Contents lists available at ScienceDirect

Computers & Security

journal homepage: www.elsevier.com/locate/cose

TC 11 Briefing Papers

The role of national cybersecurity strategies on the improvement of cybersecurity education

Saleh AlDaajeh[a], Heba Saleous[a], Saed Alrabaee[a,*], Ezedin Barka[a], Frank Breitinger[b], Kim-Kwang Raymond Choo[c]

[a] Information Systems & Security, United Arab Emirates University, 15551 Al Ain, United Arab Emirates
[b] School of Criminal Sciences, University of Lausanne, 1015 Lausanne, Switzerland
[c] Department of Information Systems and Cyber Security, University of Texas at San Antonio, San Antonio, TX 78249-0631, USA

ARTICLE INFO

Article history:
Received 26 April 2021
Revised 5 April 2022
Accepted 10 May 2022
Available online 18 May 2022

Keywords:
Cybersecurity strategic plan
Cybersecurity education
NICE framework
Cybersecurity curricula
GQO+Strategies paradigm

ABSTRACT

Digital information and telecommunication technologies have not only become essential to individuals' daily lives but also to a nation's sustained economic growth, societal well-being, critical infrastructure resilience, and national security. Consequently, the protection of a nation's cyber sovereignty from malicious acts is a major concern. This signifies the importance of cybersecurity education in facilitating the creation of a resilient cybersecurity ecosystem and in supporting cyber sovereignty. This study reviews a sample from world-leading countries National Cybersecurity Strategic Plans (NCSPs) and analyzes the associated existing cybersecurity education and training improvement initiatives. Furthermore, a proposal to adopt the Goal-Question-Outcomes(GQO)+Strategies paradigm into cybersecurity education and training programs curricula improvement to national cybersecurity strategic goals is presented. The proposal maps cybersecurity strategic goals to cybersecurity skills and competencies using the National Initiative for Cybersecurity Education (NICE) framework. The newly proposed cybersecurity education and training programs' curricula learning outcomes were generated from the GQO+Strategies paradigm based on the three major cybersecurity strategic goals: Development of secure digital and information technology infrastructure and services, defending from sophisticated cyber threats, and enrichment of individuals' cybersecurity maturity and awareness. It is highly recommended that cybersecurity university program administrators utilize the proposed GQO+Strategies to align their program's curriculum to NCSP. Hence, closing the gap that exists with the relevant skills and sustain national cybersecurity workforces.

1. Introduction

Information and telecommunication technology (ICT) in its various forms pervades our modern society and is integral to the nations' sustained economic growth, societal well-being, national security, and global competitiveness. Its importance is clearly evidenced during the COVID-19 pandemic, where people rely on ICT to work, live, and socialize. Hence, it is not surprising that there have been significant interest and investments in various ICT research efforts, such as cybersecurity. On the other hand, the frequency of cybersecurity attacks is expected to continue rising as new and more sophisticated attacks are coming to light Herjavec (2019). The increased number of cyber attacks during the COVID-19 pandemic has also highlighted an urgent need for more cybersecurity professionals and effective cybersecurity awareness programs and initiatives (Hakak et al., 2020; Pranggono and Arabo, 2020). Nearly a decade ago, a study conducted by Evans and Reeder (2010) reported an existing shortage not only of highly skilled professionals needed to manage the operation of deployed systems, but, more pressingly, individuals who can design secure systems, write secure code, and create the necessary tools to deter, detect, mitigate, and recover from any damage caused by malicious cyber acts. Studies conducted by Cobb (2016) and Hranický et al. (2021) indicated that ICT professional agencies and recruiters agree that technical cybersecurity skills, such as intrusion detection, secure software development, and attack mitigation, are of urgent demand. The study conducted by the *California Community Colleges Center of Excellence for Labor Market Research* highlighted that challenges exist when one attempts to close the gap between the supply shortage in cybersecurity professionals and the

[*] Corresponding author.
E-mail address: salrabaee@uaeu.ac.ae (S. Alrabaee).

https://doi.org/10.1016/j.cose.2022.102754

labor-market demands for certain cybersecurity professional skills (Crumpler and Lewis, 2019).

Cybersecurity resilience is a key concern for global leaders and individuals, particularly as individuals are becoming more privacy-aware. Hence, we predicate that cybersecurity education is an intrinsic step towards creating a resilient cyber secure society and organizations. There are, however, limitations in many existing cybersecurity strategies and education approaches. The study done by Evans and Reeder (2010) mentioned that having competent employees at every level to identify, build, and staff the cybersecurity infrastructure defences and responses is critical to any robust cybersecurity strategy. Cobb (2016) addressed a number of increasingly urgent arguments about defending information systems against cyber attackers. One of the mentioned questions is whether the world can supply enough cybersecurity professionals to defend our information technology infrastructures and defeat cyber attackers. Crumpler and Lewis (2019) highlighted the gap that exists in the United States of America's (USA) current cybersecurity education and training landscape and elaborates on several examples of successful programs for addressing the existing gap. Additionally, their study offered several recommendations for improving cybersecurity education from policymakers, educators, and employers perspectives. A holistic framework for analyzing the skill gap in cybersecurity professionals was proposed by (Kreider and Almalag, 2019), which identified three dimensions to analyze the existing gap in cybersecurity educational programs in higher education: Student pipelines, program offering, and program capacity. The *Global Information Security Workforce Study* indicated in their report that there are not enough cybersecurity professionals in organizations to combat cyber crimes (Booz, 2017). Furthermore, their latest report published in 2017 reveals that cybersecurity workforce gap would reach of 1.8 million by 2022, a 20% increase over the forecast made in the 2015.

