source: ITU

Key system components

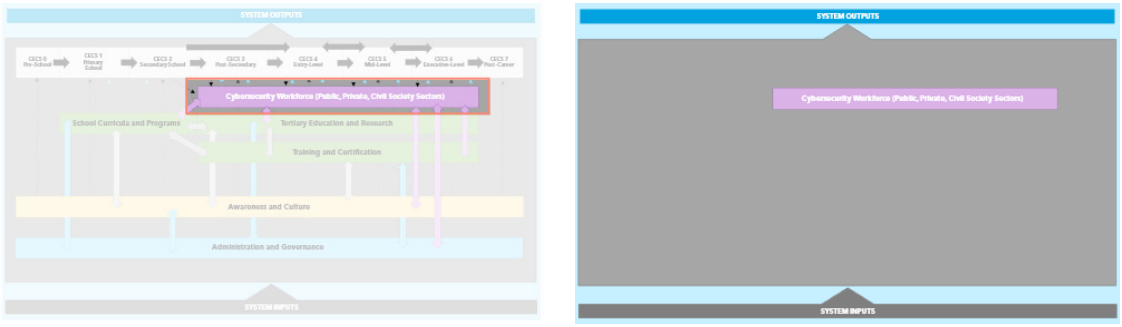
Five components were identified in section 2.2 as part of the review of leading frameworks for assessing national cybersecurity education capacity: school curricula and programmes; tertiary education and research; training and certification; awareness and culture; administration and governance. These components are organized into three different categories in Figure 7:

- **Coordinating components** (light blue box) represent the administration and governance components of national cybersecurity education capacity and interacts with the system by guiding the allocation, intent, and direction of inputs within the system.
- **Awareness components** (yellow box) represent the awareness and culture components of national cybersecurity education capacity, which focuses on informing stakeholders within the system of the importance, relevance, and scope of cybersecurity.
- **Education delivery components** (green boxes) include school curricula and programmes, tertiary education and research, and training and certification. These components have been grouped together as they represent opportunities for the direct transfer of cybersecurity knowledge, skills, and abilities that enable recipients to complete cybersecurity related tasks and practices.

The solid-coloured arrows (light blue (⇧), yellow (), green ()) represent the relationships between components. Depending on the country, such relationships may or may not exist, or may only travel in one rather than both directions. This is something that can be customized for each country system concept to help understand how each component influences the operation and effectiveness other components.

The dotted-coloured arrows (light blue, yellow, green) represent how each component directly interacts with individuals in the system as they move through each CECS. This interaction includes the range of cybersecurity aspiration, awareness, knowledge, skill, and ability building activities that exist within a country. This can be customized to show where interaction is most prominent and identify where there might be gaps in the system.

Figure 8: National cybersecurity workforce



Source: ITU

Cybersecurity workforce

The composition of the national cybersecurity workforce represents professionals from all public, private, and civil society sectors and reflects national priorities and requirements, the resources available, and the effectiveness of the national cybersecurity education capacity system.

The purple arrows indicate the relationships between the cybersecurity workforce and the five national cybersecurity education capacity system components, as well as how they impact each other. Depending on the country, such relationships may or may not exist, or may only travel in one rather than both directions.

Considerations for each cybersecurity education capacity stage

Figure 9 highlights the CECS 2 (secondary school) part of the system and Table 6 presents an example of what governments might consider when looking at each stage in the education cycle.

