Bridging the Gap

Harmonizing Cybersecurity Qualifications and Frameworks Across Nations

By Erisa Karafili, Sampath Rajapaksha, Ruby Rani, Mahender Kumar

University of Southampton

e.karafili@soton.ac.uk

1. Introduction

The global shortage of skilled cybersecurity professionals presents a serious risk to the stability of international digital infrastructure. To tackle this critical challenge, this report presents our research aimed at mapping commonalities and differences across cyber skills frameworks in key regions: the UK, EU, USA, Canada, Singapore, Japan, Ghana, India, and Dubai. By identifying shared elements and discrepancies in these frameworks, we seek to support the mutual recognition of cybersecurity qualifications, fostering a more fluid and cohesive global workforce.

This report begins with an overview of the cyber skills frameworks analyzed. We have selected countries at varying stages of cybersecurity framework development—ranging from mature systems like that of the UK and USA, to those in the early stages, such as Ghana and India. The frameworks also differ in their level of specificity, from comprehensive cybersecurity frameworks in countries like the USA and Singapore, to broader security frameworks, as seen in Japan. Some countries, such as India, currently lack a dedicated cyber skills framework but possess related security frameworks that could serve as a foundation for a future Cyber Skill Framework.

We provide a comparative analysis of the frameworks. In particular, we provide a numerical analysis, where we compare the number of groups/clusters, roles, and the core elements for each framework. We also offer a preliminary effort to harmonize these frameworks by categorizing them into common specialization areas. This categorization could serve as a foundation for developing a universal Cyber Skills Framework or a translation tool to align the frameworks across different nations.

Finally, we summarize the main findings, highlighting key similarities and discrepancies between frameworks. The report concludes with a set of recommendations for advancing the development of existing frameworks and guiding the creation of new ones.

2. Cyber Skill Frameworks

The countries selected for this study have distinct cybersecurity skill frameworks tailored to their labor market needs. This section reviews each framework and provides a brief overview. For more detail information we recommend the reader to check the references provided for each of the frameworks.

2.1. Australia

In July 2019, the Australian Signals Directorate (ASD) introduced the ASD Cyber Skills Framework v1.0 as an iterative tool for assessing, maintaining, and monitoring the skills, knowledge, and attributes of its cyber workforce. This report references the most recent version, ASD Cyber Skills Framework v2.0 (Australian Signal Directorate). This framework is built on the following core elements

- 9 Cyber role definitions
- 9 Capability and skill definitions
- 6 Proficiency levels
- 4 Career pathways
- 1 Learning and development pathway

These elements were developed from three core frameworks: Chartered Institute of Information Security (CIISec) Skills Framework; Skills Framework for the Information Age (SFIA); and Integrated Leadership System (ILS). Defined 9 Cyber roles are shown in Figure 1.

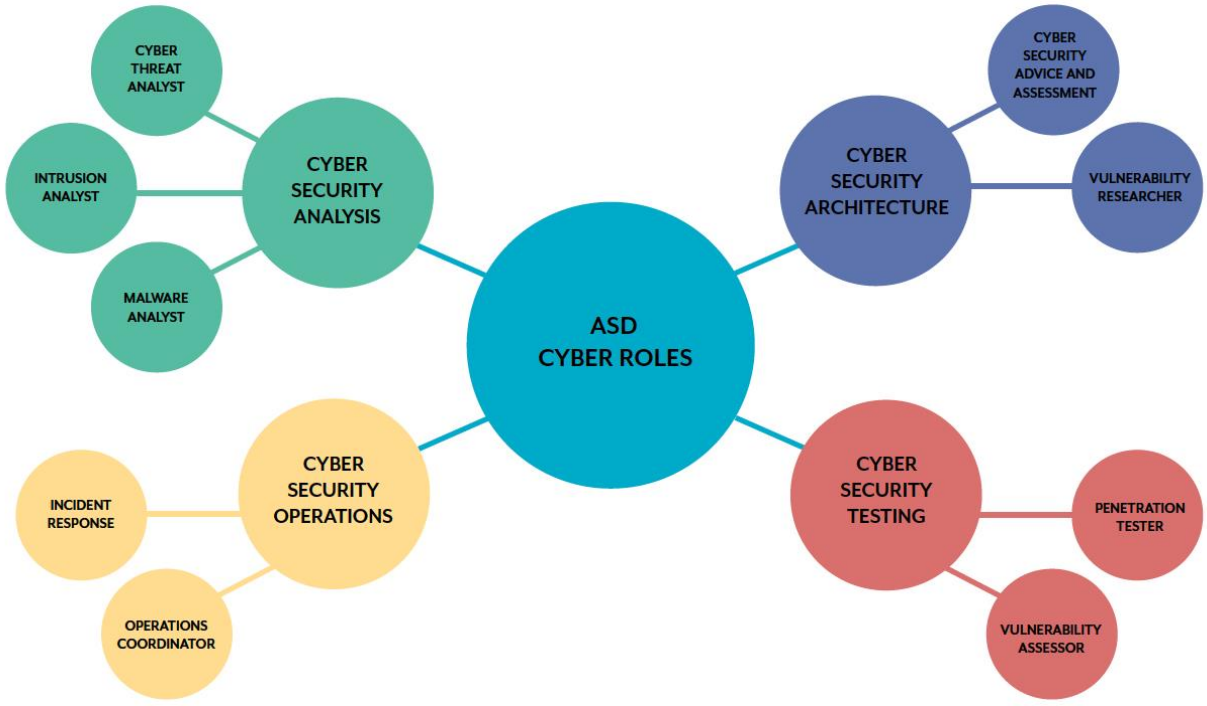

Figure 1: ASD Cyber Roles, taken from (Australian Signal Directorate)

This framework outlines expectations for each role and provides a skill matrix that includes roles, capabilities, the skills associated with each capability, and the required proficiency level for each skill. The capabilities covered include Information Security Governance and Strategy, Threat Assessment and Information Risk Management, Systems Development and Implementation, Assurance (Audit, Compliance, and Testing), Operational Security Management, Incident Management, Investigation and Forensics, Information Security Research, Management, Leadership, Business and Communications, and Specialist Advice. The six defined proficiency levels are: Level 1 (Learner), Level 2 (Novice), Level 3 (Practitioner), Level 4 (Senior Practitioner), Level 5 (Principal Practitioner), and Level 6 (Expert Practitioner).