The underlying objective of this study is to improve cybersecurity education curricula by providing a systematic approach to synthesis and align cybersecurity skills, competencies, and knowledge needed to fulfill National Cybersecurity Strategic Plan requirements (NCSP). This study reviews a sample of world-leading countries NCSP from different regions, elaborates on cybersecurity curricula improvement initiatives and best-practices, and investigates the best approaches to create attractive cybersecurity education and training programs for individuals to consider for their future careers. Furthermore, this study examines the different approaches to align cybersecurity education and training programs' curricula improvements to high-level strategic goals. The Goal-Question-Outcomes (GQO)+Strategies paradigm is utilized to synthesize the cybersecurity competencies required to fulfill the NCSP requirement in terms of supplying professional cybersecurity specialists. The National Initiative for Cybersecurity Education (NICE) framework was used as a lexicon to determine the required cybersecurity workforce competencies and to define cybersecurity education and training programs' learning outcomes accordingly.

The article is organized as follows: Guidelines for the development of NCSP and a sample of NCSP from world-leading countries from different regions are reviewed in Section 2. Various efforts, standards, and frameworks used as guidelines and/or lexicon for cybersecurity knowledge-areas, competencies, and skills are discussed in Section 3. Section 4 reviews different initiatives taken towards improving cybersecurity programs' curricula and allurement. Strategy mapping models approaches are reviewed and discussed in Section 5. The newly proposed updated model GQO+Strategies and its application to improve cybersecurity program curriculum of the United Arab Emirates University (UAEU) Master Program in Information Security is discussed in Section 6. Finally, the article is discussed and concluded in sections 7 and 8 respectively. Table 1 lists the notations used in this article.

Table 1
Summary of notations.

Abbrev.	Description
ABET	Accreditation Board for Engineering and Technology
ACM	Association for Computing Machinery
ASEAN	Association of Southeast Asian Nations
BCS	British Computer Society
CAA	Commission of Academic Accreditation (UAE)
CAC	Cyberspace Administration of China
CII	Critical Information Infrastructure
ComSec	Commonwealth Secretariat
CPTC	Collegiate Penetration Testing Competition
CSCP	Cyber Security Cooperation Program (Canada)
CSE	Communications Security Establishment
CSIS	Center for Strategic and International Studies
CSIS	Canadian Security Intelligence Service
CSTA	Computer Science Teachers Association
CTO	Commonwealth Telecommunications Organization
DoHA	Department of Home Affairs
DHS	Department of Homeland Security
DSP	Digital Service Providers
ENISA	European Union Agency for Cybersecurity
ESDC	Employment and Social Development Canada
EU	European Union
GAC	Global Affairs Canada
GCSCC	Global CyberSecurity Capacity Centre
GCSP	Geneva Center for Security Policy
GQP	Goal Question Purpose
ICT	Information & Communication Technology
IoT	Internet of Things
ISTE	International Society for Technology in Education
ITU	International Telecommunication Union
KPI	Key Performance Indicator
MOE	Ministry of Education (UAE)
NCAF	National Capabilities Assessment Framework
NCSC	National Cyber Security Certification
NCSP	National Cybersecurity Strategic Plan
NCSS	EU National CyberSecurity Strategy
NICE	National Initiative for Cybersecurity Education
NISA	National Institution of Standards and Technology
NRCan	Natural Resources Canada
NSA	National Security Agency
OES	Operators of Essential Services
PEU	Pink Elephant Unicorn (Cybersecurity Competition)
PLOs	Program Learning Outcomes
PS	Public Safety (Canada)
RCMP	Royal Canadian Mounted Police
SCC	Standards Council of Canada
SMEs	Small and Midsize Enterprises
TRA	Telecommunication Regulatory Authority
UAEU	United Arab Emirates University
UNCTAD	United Nations Conference on Trade and Development

2. Review of international cybersecurity strategic plans

Digital and information technology cybersecurity challenges have cultivated an urgent need for a more structured discipline in curricula, academic programs, and awareness initiatives. Although some success has been witnessed in expanding the workforce of cybersecurity practitioners and professionals, the supply and demand gap is estimated to reach between 1.8-3.5 million professionals worldwide by the year 2022 (Booz, 2017; NeSmith, 2018). In addition to filling this gap by educating more individuals, cybersecurity specialists are also encouraged to further expand their skillset to flourish and progress in their careers (Crumpler and Lewis, 2019; Kreider and Almalag, 2019).

Section 2.1 describes the guidelines for the development of the NCSP presented by the International Telecommunication Union. Subsequent sections review the ten world-leading NCSPs. A summary of the reviewed plans with focus on cybersecurity education and training is provided in the last section.

Table 2
Cybersecurity national strategic plan development phases .