Figure 9: Defining CECS 2 secondary school part of system concept

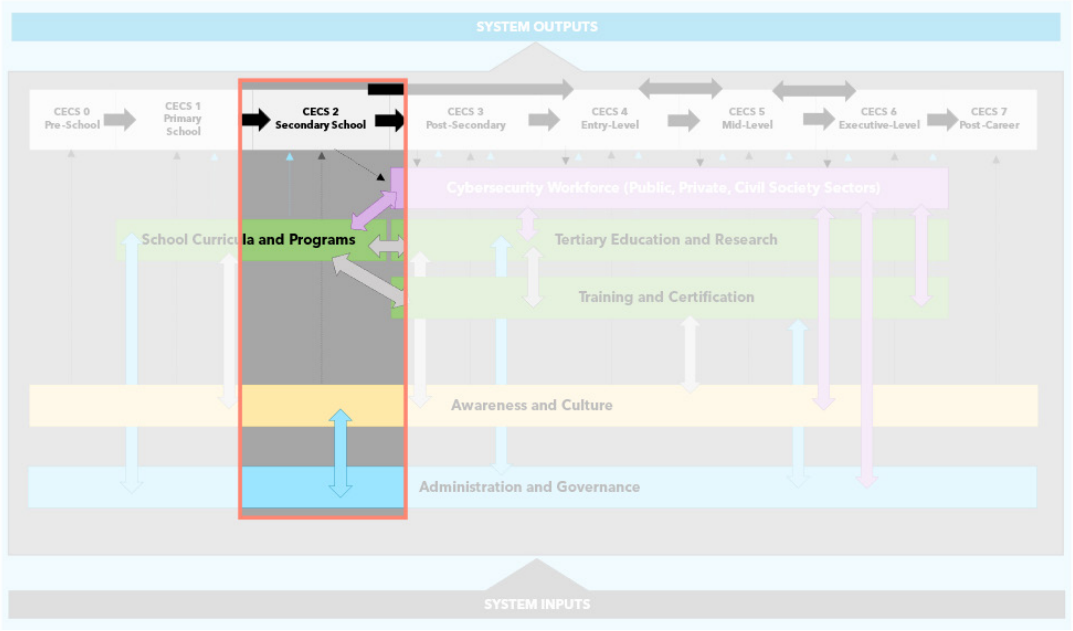


Table 6 presents potential key stakeholders, policy success indicators, moderating factors, and existing actions and resource allocations as examples of characteristics that could be considered for each CECS. By replicating this process across each identified CECS, policy-makers will be able to develop a comprehensive and holistic understanding of their national cybersecurity education capacity system, including gaps and intervention opportunities.

Table 6: CECS 2 – Example secondary school characteristics

CECS descriptors	CECS 2 - Secondary school	
Key stakeholders	• students (aged 13 to 18) • parents • school teachers • secondary schools	• universities • trade schools • government agencies • entry-level employers
Policy success indicators	• numeracy and literacy academic attainment • participation in cybersecurity initiatives • interest in cybersecurity careers • application for tertiary cybersecurity programmes (vocational and university)	
Moderating factors	• school types and resourcing levels • urban and rural digital divide • education attainment of parents • awareness of cybersecurity as a career	
Existing actions and resource allocations	• cybersecurity as a part of secondary school curriculum • teacher cybersecurity training programmes • cybersecurity competitions • national cybersecurity awareness month	

Application of the systems concept to cybersecurity education capacity building

Looking at national cybersecurity education capacity as a system (as illustrated in Figure 5) can provide planning and implementation benefits for future capacity building measures:

- **Goal setting**: Assisting government in the formulation of short, medium, and long-term cybersecurity education capacity development and workforce planning by mapping prospective cybersecurity professionals through the different CECS in each country and aligning it to current and future national cybersecurity workforce demand.
- **Holistic perspectives**: Improving the understanding of system stakeholders and their levels of interests, roles, and influence in relation to national cybersecurity education capacity building.
- **Key leverage points**: Assisting policy-makers to identify and understand the various leverage or primary intervention points in national cybersecurity education capacity systems that could significantly improve the capacity and outputs of the overall system. This can help resource allocation and focus efforts on points in the system where smaller changes might unlock bigger opportunities in the future. For example, if the cybersecurity education capacity system were to increase awareness of cybersecurity careers in early secondary school, this might lead to higher levels of engagement and participation in education development pathways, which would in turn increase the overall size of the cybersecurity workforce.
- **Efficacy improvements**: Supporting future national cybersecurity capacity building programme design and resource allocation by assisting policy-makers in understanding how investments in certain parts of the system will contribute towards policy goals, and

how such investments in one part of the system will interact with existing or proposed measures in other parts of the system. Knowledge of these relationships and leverage points in the system has the potential to improve the effectiveness of the programme as a whole and optimize resource allocations.

- **Outcomes and impact:** Improving the short-term outcomes and long-term impact of national cybersecurity education capacity building programmes by ensuring that the prioritization of efforts and resources aligns with the needs of the cybersecurity education system and workforce.