The defined digital career pathways offer guidance on how existing ICT skills can be applied to other roles and identify the new skills employees may need to succeed in those roles. This gives individuals a clear understanding of their current career position and how to navigate their future potential. Within the learning and development pathway, the ASD framework specifies the required skills, learning outcomes, recommended learning and development opportunities, suggested professional growth activities, experiential learning, and relevant certifications for each proficiency level.

2.2. USA

The National Initiative for Cybersecurity Education (NICE) outlines the Workforce Framework for Cybersecurity (NICE Framework), a key reference for defining and sharing information about cybersecurity roles. The NICE Framework offers a structured approach to describing the tasks, knowledge, and skills required to carry out cybersecurity functions by individuals and teams. This report refers to the most recent version, published in (The National Institute of Standards and Technology - NIST SP 800-181r1).

The main building blocks of the NICE Framework are Tasks, Knowledge, and Skills (TKS) statements. Relationships of these building blocks are shown in Figure 2.

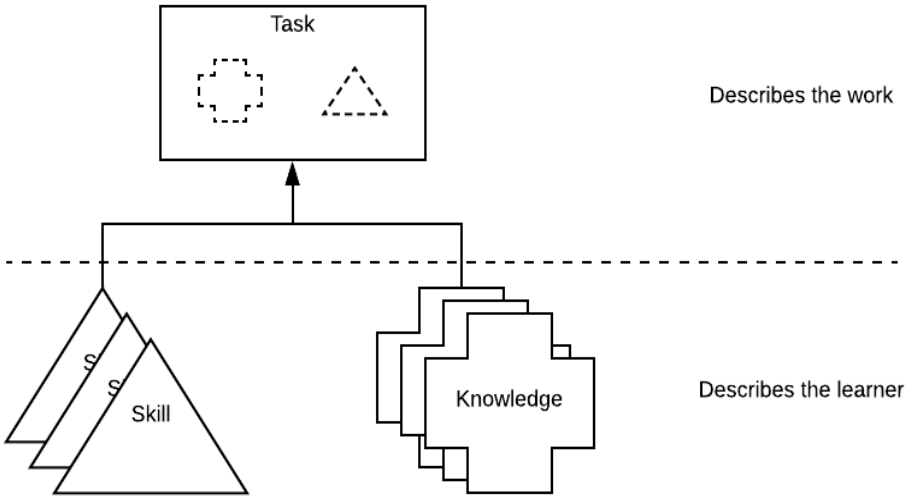

Figure 2: NICE Framework building blocks approach, taken from (The National Institute of Standards and Technology).

The NICE Framework defines the following based on its core building blocks:

- 7 Work role categories
- 52 work roles
- 2200+ TKS statements
- 11 competency areas

The 7 work role categories are:

- Oversight and Governance (16 roles)
- Design and Development (8 roles)
- Implementation and Operation (7 roles)
- Protection and Defence (7 roles)
- Investigation (2 roles)
- Cyberspace Intelligence (5 roles)
- Cyberspace Effects (7 roles)

The work role names defined under each work role category are not necessarily equivalent to job titles. In some cases, a work role may align with a job title, depending on how an organization uses job titles. Moreover, work roles are also not synonymous with occupations

The NICE Framework establishes 11 competency areas as a way for organizations to assess learners' skills. These areas include:

- Access control
- Artificial Intelligence (AI) Security
- Asset Management
- Cloud Security
- Communications Security
- Cryptography
- Cyber Resiliency
- DevSecOps
- Operating Systems (OS) Security
- Operational Technology (OT) Security
- Supply Chain Security

Each competency includes a name, a description, an assessment method, and a set of related TKS (Tasks, Knowledge, and Skills) statements. Organizations can leverage these competencies during the hiring process to meet specific goals or to evaluate whether a learner has acquired a defined set of skills and knowledge.

2.3. Canada

The Canadian Cyber Security Skills Framework is derived from the U.S. NICE Workforce Framework for Cybersecurity (NICE framework), tailored to fit the Canadian labor market. It adopts key elements of the NICE framework but simplifies them through a business-oriented approach, recognizing talent from an organizational security perspective. This makes the framework more accessible to non-cybersecurity stakeholders. This report refers to the most recent version, published in (Canadian Centre for Cyber Security) and (TECHNATION Canada).

The Canadian Cyber Security Skills Framework is described in Figure 3. This also uses the same 7 work role categories used in the NICE framework with slightly different naming.