Phase	Objective	Outcome	Tasks/ Activities
Initiation Phase	Defining processes, timelines, and identifying key stakeholders involved in the production of the cybersecurity strategic plan.	Elaboration on the development plan of the strategy	• Identifying the Lead Project Authority. • Establishing a Steering Committee. • Identifying stakeholders. • Planning the development of the Strategy.
Stocktaking and Analysis Phase	Collecting the necessary data and information to evaluate the national perspective on cybersecurity and the current and future cyber risk.	Report on the assessment and evaluation of the strategic national cybersecurity posture and risk landscapes.	• Evaluating national perspective on cybersecurity. • Evaluating the cyber risk landscape.
Production of National Cybersecurity Strategy Phase	Define the strategic vision, context, and high-level objectives, evaluation of the current situation and future direction, prioritization of strategic objectives based on their influence and impact.	Develop strategy narrative by involving key stakeholders through series of working groups and public consultation.	• Compiling the National Cybersecurity Strategy. • Maximize involvement of a wide range key-stakeholders. • Obtain formal approval and consent. • Publication of the National Cybersecurity Strategy.
Implementation Phase	Develop action plans and confirm adequate human and financial resources required to implement various action plans envisioned in NCSP	Action plans and resource distributions.	• Constitution of action plans. • Highlighting strategic initiatives that are to be implemented. • Allocating required resources (human and financial) for the implementation phase. • Defining timeframes and progress assessment metrics.
Monitoring and Evaluation Phase	Monitoring: Government seeks to assure that the strategy is implemented in accordance to preset action plans. Evaluation: Government assesses the validity of the NCSP in view of evolving and new risks, the environment, and determine if the plan still reflects their vision.	Adjustment recommendations (Strategic Plan, Action Plans, and Initiatives and Programs). Audits and Progress reports. Other related KPIs.	• Implementing a formal monitoring process. • Continuous observation for strategy implementation progress. • Strategy outcomes assessment and evaluation.

2.1. International telecommunication union-cybersecurity strategic plan development guidelines

Twelve partners[1] from diverse governmental sectors, international organizations, private sector key-stakeholders, academia, and the civil society collaborated in order to design a guide to assist nations in developing their national cybersecurity strategy (Sapolu et al., 2018). This NCSP development guide adopts an iterative five stage process (elaborated in Table 2) towards comprehending and addressing the following seven pillars (focus areas):

1. Governance: The NCSP is required to outline a set of roles and responsibilities, authorities, resources, and processes to guide the development and implementation of the cybersecurity national strategic plan.
2. Risk Management in National Cybersecurity: This practice focuses on identifying a risk-management approach and categorise sectoral risk profiles.
3. Preparedness and Resilience: This is the NCSP for incident responses and to achieve resilient operational environment and infrastructure.
4. Critical Infrastructure Services and Essential Services: The ultimate goal of all NCSP is to implement effective plans to protect national critical infrastructure services and essential services. Hence, this pillar focuses on identifying critical infrastructure services and essential services and plan for their protection accordingly.
5. Capability and Capacity Building and Awareness Raising: As an integral part for developing professional cybersecurity national manpower, the NCSP shall plan to fulfill their demand towards achieving resilience and protecting their critical infrastructure services and essential services. Hence, this pillar is considered crucial and requires rigorous planning and collaboration with national and international academic and professional associations.
6. Legislation and Regulations: Prohibiting cybercrime starts by establishing well-defined legislations and safeguarding individual rights and liberties. This pillar must be addressed in the NCSP in order to ensure compliance and consolidate international cooperation towards combating cybercrime.
7. International Cooperation: The NCSP is required to contribute to the international effort towards combating cybercrimes and aligning domestic or national cybersecurity strategies with international foreign policies and efforts towards space cyberspace.

Successful NCSP design and development need to address the aforementioned listed pillars and associated elements enclosed for each focus area. Table 3 elaborates on elements associated with the NCSP design and development focus areas (Sapolu et al., 2018). In this study, we concentrate on *Capability and Capability Building and Awareness Raising*. Specifically, this study is only concerned with addressing how to improve cybersecurity education from a national cybersecurity strategy perspective.

The below reviewed NCSPs are samples of available and accessible NCSPs. Nevertheless, there are many others that are reputable and worth reviewing. The current study will be implementing the United Arab Emirates NCSP in its analysis.

2.2. NCSP 1 – United States

The United States of America's (US) national cyber strategy priorities are focused on empowering the country's cybersecurity capabilities and securing the nation from cyber threats (Sabillon, 1993; The White house, Washington DC, 2018). The US cyber strategy is based on the following strategic priorities:

- Defend the US cyberspace by protecting critical assets. This constitutes to elements such as: networks, systems, functions, and data.

[1] Commonwealth Secretariat (ComSec), the Commonwealth Telecommunications Organization (CTO), Deloitte, the Geneva Centre for Security Policy (GCSP), the Global CyberSecurity Capacity Centre (GCSCC) at the University of Oxford, the International Telecommunication Union (ITU), Microsoft, the NATO Cooperative Cyber Defense Centre Of Excellence (NATO CCD COE), the Potomac Institute for Policy Studies, RAND Europe, The World Bank and the United Nations Conference on Trade and Development (UNCTAD).

Table 3
Cybersecurity national strategic plan pillars and focus areas enclosed Elements.