5 Recommendations and conclusions

This study focuses on a systems approach to assist policy-makers, practitioners, and stakeholders working in a wide range of national contexts to improve the targeting, design, implementation, and impact of future cybersecurity education capacity building actions. It defines key terms, explores the current supply and demand challenges and sets out key components of national cybersecurity education capacity, as well as a range of capacity-related indicators. In addition, some key frameworks and insights from the cybersecurity capacity building community were highlighted.

This showed how a systems approach will support effective capacity building efforts, as well as how it integrates with existing cybersecurity capacity building processes. This included showing how applying tools and stakeholder analysis and breaking down the systems concept might work and the potential benefits of the systems concept to cybersecurity education capacity building.

These findings reinforce the notion that national cybersecurity education capacity building is a complex system composed of many interacting components that exist in a dynamic environment. In response, capacity building actions must reflect this complexity and develop holistic and multi-stakeholder solutions to find targeted and sustainable ways to improve national cybersecurity education capacity and create a resilient cybersecurity workforce and society.

Based on these conclusions, the following recommendations and next steps are intended for countries to consider as part of their own national cybersecurity education capacity building efforts.

5.1 Recommendations

The following recommendations have been developed for consideration by Member States looking to better understand and build national cybersecurity education capacity.

General recommendations for national cybersecurity capacity building

- Develop a national cybersecurity capacity systems concept: map the existing environment, identify current capacity building actions, and identify gaps and opportunities to strengthen and expand these activities.
- Complete a national cybersecurity education capacity maturity assessment: map current capacity and establish a baseline or benchmark against which progress in future national capacity building efforts can be measured.
- Explore a wide range of relevant systems thinking tools to develop a national cybersecurity capacity systems concept: define national challenges and opportunities for capacity building.
- Consider the absorption capacity of the national cybersecurity education system when designing a capacity building programme: integrate any new measures both in terms of volume and type.
- Consider how cybersecurity capacity building integrates with the broader national development context and priorities.
- Collate existing and new research to support the analysis of national cybersecurity capacity environment.
- Support bilateral and multilateral knowledge exchange to share lessons learnt from national cybersecurity education in different geographical and development contexts.

- Encourage knowledge exchange and cooperation between governments, private sector, and civil society stakeholders.
- Share successful approaches to reduce duplication of effort and increase economies of scale.
- Consider the three levels of capacity (individual, organisational, and enabling environment) and how these will be addressed as part of the intervention design, implementation, and evaluation. When designing capacity building for primary school students, for example, the individual might be the primary school students or teachers, the organisation might be the schools, and the enabling environment might be the education policy and system in each country.

Annex A provides a checklist of national cybersecurity education capacity building actions.

5.2 Next steps and future research

The next steps and areas for future work to support Member States to further their cybersecurity capacity building include:

1 Reaching out to members of the global cybersecurity capacity building community to collect feedback on the application and benefits of the systems concept and approach to national cybersecurity capacity building.

2 Working with low- and middle-income economies to utilize systems thinking concepts as a basis for the development of national cybersecurity education frameworks.

3 Continuing with regular reviews of cybersecurity education capacity building research, incorporating a broad range of sources and perspectives with potential focus areas including:

   - how to engage with underrepresented communities and groups such as women, older people, and people with disabilities;
   - how to feature and prioritize cybersecurity education in existing national cybersecurity strategies;
   - how to ensure sustainable capacity building.

4 Refining, testing, and validation of the cybersecurity capacity systems concept through research in relevant cybersecurity education contexts including expert interviews, surveys, and focus groups, with particular consideration to:

   - key stakeholders;
   - success indicators for capacity building;
   - system component relationships;
   - system leverage points; and
   - future applications to a variety of national contexts (e.g., different levels of income, population size and distribution, technology adoption and reliance, as well as systems of government and other relevant factors).

5. Exploring the use and integration of other systems thinking tools in relation to national cybersecurity education capacity building.
6. Considering how to convert this study and future research into a guide for Member States to develop a national cybersecurity education and training capacity building strategy.
7. Developing a toolkit that includes templates and guidance notes to support Member States to apply the systems concept.
8. Exploring the development of an interactive digital dashboard resource that can be customed to assist Member States to map a national cybersecurity education capacity system and linkages, and track changes over time.