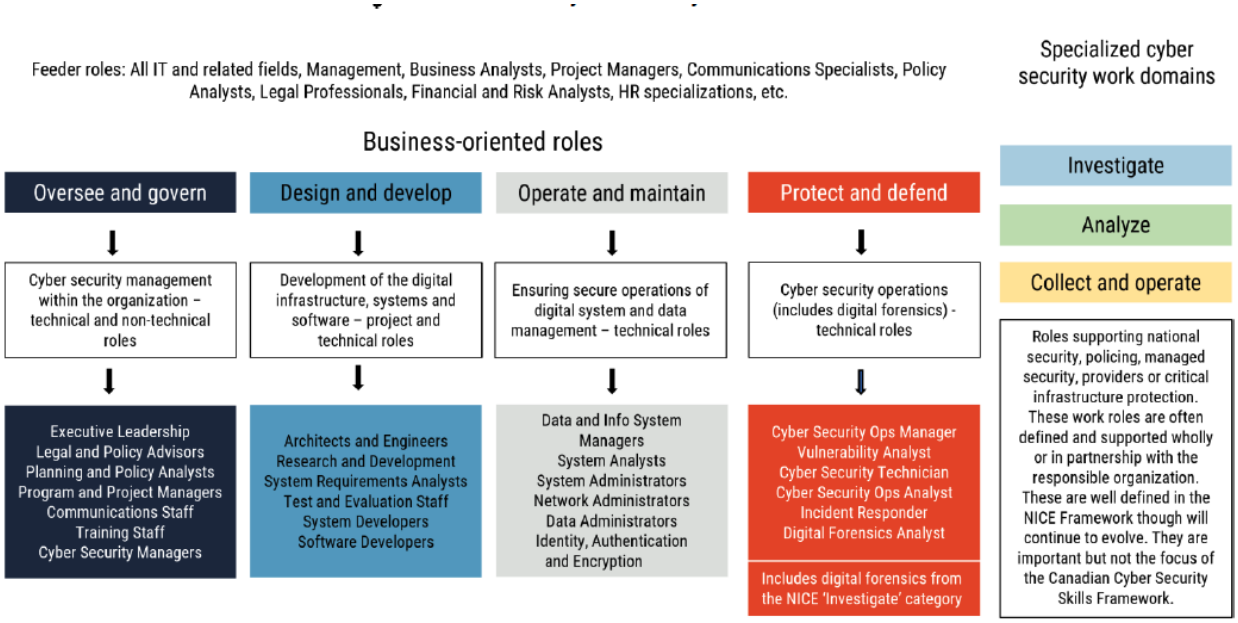

Figure 3: Canadian Cyber security skill framework, taken from (Canadian Centre for Cyber Security).

Although the U.S. NICE framework highlights several additional or adjacent cybersecurity roles, the Canadian Cyber Security Skills Framework focuses on core cybersecurity roles and related competencies within the broader Canadian business context. Here, the majority of work aligns with organisational cybersecurity objectives and outcomes. The Canadian framework prioritises four of the original seven work categories, which encompass most cybersecurity activities in Canadian businesses and industries. These categories are: oversee and govern, design and develop, operate and maintain, and protect and defend.

In addition to the cybersecurity specialist roles outlined within the core roles, this framework also defines cybersecurity-adjacent roles and a cybersecurity generalist role, which are commonly found within small and medium-sized organizations (SMOs).

In TECHNATION Canada, the National Occupational Standard (NOS) outlines several fields for each occupational title defined in this framework, including:

NICE Framework reference, Functional Description & Scope, Consequence of error or risk, Common development pathway, Other titles, Related national occupation classification code(s) and title(s), Required qualifications (Education, Training, Work experience), Tools & technology, Key competencies, Future trends affecting key competencies.

2.4. Singapore

The Operational Technology Cybersecurity Competency Framework (OTCCF) maps out various OT cybersecurity job roles and the corresponding technical skills and core competencies required. OTCCF is made up of three key components:

1. Career pathways: The Career Pathways show the possible options for vertical and lateral progression for advancement and growth.
2. Skill maps: The Skills Maps cover the job roles, critical work functions, key tasks, and skills and competencies.
3. Skills and competencies: Competencies identified for each of the job roles fall under two broad classifications:
    a. Technical Skills and Competencies;
    b. Critical Core Skills.

This report references the most recent version, published in (Cyber Security Agency of Singapore). The career map of OTCCF is shown in Figure 4.

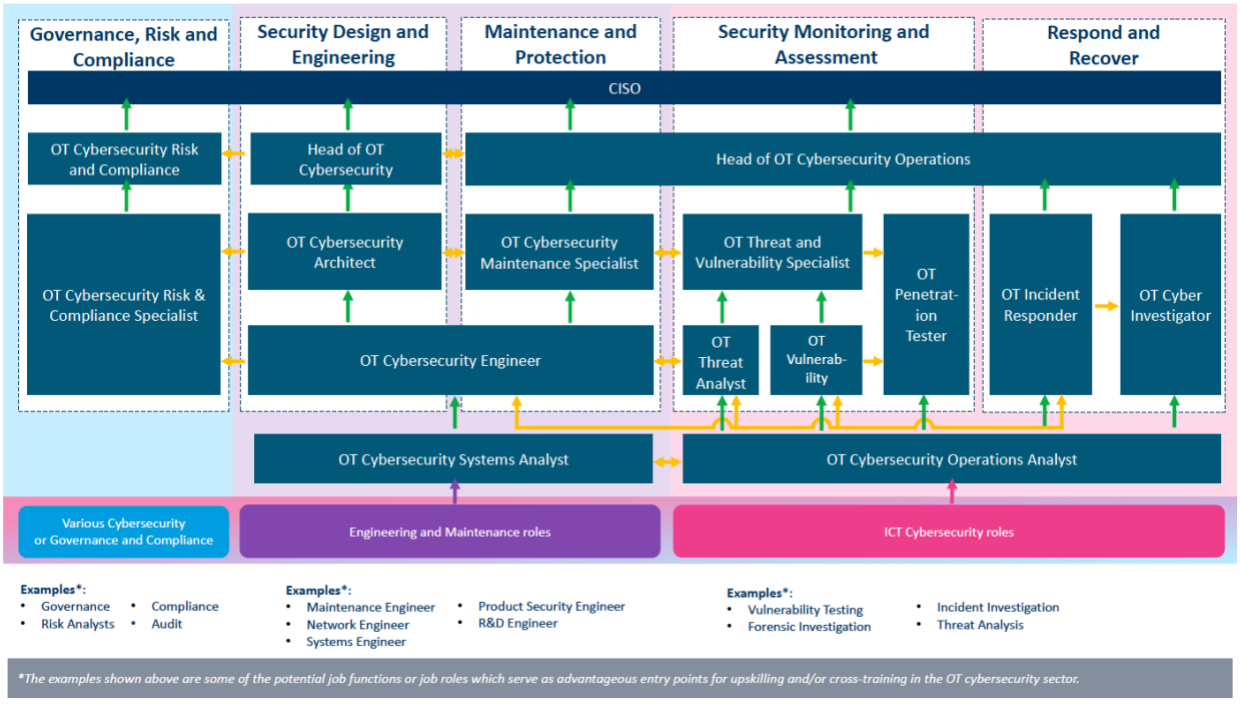

Figure 4: Career Map, taken from (Cyber Security Agency of Singapore)