Focus Area	Elements
Governance	• Ensure the highest level of support • Establish a competent cybersecurity authority. • Ensure intra-government cooperation • Ensure inter-sectoral cooperation • Allocate dedicated budget and resources • Develop an implementation plan
Risk Management in National Cybersecurity	• Define a risk-management approach • Design a prevailing methodology or framework for cybersecurity risk management • Develop sectoral cybersecurity risk profiles. • Establishing cybersecurity policies Preparedness and Resilience • Establish cyber incident response capabilities • Establish contingency plans for cybersecurity crisis management. • Promote information-sharing • Conduct cybersecurity exercises
Critical Infrastructure Services and Essential Services	• Protecting critical infrastructures and services by adopting a prevailing risk-management approach. • Adopt a governance model with clear responsibilities. • Define minimum cybersecurity baselines • Utilise a wide range of market levers. • Establish public-private partnerships.
Capability and Capacity Building and Awareness Raising	• Develop cybersecurity curricula • Stimulate skills development and workforce training. • Implement a coordinated cybersecurity awareness-raising program. • Nurture cybersecurity innovation, research, and development.
Legislation and Regulation	• Establish cybercrime legislation • Recognise and safeguard individual rights and liberties. • Create compliance mechanisms • Promote capacity-building for law enforcement. • Establish inter-organisational processes. • Support international cooperation to combat cybercrime.
International Cooperation	• Prioritize cybersecurity as an integral part of foreign policy. • Engage in international discussions • Promote formal and informal cooperation in cyberspace. • Align domestic and international cybersecurity efforts.

- Elevate the prosperity of the US by fostering a secure, burgeoning digital economy and prosper strong indigenous innovation.
- Maintain peace and security by bolstering the ability of the US – in collaboration with allies and partners – to deter and penalize those who use cyber tools for malicious acts.
- Extend US influence abroad to reach the key tenets of an open, interoperable, reliable, and secure internet and cyber space.

The Department of Homeland Security (DHS) and National Security Agency (NSA) have a joint project with the objective to set a criteria to regulate institutions who intend to offer cybersecurity and defense education (National Security Agency and Department of Homeland Security, 2020). Their main objective is to create standards for cybersecurity education in the US and to determine the appropriate curriculum to offer students. This joint project concluded that cybersecurity programs should include hands-on exercises as part of their skill development. Furthermore, institutions hosting cybersecurity or related disciplines should establish a center for cybersecurity education to offer guidance and promote collaboration among academia. The *National Institution of Standards and Technology* (NIST) has also established their own initiatives to address various challenges faced in the realm of cybersecurity education. These initiatives have successfully delivered the *National Initiative for Cybersecurity Education* (NICE) program since 2010. The underlying objective of the NICE is to provide a reference-model for educators to create training, degree, and certification programs, as well as developing the appropriate curriculum (Daimi and Francia III, 2020; Dawson et al., 2019; Haney and Lutters, 2021; Newhouse et al., 2017). This initiative goes hand-in-hand with the guidelines established by the DHS and NSA.

2.3. NCSP 2 - United Kingdom

The United Kingdom's (UK) NCSP for the years 2022–2025 is designed to support the achievement of their national goals. It focuses on the accomplishment of the UK Cabinet office's long-term 2030 vision to continue leading responsible and democratic cyber power capable of protecting and promoting the UK's interests within cyberspace (HM-Government - The Rt Hon Steve Barclay MP Chancellor of the Duchy of Lancaster and Minister for the Cabinet Office, 2022). The UK's national cyber goals are as follows:

- Using their cyber capabilities to be more secure and resilient by preparing for evolving threats and risks, and therefore protecting citizens against crime, fraud and state threats.
- Prosperous and innovative digital economy that shall evenly spread across the nation and its diverse population.
- Employing science and advanced technologies to securely control transformative technologies in support of a more sustainable and healthier society.
- Taking a more influential role and valuing global partners while defining the future frontiers for an open and steady international order and preserving their freedom of action in cyberspace.

The UK's 2022–2025 NCSP builds on the achievements of the predecessor NCSP (2016–2021) (UK (H.M) Government, 2016) and is designed based on the conclusions derived from the government's integrated review of security, defence, and development and foreign policy. The conclusions drawn from the integrated review are focused on strengthening the UK's cyber power as follows:

- The UK's cyber power will become more important force towards the achievement of UK national goals.
- Its sustainability requires a comprehensive and integrated strategy to cover various aspects.
- The nation's cyber power must be a society-oriented, hence deeming partnerships essential to successfully achieve this conclusion.

The UK's 2022–2025 NCSP is roughly categorized into two main parts: Strategic context, and Implementation. The strategic context demonstrates the rationale for focusing on the 5 strategic pillars. The implementation part presents an organized break-down of the 5 strategic pillars to 16 objectives. The UK has allocated approximately 22 billion £to the achievement of this NCSP including the following pillars and objectives:

- **Pillar 1: Strengthening the UK's cyber ecosystem.**
  - Objective 1: Support the whole-society approach by strengthening the necessary structures, partnerships and networks.
  - Objective 2: Empowering national future talent with cyber skills at every level through world class and diverse cyber professions and competencies.
  - Objective 3: Foster the growth of internationally competitive cyber- and information security sector by delivering quality products and services.
- **Pillar2: Building a resilient and prosperous digital UK.**