Annex A – Checklist of national cybersecurity education capacity building actions

There is a broad range of actions that countries can pursue to support national cybersecurity education capacity building efforts having completed their mapping exercise as recommended above. These include short-to-medium term measures that rapidly improve capacity and mitigate risk and threats. In addition, Member States should also consider medium- to long-term measures that focus on building a more sustainable and resilient approach.

Short- to medium-term measures

- Create cyber career conversion programmes focused on professions with translatable skill sets that can easily transition into cybersecurity roles.
- Support train-the-trainer initiatives to build a cadre of cybersecurity trainers.
- Build targeted talent programmes e.g., focused at increasing the participation of women in the cybersecurity workforce.
- Transfer and adopt existing successful training and courses and best practice.
- Ensure support for underrepresented groups such as women in cyber fellowship programmes.
- Ensure grassroots support such as cybersecurity apprenticeship programmes.
- Promote cybersecurity hiring practices that focus on core requirements and avoid unnecessary barriers to entry.
- Support and expand on-the-job cybersecurity training and employee development.

Medium- to long-term measures

- Develop a national cybersecurity education strategy to outline a holistic approach and communicate priority areas and goals.
- Analyse strategic drivers that will reflect the need for specific cybersecurity skills to reach national digital development goals and mitigate against anticipated cybersecurity risks and threats.
- Developing a national cybersecurity workforce framework to create a common reference point and taxonomy for supply and demand side stakeholders.
- Develop a training needs assessment strategy to determine cybersecurity roles, proficiency levels and volume required to upskill the workforce.
- Design a national learning model, as well as training development pathways to determine the cybersecurity curriculum, certification process, and learning preferences that can most efficiently build a scalable and quality assured national model.
- Run targeted initiatives at primary and secondary schools aimed at building the relevant knowledge, skills, and interest for a career in cybersecurity.
- Run targeted initiatives to build awareness, knowledge, and skills of priority groups to effectively contribute to a cybersecure workforce and cybersecure society.
- Runn executive level initiatives focused to promote leadership and buy-in to the importance of cybersecurity.
- Invest in national cybersecurity research and development that will improve education and training.
- Develop an interactive dashboard to provide actionable data on supply and demand in the cybersecurity job.[46]

[46] See an example of such an interactive dashboard for the United States of America: Cyber Seek. (2023). Hack the gap. https://www.cyberseek.org/

Office of the Director
International Telecommunication Union (ITU)
Telecommunication Development Bureau (BDT)
Place des Nations
CH-1211 Geneva 20
Switzerland

Email: bdtdirector@itu.int
Tel.: +41 22 730 5035/5435
Fax: +41 22 730 5484

Office of Deputy Director and Regional Presence
Field Operations Coordination Department (DDR)
Place des Nations
CH-1211 Geneva 20
Switzerland

Email: bdtdeputydir@itu.int
Tel.: +41 22 730 5131
Fax: +41 22 730 5484

Digital Networks and Society (DNS)
Email: bdt-dns@itu.int
Tel.: +41 22 730 5421
Fax: +41 22 730 5484

Digital Knowledge Hub Department (DKH)
Email: bdt-dkh@itu.int
Tel.: +41 22 730 5900
Fax: +41 22 730 5484

Partnerships for Digital Development Department (PDD)
Email: bdt-pdd@itu.int
Tel.: +41 22 730 5447
Fax: +41 22 730 5484

Africa

Ethiopia
International Telecommunication Union (ITU) Regional Office
Gambia Road
Leghar Ethio Telecom Bldg. 3rd floor
P.O. Box 60 005
Addis Ababa
Ethiopia

Email: itu-ro-africa@itu.int
Tel.: +251 11 551 4977
Tel.: +251 11 551 4855
Tel.: +251 11 551 8328
Fax: +251 11 551 7299

Cameroon
Union internationale des télécommunications (UIT)
Bureau de zone
Immeuble CAMPOST, 3e étage
Boulevard du 20 mai
Boîte postale 11017
Yaoundé
Cameroon