The skills map outlined in the framework includes the following fields for each occupation/job role: track, job role description, critical work functions, and key tasks/performance expectations, as well

as skills and competencies. Technical skills and competencies are categorized into six levels, ranging from Level 1 to Level 6. Additionally, critical core skills are classified into three levels: basic, intermediate, and advanced. However, the framework does not specify the required education levels or certifications.

2.5. UK

The UK Cyber Career Framework (UK Cybersecurity Council) outlines 16 specialisms in cybersecurity and proposes pathways for transitioning between them. It provides an introduction to each specialism, detailing typical responsibilities and tasks, required skills and knowledge, necessary certifications and qualifications, as well as relevant prior experience for those looking to enter the field from outside cybersecurity. Additionally, it includes a list of common job titles and average salary ranges. These 16 specialisms are illustrated in Figure 5.

Figure 5: UK cyber security career framework 16 specialisms (taken from the UK Cyber Security Council website)

The knowledge areas outlined in the framework are based on The Cyber Security Body of Knowledge - CyBOK (University of Bristol, Bristol Cyber Security Group). This framework has

mapped certifications to the CyBOK knowledge areas, illustrating how these certifications are associated with each specialism.

The Chartered Institute of Information Security (CIISec) skill framework defines 16 skill areas, labelled A to K, along with six skill levels: Level 1 (Knowledge) for basic knowledge, Level 2 (Knowledge and Understanding) for basic principles, Level 3 (Apply) for junior practitioners, Level 4 (Enable) for practitioners, Level 5 (Advise) for senior practitioners, and Level 6 (Initiate, Enable, Ensure) for principal/lead practitioners.

2.6. India

We did not identify a Cyber Skills Framework for India. Instead, we identified the Data Security Council of India, which was setup by nasscom, and committed to making the cyberspace safe, secure, and trusted by establishing best practices, standards, and initiatives in cyber security and privacy. DSCI developed a security framework, which comprises of 16 disciplines that are organised in four layers (see Figure 6).

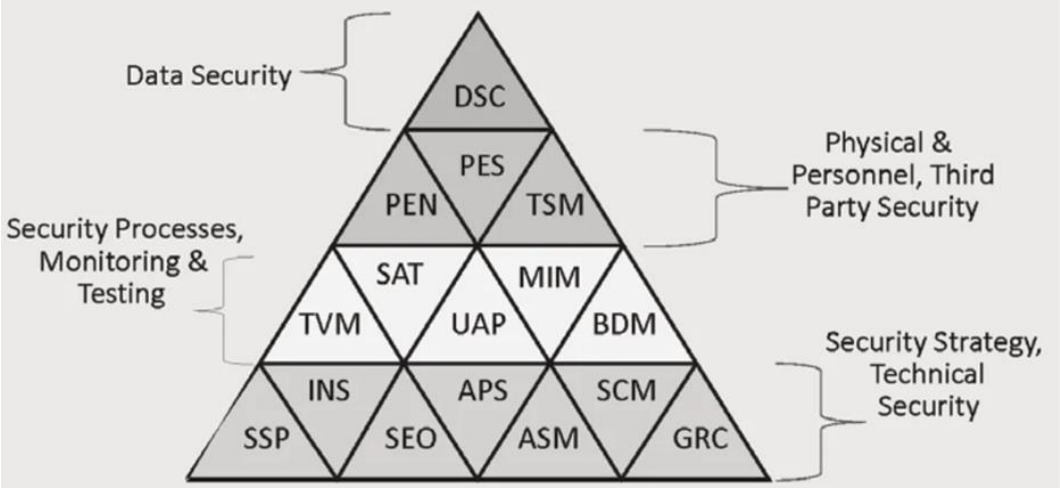

Figure 6: DSCI Security framework (taken from the DSCI Security Framework (DSF©))

Four layers of security were defined:

- Data security (1 discipline)
- Physical and Personnel, third parties security (3 disciplines)
- Security strategy, technical security (5 disciplines)
- Security processes, monitoring and testing (7 disciplines)

Following disciplines has been outlined:

- Security Strategy and Policy (SSP)
- Security Organization (SEO)
- Asset Management (ASM)
- Governance Risk and Compliance (GRC)
- Infrastructure Security (INS)
- Application Security (APS)
- Secure Content Management (SCM)
- Threat and Vulnerability Management (TVM)
- User Access and Privilege Management (UAP)
- Business Continuity & Disaster Recovery Management (BDM)
- Security Audit and Testing (SAT)
- Security Monitoring and Incident Management (MIM)
- Physical and Environmental Security (PEN)
- Third Party Security Management (TSM)
- Personnel Security (PES)
- Data Security (DSC)

2.7. Japan

We did not identify a Cyber Skills framework for Japan. Instead, we identified the Information technology Promotional Agency (IPA). IPA has developed the common careers/skill framework to serve as a reference model for the Information Technology Engineers Examination (ITEE) and three skill standards: Skill standards for IT professionals (ITSS), User's information Systems skills framework (UISS), and Embedded technology skills standards (ETSS) (see Figure 7). The cyber skills and professions are considered as part of the IT professionals. Therefore, IPA is presented in this report.