  - Objective 1: Enhance the understanding of cyber risks in order to derive the appropriate actions on cybersecurity and resilience.
  - Objective 2: Improving cyber risk management within UK organizations and providing greater protection to citizens to prevent and resist cyberattacks effectively.
  - Objective 3: To prepare for, respond to, and recover from cyberattacks by strengthening resilience at both the national and organizational levels.
- **Pillar 3: Taking the lead in the technologies vital to cyber power.**
  - Objective 1: Improve foresight and act on the investments in vital science technology development for cyber power.
  - Objective 2: Nurture and sustain sovereign and allied advantages in the security of critical technologies.
  - Objective 3: Preserve a robust and resilient national Crypto-Key enterprise which meets the needs of the government and their partners and allies.
  - Objective 4: Securing the next generation of connected technologies and infrastructure, and ensuring that the UK achieves low-dependence on the global market and that the nation's users are provided with trustworthy and diverse supplies.
  - Objective 5: Collaboration with multiple stakeholders for the development of global digital standards, ensuring cybersecurity is integrated, and advancing in strategic advantage that is science- and technology-based.
- **Pillar 4: Advancing the UK's global leadership and influence.**
  - Objective 1: Ensure cybersecurity and resilience of the UK's international partners and increase collective action to disrupt and deter cyber attacks.
  - Objective 2: Global governance to encourage a free, open, peaceful, and secure cyberspace.
  - Objective 3: Enhance the UK's strategic advantage and promote its broader foreign policy and interest through leveraging and exporting cyber capabilities.
- **Pillar 5: Advancing the UK's global leadership and influence.**
  - Objective 1: Protect the UK, its interests, and its citizens by detecting and sharing investigation information on criminals and other malicious entities and activities.
  - Objective 2: Deterring and disrupting criminal parties and activities.
  - Objective 3: Preventing and detecting serious crimes by taking appropriate actions that support national security throughout cyberspace.

2.4. NCSP 3 - European Union

The European Union Agency for Cybersecurity (ENISA) was established in 2004 with the objective of achieving a common high-level cybersecurity across Europe and its member states (ENISA, 2020). Strengthened by the EU Cybersecurity Act, the ENISA is tasked with contributing to the definition and setup of EU cyber policies, the enhancement of the trustworthiness of information and communication technology products and deliverables, cybersecurity certification assurance, and schemes for services and processes. Additionally, they are tasked with fostering cooperation with Member States and EU bodies and bolstering Europe to overcome and prepare for future cyber challenges. ENISA's scope is focused on knowledge sharing and transfer, building cybersecurity key-enablers and enriching mature awareness, collaborating with and involving key stakeholders to strengthen trust in the connected economy. Ultimately, this is done in order to advance the resilience of the EU's critical infrastructures, and, ultimately, to preserve Europe's society and ensure that citizens are digitally secure (ENISA, 2020).

ENISA has developed a cybersecurity strategy with the aim of improving security and resilience of the EU's national infrastructure and services. This is done by adopting a high-level top-down approach to establish action plans with a specific time frame for the implementation of a range of national objectives and strategic priorities (ENISA, 2020). Furthermore, ENISA developed the National Capabilities Assessment Framework (NCAF) to provide member states with a self-assessment tool to evaluate their maturity and progress towards the achievement of NCSS objectives and to build cybersecurity capabilities at both the strategic and operational levels (ENISA, 2020). The NCAF elaborates on four main clusters, namely: Cybersecurity Governance and Standards, Capability-building and awareness, Legal and regulatory, Cooperation. Each one of these clusters is defined with a set of objectives in which the national cybersecurity strategy implementation maturity is being assessed.

Fig. 1 depicts NCAF clusters and related objectives.

2.5. NCSP 4 - Canada

The National Cybersecurity Action Plan (2019–2024) is the blueprint of Canada's national cybersecurity strategy (Ministry of Public Safety and Emergency Preparedness of Canada, 2019). In this plan, strategic initiatives and projects are explained, the implementation time frame is defined, and responsible departments and agencies are allocated. Specifically, this plan focuses on the achievement of three main cybersecurity strategic goals:

Secure and Resilient Systems The achievement of this goal is done by implementing seven strategic initiatives: Supporting Canadian Critical Infrastructure Owners and Operators, Improved Integrated Threat Assessment, Preparing Government of Canada Communications for Advances in Quantum, Expanding Advise and Guidance to the Finance and Energy Sectors, Cyber Intelligence Collection and Cyber Threat Assessments, National Cybercrime Coordination Unit, and Federal Policing Cybercrime Enforcement. These seven initiatives are focused on protecting against cybercrimes and attacks, as well as responding to and defending from sophisticated threats targeting critical government and private sectors' digital assets. Multiple Canadian governmental agencies and organizations, such as Public Safety Canada (PS), Canadian Security Intelligence Services (CSIS), Communications Security Establishment, and Royal Canadian Mounted Police (RCMP), are assigned to implement these initiatives.

Create an Innovative and Adaptive Cyber Ecosystem: This strategic goal aspires Canada to become a global leader in cybersecurity. Specifically, this goal can be achieved by Canada's National Cybersecurity Action Plan for 2019–2024, which includes two main initiatives:

- The Cybersecurity Student Work Placement Program, which is facilitated by the Employment and Social Development Canada (ESDC).
- The cybersecurity assessment and certification for small-and-Medium-sized Enterprises (SMEs), which is organized by Innovation, Science, and Economic Development Canada (ISEDC) in collaboration with the Communications Security Establishment (CSE) and Standards Council of Canada (SCC).

These two initiatives are focused on aiding advanced research, nurturing digital innovation, and developing cyber skills, knowledge, and awareness.