Email: itu-yaounde@itu.int
Tel.: + 237 22 22 9292
Tel.: + 237 22 22 9291
Fax: + 237 22 22 9297

Senegal
Union internationale des télécommunications (UIT)
Bureau de zone
8, Route du Méridien Président
Immeuble Rokhaya, 3e étage
Boîte postale 29471
Dakar - Yoff
Senegal

Email: itu-dakar@itu.int
Tel.: +221 33 859 7010
Tel.: +221 33 859 7021
Fax: +221 33 868 6386

Zimbabwe
International Telecommunication Union (ITU) Area Office
USAF POTRAZ Building
877 Endeavour Crescent
Mount Pleasant Business Park
Harare
Zimbabwe

Email: itu-harare@itu.int
Tel.: +263 242 369015
Tel.: +263 242 369016

Americas

Brazil
União Internacional de Telecomunicações (UIT)
Escritório Regional
SAUS Quadra 6 Ed. Luis Eduardo Magalhães,
Bloco "E", 10º andar, Ala Sul (Anatel)
CEP 70070-940 Brasilia - DF
Brazil

Email: itubrasilia@itu.int
Tel.: +55 61 2312 2730-1
Tel.: +55 61 2312 2733-5
Fax: +55 61 2312 2738

Barbados
International Telecommunication Union (ITU) Area Office
United Nations House
Marine Gardens
Hastings, Christ Church
P.O. Box 1047
Bridgetown
Barbados

Email: itubridgetown@itu.int
Tel.: +1 246 431 0343
Fax: +1 246 437 7403

Chile
Unión Internacional de Telecomunicaciones (UIT)
Oficina de Representación de Área
Merced 753, Piso 4
Santiago de Chile
Chile

Email: itusantiago@itu.int
Tel.: +56 2 632 6134/6147
Fax: +56 2 632 6154

Honduras
Unión Internacional de Telecomunicaciones (UIT)
Oficina de Representación de Área
Colonia Altos de Miramontes
Calle principal, Edificio No. 1583
Frente a Santos y Cía
Apartado Postal 976
Tegucigalpa
Honduras

Email: itutegucigalpa@itu.int
Tel.: +504 2235 5470
Fax: +504 2235 5471

Arab States

Egypt
International Telecommunication Union (ITU) Regional Office
Smart Village, Building B 147,
3rd floor
Km 28 Cairo
Alexandria Desert Road
Giza Governorate
Cairo
Egypt

Email: itu-ro-arabstates@itu.int
Tel.: +202 3537 1777
Fax: +202 3537 1888

Asia-Pacific

Thailand
International Telecommunication Union (ITU) Regional Office
4th floor NBTC Region 1 Building
101 Chaengwattana Road
Laksi,
Bangkok 10210,
Thailand

Email: itu-ro-asiapacific@itu.int
Tel.: +66 2 574 9326 – 8
+66 2 575 0055

Indonesia
International Telecommunication Union (ITU) Area Office
Gedung Sapta Pesona
13th floor
Jl. Merdeka Barat No. 17
Jakarta 10110
Indonesia

Email: bdt-ao-jakarta@itu.int
Tel.: +62 21 380 2322

India
International Telecommunication Union (ITU) Area Office and Innovation Centre
C-DOT Campus
Mandi Road
Chhatarpur, Mehrauli
New Delhi 110030
India

Email:
Area Office: itu-ao-southasia@itu.int
Innovation Centre: itu-ic-southasia@itu.int
Website: ITU Innovation Centre in New Delhi, India

CIS

Russian Federation
International Telecommunication Union (ITU) Regional Office
4, Building 1
Sergiy Radonezhsky Str.
Moscow 105120
Russian Federation
Email: itu-ro-cis@itu.int
Tel.: +7 495 926 6070

Europe

Switzerland
International Telecommunication Union (ITU) Office for Europe
Place des Nations
CH-1211 Geneva 20
Switzerland

Email: eurregion@itu.int
Tel.: +41 22 730 5467
Fax: +41 22 730 5484

International Telecommunication Union
Telecommunication Development Bureau
Place des Nations
CH-1211 Geneva 20
Switzerland

ISBN: 978-92-61-39031-0

Published in Switzerland
Geneva, 2024

Photo credits: Adobe Stock