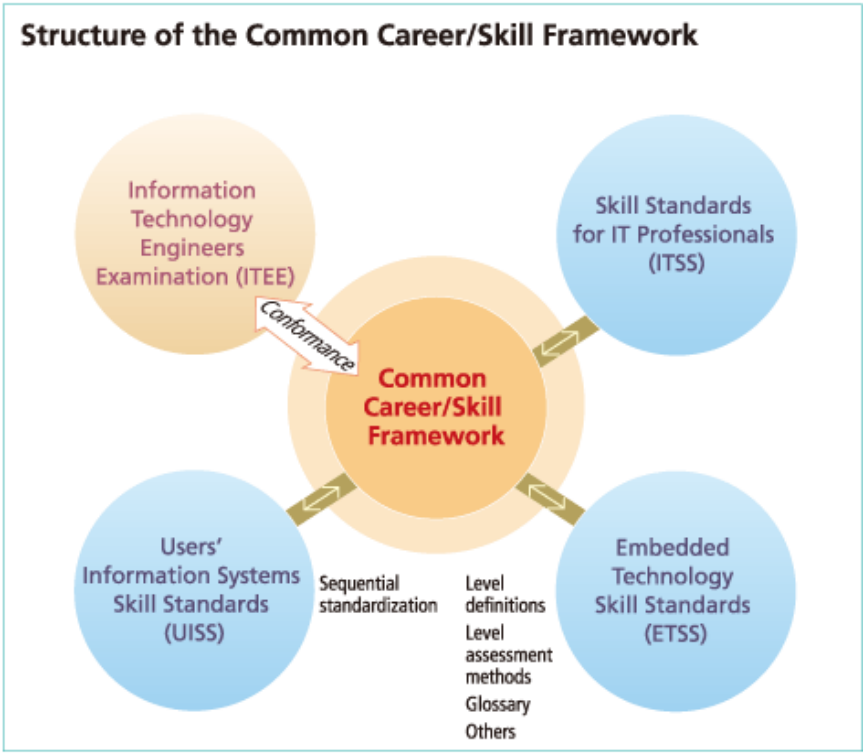

Figure 7: Structure of the common career/skill framework of Japan (taken from "ITSS framework")

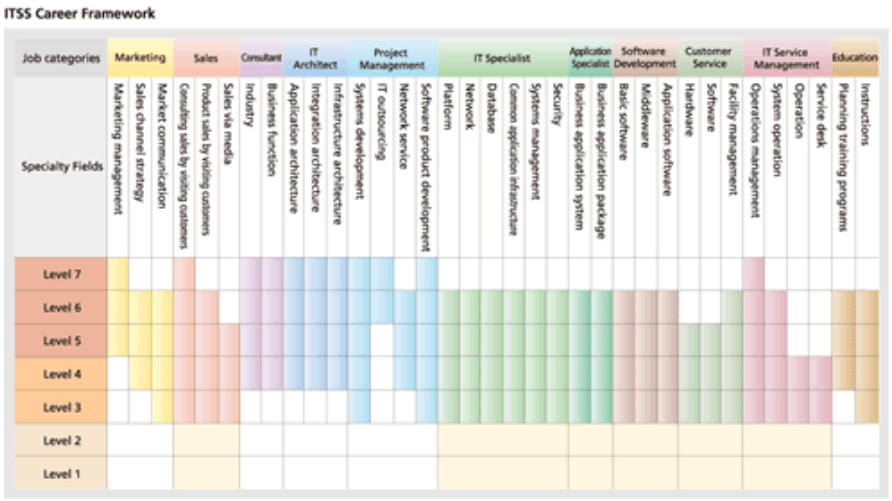

Figure 8: ITSS career framework (taken from "ITSS framework")

The Cyber Skills Framework is an integral component of the broader IT Skill Standard (ITSS), designed to systematically define and organise the skills necessary for the IT services industry (see Figure 8). ITSS is managed by the Information-technology Promotion Agency (IPA), which includes the Cyber Skills Framework as a critical element to address the increasing demand for cybersecurity expertise in the workforce.

The ITSS classifies skills into 11 job categories and 35 speciality fields, offering a structured approach to skill development. By embedding cybersecurity skills across these categories and fields, the ITSS ensures that cybersecurity is recognised as a vital area in the IT profession. This integration highlights the importance of cybersecurity within Japan's IT sector, emphasising the development of specialised skills to bolster the nation's cybersecurity capabilities.

Each field has seven levels based on individual experience and results. One appealing feature of ITSS is that this standard allows engineers to draw roadmaps for their futures and career advancement (Career Path). Approximately 90% of large enterprises and over 60% of SMEs have introduced or considered using ITSS. As reflected by these figures, ITSS is effectively utilised as an indicator for business managers and engineers to systematically evaluate both their own and the future of their respective companies.

2.8. The European Union

The European Union Agency for Cybersecurity (ENISA) developed a European cybersecurity skills framework (ESCF). Its motive is to standardise the identification and articulation of tasks, competencies, skills, and knowledge associated with various roles in the cybersecurity fields across Europe.

The main building blocks of ESCF framework are cybersecurity professional roles, detailing their responsibilities, required skills, and competencies.

The framework outlines the following 12 typical cybersecurity professional roles (see Figure 9):

- Chief Information Security Officer (CISO)
- Cyber Incident Responder
- Cyber Legal, Policy & Compliance Officer
- Cyber Threat Intelligence Specialist
- Cybersecurity Architect
- Cybersecurity Auditor

- Cybersecurity Educator
- Cybersecurity Implementer
- Cybersecurity Researcher
- Cybersecurity Risk Manager
- Digital Forensics Investigator
- Penetration Tester

Figure 9: Cybersecurity professional roles in ECSF framework (taken from “European Cybersecurity Skills Framework Role Profiles — ENISA”)

The European Cybersecurity Skills Framework (ECSF) outlines the tasks, responsibilities, and skills required for various professional roles in the cybersecurity domain. To assess learners' skills and competencies, the ECSF aligns with the five competency levels defined in the European e-Competence Framework (e-CF). These levels serve as benchmarks for gauging the expertise, autonomy, and responsibility of professionals at different stages of their careers.