Effective Leadership, Governance and Collaboration: This goal focuses on establishing collaboration among Canada's provinces, territories, the private sector, governmental agencies, and international allies to work towards shaping the international cybersecurity environment to consolidate Canada's interests. This strategic

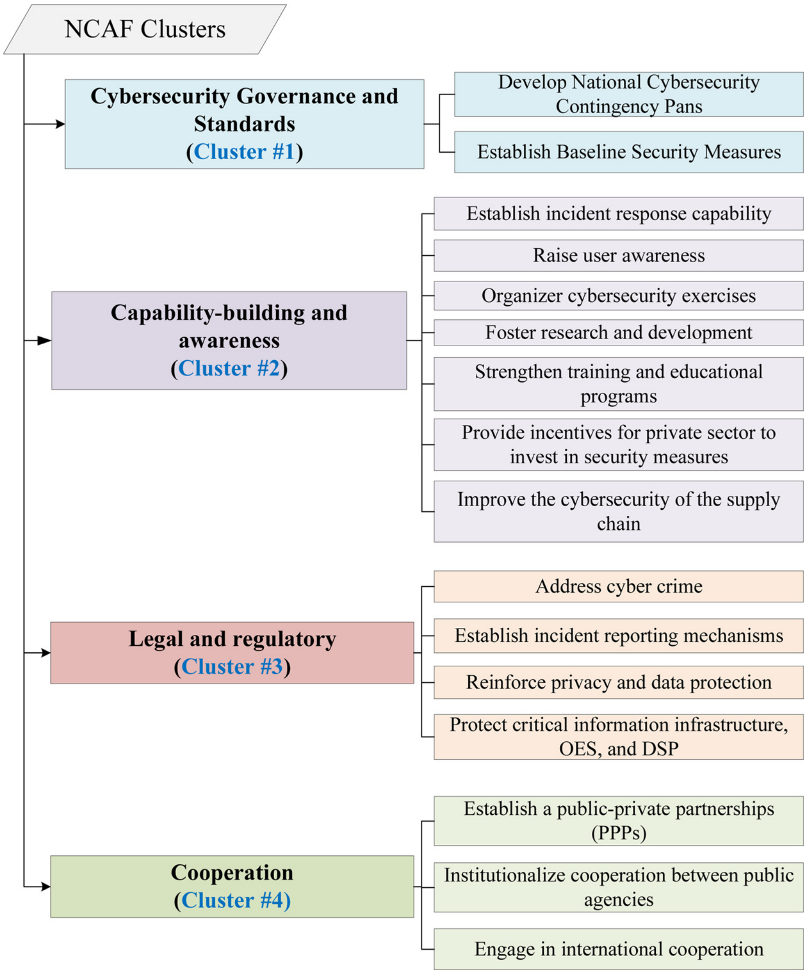
NCAF Clusters
Cybersecurity Governance and Standards (Cluster #1)
Develop National Cybersecurity Contingency Pans
Establish Baseline Security Measures
Capability-building and awareness (Cluster #2)
Establish incident response capability
Raise user awareness
Organizer cybersecurity exercises
Foster research and development
Strengthen training and educational programs
Provide incentives for private sector to invest in security measures
Improve the cybersecurity of the supply chain
Legal and regulatory (Cluster #3)
Address cyber crime
Establish incident reporting mechanisms
Reinforce privacy and data protection
Protect critical information infrastructure, OES, and DSP
Cooperation (Cluster #4)
Establish a public-private partnerships (PPPs)
Institutionalize cooperation between public agencies
Engage in international cooperation

Fig. 1. ENISA: NCAF clusters and their corresponding cybersecurity objectives. OES: Operators of essential services. DSP: Digital services providers (ENISA, 2020).

goal is can be achieved through five initiatives: Strategic Policy Capacity in Cybersecurity and Cybercrime, Cyber Security Cooperation Program (CSCP), Canadian Centre for Cyber Security, International Strategic Framework for Cyberspace, and Bilateral Collaboration on Cybersecurity and Energy. The organization and facilitation for implementing these strategic initiatives is assigned to various Canadian government entities, such as Public Safety Canada (PS), Communications Security Establishment (CSE), Global Affairs Canada (GAC), and the Natural Resources Canada (NRCan).

2.6. NCSP 5 - Russian Federation

The Russian Federation has set a long-term strategy to cover the years 2017 to 2030. Their strategy outlines strategic goals, objectives, and measures for the implementation of domestic and foreign information and telecommunication related policies (United Nations Institute for Disarmament Research, 2017). The Russian Federation's strategy for the development of information society focuses on six national interests: human development, preserving citizens and state security, promoting Russia's role and contribution in the global humanitarian and cultural space, development of a free sustainable and secure communication, efficient public administration, economic and social development, and the formation of digital economy. The Russian cybersecurity strategy evolves from their understanding of the nature of information warfare. Hence, the Russian Federation has a strong need for cybersecurity as a pillar for their national security (Lilly and Cheravitch, 2020).

2.7. NCSP 6 - China

China has the intention of becoming a cyber power while also promoting a regulated, secure, and open cyberspace. Additionally, the country intends on safeguarding national cyber sovereignty. China has set their national cybersecurity strategy to address cybersecurity as *the nation's new territory for sovereignty* marking a new step in streamlining cyber control. The Cyberspace Administration of China (CAC) set the strategy with the focus on: defending cyberspace sovereignty, protecting national security and Critical Information Infrastructure (CII), building a healthy online culture to combat cyber crime, espionage, and terrorism, improving cyber governance, enhancing baseline cybersecurity, elevating cyberspace defense capabilities, and strengthening international cooperation (Daricili and Özdal, 2018). In addition, China plans to prepare and graduate more cybersecurity professionals by opening ten cybersecurity-specialized educational institutions between 2017–2027.

2.8. NCSP 7 - Australia

The Australian government has taken vigorous action towards national cybersecurity. In their recent cybersecurity strategy for 2020, they allocated $1.67 billion over the coming decade to invest in a secure online world for Australians, their businesses, and their critical infrastructures and essential services (Government of Australia, Department of Home Affairs, 2020). According to the Australian Government's Department of Home Affairs (DoHA), the development of a cybersecurity strategy effort is based on extensive consultation from across the country. Additionally, the DoHA has formed an Industry Advisory Panel to provide their strategic insights and guidance on the development of the 2020 strategy and ensure consistency with industries. The Australian Cybersecurity Strategy 2020 has undertaken three classifications:

- Governments are responsible to protect Australian residents, businesses, and critical infrastructures from sophisticated cyber threats by bolstering defense and countermeasures of their cyber space.
- Businesses are required to protect their customers from known cyber vulnerabilities by securing their products and services.
- Communities are prohibited from practicing malicious cyber acts and must protect themselves by practicing secure online behaviours and making informed decisions.

The Australian Cybersecurity Strategy 2020 focuses on growing the cyber workforce. In their strategy, they emphasized the importance of having of Australia's digital economy and security. Realizing its importance, Australia established a Cybersecurity National Workforce Growth Program to assist businesses and academia.

2.9. NCSP 8 - Association of southeast asian nations

The Association of Southeast Asian Nations (ASEAN) collaborated with the European Union to establish a comprehensive cybersecurity framework (De Inovação, 2018). Within this framework, two important plans that are mentioned are the Master Plan and the ASEAN Declaration to Prevent and Combat Cybercrime. The key objectives of the Master Plan (2016–2020) focus on enabling the transformation of the digital economy and the development of human capacity for an attractive and secure digital investment environment. As part of the strategic thrust of the Master Plan, two initiatives were undertaken to strengthen information security and preparedness in ASEAN. The ASEAN Declaration to Prevent and Combat Cybercrime focuses on developing awareness and effective work on cybersecurity related topics and disciplines (De Inovação, 2018).

2.10. NCSP 9 - United Arab Emirates

The United Arab Emirates (UAE) has successfully developed and deployed an advanced digital and information technology solution for their critical infrastructure (Ghafir et al., 2018). The government realized the importance of planning and working towards strengthening their defense and resilience countermeasures to combat sophisticated cybersecurity threats and attacks (Ghafir et al., 2018). This includes enriching the skillsets and awareness of individuals and organizations. The UAE Cybersecurity strategic plan was developed by the Telecommunication Regulatory Authority UAE - Telecommunication Regulatory Authority (2019). It consists of five pillars and 60 initiatives. The underlying objective of the UAE's NCSP is to create a safe and strong cybersecurity ecosystem in order to enable citizens to fulfill their aspirations and empower businesses. This NCSP has specific initiatives aimed at consolidating advanced innovation, research, and development undertaken by academic institutions and motivating students to pursue cybersecurity as their future career.

2.11. NCSP 10 - Switzerland

In 2018, Switzerland's Federal IT Steering Unit (FITSU) Federal IT Steering Unit (FITSU) (2018) released a four year plan on protecting their country against cyber risks, which was the continuation of the previous plan that took effect from 2012 to 2017. In order to achieve their objectives, their NCSP "distinguishes among ten spheres of action, which address different aspects of cyber risks": (1) Building competencies and knowledge, (2) threat situation, (3) resilience management, (4) standardisation / regulation, (5) incident management, (6) crisis management, (7) prosecution, (8) cyber defence, (9) active positioning of Switzerland in international cyber security policy, and (10) public impact and awareness raising. Each of these spheres includes specific measures (total of 29 measures). For instance, the measures (1) Building competencies and knowledge are: (i) early identification of trends and technologies and knowledge building, (ii) Expansion and promotion of research and educational competence, and (iii) Creation of a favourable framework for an innovative ICT security economy in Switzerland.

2.12. Summary

Worldwide, cybercrimes and their ramifications have become a predicament. National security and cybersecurity ecosystems are strongly dependent on the supply of qualified and proficient cybersecurity professionals and a cybercrime-educated society. Cybersecurity education is perceived as the primary pipeline supply for cybersecurity professionals. All reviewed NCSPs concede to certain cybersecurity strategic goals or pillars:

- Achieving a strategic vision of becoming cybersecurity resilient, which is a joint effort between government, industry, and community.
- Cybersecurity professionals are urgently required to protect government and private sector systems from malicious acts and sophisticated cyber attacks.
- A country is required to invest in research and developments of cybersecurity countermeasures against emerging sophisticated attacks targeting their critical infrastructures.
- Societies' maturity and awareness of cybersecurity plays a crucial role in combating cybercrime.

Table 4 summarizes the review of selected sample from world-leading countries' NCSPs, outlining the urgent need to invest in the development and implementation of an effective cybersecurity education and awareness initiatives and programs to supply professional cybersecurity specialists.