The competency levels are structured as follows:

- Level 1: Associate
- Level 2: Professional
- Level 3: Senior Professional/Manager
- Level 4: Lead Professional/Senior Manager
- Level 5: Principal

These five levels provide a structured pathway for career progression, ensuring that professionals develop the necessary skills and competencies to meet the demands of an evolving cybersecurity landscape.

2.9. Dubai

Dubai Cyber Innovation Park (DCIPark), as the research and knowledge division of the Dubai Electronic Security Center (DESC), aims to create a world-class integrated cybersecurity ecosystem, empowering the next generation of experts in cybersecurity from the public and private sectors along with academic institutions (“Strategic Cybersecurity Talent Framework”).

DCIPark runs projects such as the Cyber Security Competency Framework (Qudraat), which maps all cybersecurity employees in the city to the framework, linking employee assessment and evaluation with training and development. Qudraat also ensures that capacity-building extends to academic institutions and maintains a balance between the city’s demand and the supply of skills.

The training and upskilling initiatives are delivered through the CyberNode programme, a partnership between the government, private sector, and academia, to empower cybersecurity capabilities in the city and beyond.

Another DCIPark project is Emirati Capture The Flag, which aims to promote cybersecurity skills among Emirati students and youth and invest in their cybersecurity innovations.

2.10. Ghana

Ghana's cyber framework is anchored by the *Cyber Security Authority (CSA)*, which is responsible for regulating cybersecurity activities across the country and advancing the development of cybersecurity initiatives (“Cyber Security Authority”). A key element of this framework is the protection of *Critical Information Infrastructure (CII)*, which encompasses essential assets, networks, systems, processes, information, and functions vital to the nation's security and economy (“Critical Information Infrastructure”). This comprehensive approach ensures that both

regulatory oversight and critical infrastructure protection are central to Ghana's cybersecurity efforts.

To the best of current knowledge, Ghana still needs to develop a formal cybersecurity skills framework. While the country has made significant strides in digital transformation and awareness of cybersecurity issues, a comprehensive framework outlining the specific competencies, skill levels, and training pathways required to build and sustain a cybersecurity workforce still needs to be implemented.

3. Comparative Analysis of the Frameworks

The frameworks discussed above are developed based on different core elements and define role categories and roles according to each country's context. Table 1 presents a numerical comparison of key elements of these frameworks, including the framework (country and name), the basis on which the framework was developed (base frameworks used), groups (high-level role categorisation), roles (number of defined roles), and core elements (the foundational components of these frameworks). The naming conventions used in each framework have been retained. For instance, in Australia's ASD framework, groups are referred to as "disciplines," while in the USA's NICE framework, they are termed "work role categories."

Framework	Framework based on	Groups (Clusters)	Roles	Core Elements (Building blocks)
Australia (ASD)	CIISec (UK), SFIA, ILS.	4 Disciplines	9 cyber roles	9 core capabilities, 25 skills, 6 proficiency levels
USA (NICE)		7 Work role categories	52 work roles	1084 tasks, 640 knowledge, 556 skills (TKS statements), 11 competency areas
Canada	NICE	7 Activity areas	39 Core roles + 37 Adjacent roles + Cybersecurity generalist	Knowledge, skills, and abilities (KSA)

UK (UKCSC)		16 Specialisms	16 Roles (156+ job titles within roles)	21 knowledge areas (KAs) spanning five categories, 6 proficiency levels
Singapore (OTCCF)		5 tracks	14 OT occupations	Technical skills and competencies (TSC), 6 proficiency levels for technical skills competencies, and 3 levels for critical core skills
India (DSF)		4 Groups	16 Security disciplines	Security disciplines are based on the approach, strategy, best practice, and maturity.
Japan (ITSS)		11 Job categories	35 Specialty fields	Specialty fields are based on 7 proficiency levels
Europe (ECSF)		7 cybersecurity profile	12 Key roles	Each role is associated with core skills and competencies, deliverables, tasks and e-competency framework.

Dubai (Cyber security competency framework (Qudraat))		not defined	Nurturing cyber skills	not defined
Ghana (National Cyber Security Policy & Strategy)		not defined	not defined	not defined

Table 1: Frameworks comparison - Numerical Analysis

The UK Cyber Security Council's international comparison policy paper (internal) identified seven main areas of specialization (groups) within the cybersecurity profession. For this analysis, they reviewed cyber skills frameworks from the UK, USA, and Europe. Our analysis of the selected countries also indicates that all frameworks can generally be classified into these seven groups. Therefore, we have used the same groups, which are shown in Tables 2 and 3. The naming conventions from each framework have been preserved in these tables. The groups include development, operations, intelligence, governance, defense, generalist, and capacity building. The numbers in blue within brackets indicate the number of job roles defined in each category. For instance, under "Design and Development" in the USA NICE framework, eight roles are defined. In Canada's activity areas, two numbers within the brackets represent core and adjacent roles. For example, "Design and Develop (9 + 7)" refers to nine core roles and seven adjacent roles.

There are a few important points to note regarding the grouping in Australia's ASD framework:

- The Australian ASD framework defines 4 disciplines and 9 roles within those disciplines. The cybersecurity architecture discipline aligns with the development group. However, the "cybersecurity advice and assessment" role, defined within the cybersecurity architecture discipline, aligns more closely with the governance group based on the role's description and expectations in the ASD framework.

- The cybersecurity operations discipline in the ASD framework corresponds to the operations group. However, the "incident response" role, though part of this discipline, is more closely aligned with the defense group, based on the expectations and role description provided.

The ECSF framework does not explicitly categorize roles but instead groups them based on the similarity of skills and responsibilities associated with each role. Some key points to note regarding the categorizing profiles in ECFS framework:

- The ECSF framework identifies in 7 profiles with a total of 12 roles spread across these profiles.
- Some roles are repeated in profiles, such as Penetration Tester, Cyber Incident Responder and Chief Information Security Officer, which suggests that certain roles can span across different profiles depending on the organization's responsibility.

Groups	Australia (ASD) Disciplines	USA (NICE) Categories	Canada Activity areas	UK Specialisms (UKCSC)
Development	Cyber Security Architecture (2) [Cyber security advice and assessment, Vulnerability researcher]	Design and Development (8)	Design and develop (9 + 7)	Secure System Development, Secure System Architecture & Design
Operations	Cybersecurity operations (2) [Operations coordinator, Incident Response]	Implementation and Operation (7)	Operate and maintain (3 + 8)	Secure Operations, Identity & Access Management
Intelligence	Cybersecurity Analysis (3) [Cyber threat analyst, Intrusion analyst, Malware analyst]	Cyberspace Intelligence (5)	Analyze (7)	Cyber Threat Intelligence

Governance	[Cyber security advice and assessment]	Oversight and Governance (16)	Oversee and govern (3 + 22)	Cyber Security Governance & Risk Management, Cyber Security Management, Data Protection & Privacy, Cyber Security Audit & Assurance
Defense	Cybersecurity Analysis (3) [Cyber threat analyst, Intrusion analyst, Malware analyst] Cyber Security Testing (2) [Penetration tester, Vulnerability Assessor] [Incident Response]	Protection and Defense (7) Cyberspace Effects (7) Investigation (2)	Protect and defend (8) Collect and operate (6) Investigate (3)	Security Testing, Incident Response, Digital Forensics, Network Monitoring & Intrusion Detection, Cryptography & Communications Security, Vulnerability Management
Generalist			Generalist	Generalist

Table 2: Specialization areas (Part 1)[1]

[1] Black color text shows high level group categorization, blue color text shows job roles within high level groups, and red color text shows grouping mismatches. The numbers represent the number of roles, while the two numbers for the Canadian framework represent core and adjacent roles, e.g., Design and Develop (9 + 7), where there are 9 core roles and 7 adjacent roles.

Groups	Singapore (OTCCF) tracks	EU (ECSF) Profiles	India Groups	Japan Job categories
Development	Security Design and Engineering (4)	Cybersecurity Architect Cybersecurity Implementer Penetration Tester	Application Security (APS) Secure Content Management (SCM) Threat & Vulnerability Management (TVM)	IT Specialist Software Development
Operations	Maintenance and Protection (3)	Cyber Incident Responder Digital Forensics Investigator	Security Monitoring & Incident Management (MIM) User Access & Privilege Management (UAP) Business Continuity & Disaster Recovery (BDM)	IT Service Management
Intelligence	Security Monitoring and Assessment (5)	Cyber Threat Intelligence Specialist	Security Audit & Testing (SAT)	Consultant
Governance	Governance, Risk and Compliance (2)	Cybersecurity Auditor Cybersecurity Risk Manager Cyber Legal, Policy & Compliance Officer Chief Information Security Officer	Security Strategy & Policy (SSP) Governance Risk & Compliance (GRC) Security Organization (SEO)	IT Architect
Defense	Respond and Recover (2), Security Monitoring and Assessment (5)	Digital Forensics Investigator Cyber Incident Responder Penetration Tester	Infrastructure Security (INS) Physical & Environmental Security (PEN)	Physical & Personnel, Third Party Security

			Third Party Security Management (TSM) Personnel Security (PES)	
Generalist		Chief Information Security Officer Cybersecurity Auditor	Data Security (DSC) Asset Management (ASM)	Marketing Customer Service Sales
Capacity Building		Cybersecurity Educator Cybersecurity Researcher	Cyber Education & Skills Program	Education

Table 3: Specialization areas (Part 2)

4. Main Findings

The key findings of this study are as follows:

1. There is a global shift towards group and role-based cybersecurity frameworks. The alignment of these groups and role-based structures is displayed in Table 2 and Table 3. This trend highlights the growing emphasis on clearly defining specific roles and responsibilities within cybersecurity teams.
2. Each country has developed its cybersecurity framework by taking into account its specific context, such as the presence of SMOs (small and medium organizations). Even when a country adopts another nation's framework as a base, there are often notable changes in role groupings and the number of defined roles. For instance, Canada based its framework on the USA NICE framework. However, since the NICE framework does not fully reflect the structure and employment functions typical of the Canadian private sector or non-federal public sector, the Canadian framework has defined a different number of core, adjacent, and generalist roles to meet its unique requirements compared to the USA.

3. The competency areas in the NICE framework better reflect an approach that broadly defines the knowledge and skills needed to be proficient in a specific domain, rather than focusing solely on the ability to complete individual tasks.
4. Our analysis noticed a good alignment between some frameworks such as NICE, Canada, and Europe Union, which prioritise the identification of core elements such as competencies, knowledge, skills, and abilities required for each cybersecurity role. This reflects a more competency-driven approach across these frameworks.
5. Core elements such as competencies, capabilities, knowledge, skills, proficiency level, and abilities differ significantly across frameworks. These elements are foundational, making it challenging to establish standardised core components that apply to all countries.
6. Countries like the USA, UK, Canada, and Australia have more mature and comprehensive frameworks with a wide range of defined roles. In contrast, emerging frameworks in Ghana and India are still under development.
7. Framework in Ghana places a significant emphasis on critical infrastructure protection, reflecting the unique needs and priorities of these regions. However, there remains a significant need for further development of a cyber skills framework to ensure a well-trained workforce capable of addressing evolving cybersecurity threats.

5. Similarities and Discrepancies

This section outlines key similarities and differences identified between the analysed cybersecurity skill frameworks. These can be summarised as follows:

- A good number of the analysed countries categorise the cyber skill frameworks into specific groups and roles. Roles can be grouped into seven common categories across all countries based on tasks and responsibilities as shown in Tables 2 and 3.
- A good number of the analysed frameworks emphasize the identification of core elements such as competencies, capabilities, knowledge, skills, proficiency levels, and abilities required for each cybersecurity role.
- The NICE framework does not specify proficiency levels for skills (such as basic, intermediate, or advanced), unlike Australia, the UK, and Singapore, which have defined six proficiency levels. Instead, NICE focuses on competencies to assess a learner's overall

capability in a specific cybersecurity domain. Singapore, on the other hand, defines two proficiency levels: one for technical skills and competencies ranging from level 1 to 6, and another for critical core skills categorized as basic, intermediate, and advanced. Although Canada bases its framework on NICE, it uses a distinct set of common competencies and assesses them using basic, intermediate, and advanced levels.

- The Ghana frameworks place a significant emphasis on critical infrastructure protection, which contrasts with the broader, industry-neutral approaches of other countries, like USA, EU, Canada, and Australia.
- Only the UK and Canada have defined a specific cybersecurity generalist role, which is important since small and medium-sized organizations (SMOs) might have more generalist roles than specialized cybersecurity roles.
- Australia's ASD framework, which is based on the UK's framework, includes five of the UK framework's core capabilities within ASD's nine capabilities, but the role groupings between the two frameworks differ significantly (4 groups in ASD vs 16 specialism in UK).
- Both the UK and ASD frameworks have similar proficiency levels defined for skills. However, ASD specifies learning and development pathways, along with related certifications for each proficiency level. In contrast, the UK framework outlines a certification structure based on each of the 16 specialisms and knowledge areas, with levels categorized as foundation, intermediate, and expert.

6. Moving Forward - Recommendations

Based on the analysis of various cybersecurity skill frameworks, several recommendations can be made for the development of a global cybersecurity skills framework. First, core elements such as competencies, capabilities, knowledge, skills, proficiency levels, and abilities should be regularly updated to address emerging technologies like AI, large language models (LLMs), and quantum computing. Notably, AI safety is currently recognised only as a competency within the USA NICE framework. It is essential to identify variations in these core elements across countries to introduce standardised global elements. Countries such as Ghana and India could benefit from adopting tiered skill levels, as seen in the NICE and Japan's ITSS frameworks, to provide clearer career progression and enhance training programs. Canada's approach of tailoring roles to meet the needs of different organisations, including small and medium-sized organisations (SMOs), by defining both core and adjacent roles, should be considered by other countries with a significant

proportion of SMOs. Additionally, global collaboration is needed to encourage countries to share best practices and certifications in cybersecurity education, thereby fostering the development of a globally skilled cyber workforce.

7. References

Australian Signal Directorate. “Cyber Skills Framework.” *Australian Signals Directorate*, https://www.asd.gov.au/careers/how-apply/cyber-skills-framework. Accessed 10 September 2024.

Canadian Centre for Cyber Security. “The Canadian cyber security skills framework.” *Canadian Centre for Cyber Security*, 31 August 2023, https://www.cyber.gc.ca/en/education-community/academic-outreach-cyber-skills-development/canadian-cyber-security-skills-framework. Accessed 1 October 2024.

CIISec. “Skills Framework.” *CIISec*, https://www.ciisec.org/frameworks/skills-framework/. Accessed 2 October 2024.

Critical Information Instrature. “Critical Information Infrastructure.” *Cyber Security Authority*, https://www.csa.gov.gh/cii. Accessed 4 October 2024.

Cyber Secuirty Authority. “Cyber Secuirty Authority.” *Cyber Security Authority*, https://www.csa.gov.gh/about-us.php. Accessed 4 October 2024.

Cyber Security Agency of Singapore. “Operational Technology Cybersecurity Competency Framework (OTCCF).” *Cyber Security Agency of Singapore*, 8 October 2021, https://www.csa.gov.sg/Tips-Resource/publications/2021/operational-technology-cybersecurity-competency-framework-(otccf). Accessed 1 October 2024.

DSCI Secuirty Framework. “DSCI Security Framework (DSF©).” *Data Security Council of India*, https://www.dsci.in/content/dsci-security-framework-dsf. Accessed 4 October 2024.

European Cybersecurity Skills Framework. “European Cybersecurity Skills Framework Role Profiles — ENISA.” *ENISA*, 19 September 2022, https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-role-profiles. Accessed 4 October 2024.

IT Secuirty Standard. “ITSS framework.” *Common Career/Skill Framework | Nurturing talents and professionals for the digital age | IPA Information-technology Promotion Agency, Japan*, https://www.ipa.go.jp/en/it-talents/skill-standard/skill-framework.html. Accessed 4 October 2024.

The National Institute of Standards and Technology. “NICE Framework: Current Versions | NIST.” *National Institute of Standards and Technology*, 8 November 2019, https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center/nice-framework-current-versions. Accessed 1 September 2024.

Strategic Cybersecurity Talent framework. “Strategic Cybersecurity Talent Framework.” *Www3.weforum.org.*, https://www3.weforum.org/docs/WEF_Strategic_Cybersecurity_Talent_Framework_2024.pdf. Accessed 3 October 2024.

TECHNATION Canada. “Cybersecurity National Occupational Standards - TECHNATION.” *TECHNATION Canada*, https://technationcanada.ca/en/resource/cybersecurity-national-occupational-standards/. Accessed 2 September 2024.

UK Cybersecurity council. “Cyber security careers: a route map through the 16 cyber security specialisms.” *UK Cyber Security Council*, https://www.ukcybersecuritycouncil.org.uk/careers-and-learning/cyber-career-framework/. Accessed 2 October 2024.

UK Cyber Security Council. “International Standards for the Cyber Security Profession.” *International Comparisons Policy Paper*, June 2023.

University of Bristol, Bristol cyber security group. “CyBOK.” *CyBOK – The Cyber Security Body of Knowledge*, https://www.cybok.org/. Accessed 2 October 2024.