3. Cybersecurity curricula improvement standards and frameworks

Given its vital contribution to cybersecurity ecosystem, numerous efforts have been made to develop cybersecurity curricula and programs. The following subsections presents a sample of various standards, guidelines, frameworks, and concepts proposed for cybersecurity curricula improvement.

3.1. NIST- NICE Framework

The National Institute of Standards and Technology (NIST) has developed the National Initiative for Cybersecurity Education (NICE) Framework, which was first published in 2017 and revised in Nov. 2020 (Petersen et al., 2020). NICE works as a reference-framework (lexicon) and is designed to ensure the following objectives:

- To provide a cybersecurity work reference taxonomy.
- To empower, advocate, and coordinate a robust ecosystem of cybersecurity education, training, and workforce development.
- To consolidate the development of a robust cybersecurity curricula by describing tasks, knowledge, and skills.
- To assist organizations/sectors with the development of a common and consistent lexicon and categories for cybersecurity

Table 4
Summary of NCSP with focus on cybersecurity education improvements and awareness enrichment.

Country/ Region	Strategic Agenda
United States (NSA & NIST)	• Create standards for cybersecurity education in the United States of America • Determine the appropriate curricula to offer students • Encourage collaboration among academia and industry • Emphasize on hands-on learning in cybersecurity • Launch the National Initiative for Cybersecurity Education (NICE) program in alignment with the guidelines established by the DHS and NSA • Provide a reference-model for educators to create training, degree, and certification programs, as well as developing the appropriate curriculum
United Kingdom (UK - Government - Cabinet Office)	• Strengthening the UK's cyber ecosystem • Building a resilient and prosperous digital UK • Taking the lead in the technologies vital to cyber power • Advancing UK global leadership and influence • Detecting, disrupting and deterring adversaries
European Union (ENISA)	• National Capabilities Assessment Framework (NCAF) to enable member states to assess their maturity towards achieving National Cybersecurity Strategy (NCSS) objectives • Definition of EU cyber policies and enhancement of trustworthiness of information and communication technology products and deliverable, services, and processes • Cybersecurity knowledge sharing and capability building through awareness enrichment • Collaborate and involvement with key stakeholders to assure trust in interconnected economy and strengthen resilience of critical infrastructure • Digitally secure EU societies and citizens.
Canada (ESDC, ISED, CSE, SCC)	• Commence student work-integrated learning program • Complete student work-integrated learning program and conduct evaluations • Launch cyber education and awareness tools • Launch cyber certification programs
Russia (Governmental Authorities)	• Human-Capital Development in Cybersecurity and preserving citizens' and states' security • Profound role and contribution in global humanitarian and cultural space, advancement of developing free sustainable and secure interaction among citizens, organizations, and authorities • Efficient public administration, economic and social development, and digital economy • Nurture cybersecurity innovation, research, and development.
China (CAC)	• Defining cyberspace sovereignty and protecting national security and critical information infrastructure (CII) • Creating a healthy online culture to fight cyber crime through improved cyber governance, enhancing baseline cybersecurity, elevating cyberspace defense capabilities, and strengthening international cooperation • Increase supply of cybersecurity professionals by establishing specialized educational institutions in the period of 2017–2027
Australia (DoHA)	• Protecting and actively defending the critical infrastructure. • Greater collaboration to build Australia's cyber skills and workforce supply • Establishing a Joint Cybersecurity Center program for stronger partnership with industry • Guidance and support for small- and medium-sized businesses and consumers to increase their cyber resilience, and securing Internet of Things devices
Association of Southeast Asian Nations	• Enabling transformation to a digital economy • Building human capacity to create an attractive and secure digital investment environment. • Developing awareness and effective work on developing advanced cybersecurity related disciplines and programs
United Arab Emirates (TRA)	• Development of national cybersecurity strategy. • Launching more than 60 initiatives to support research and development in cybersecurity. • Development of a cybersecurity ecosystem focusing on national cyber safety and cybersecurity resilience
Switzerland (FITSU)	• Focus on building competencies, knowledge, and awareness. • Improve resilience and be prepared for incidents (e.g., incident management, crisis management, and prosecution) • Build expertise on standardisation and active positions in international cybersecurity policy

work skills, knowledge, and competencies in order to develop their workforce capabilities in cybersecurity work.

- To help learners on two levels, both professional and on an awareness-level, in order to explore cybersecurity themes and to enroll in the appropriate learning activities to develop their competency in cybersecurity work.

The NICE framework structure consists of cybersecurity competency building blocks, the structure of which starts by defining a set of cybersecurity work tasks. Each of these work tasks are judiciously mapped and referenced to correlated knowledge and skills (Petersen et al., 2020), which are further classified to assess cybersecurity professional competency levels (i.e. beginner, intermediate, and advanced). Thus, the NICE framework can be utilized to outline cybersecurity education and training program learning outcomes (Trilling, 2018).

3.2. ACM/IEEE

International professional associations such as *Association for Computing Machinery* (ACM) and *IEEE Computer Society* (IEEE-CS) have formed a joint team in an attempt to define the structure of the cybersecurity discipline, support the alignment of academic programs from other related disciplines, and to propose guidelines for cybersecurity curriculum (IEEE Computer Society and ACM, 2017). This collaboration officially began in 2015, and has continued since. The most recent version of their guidelines was published in 2017 (Shoemaker et al., 2017), which ensures that cybersecurity programs include a combination of fundamental topics ranging from computing disciplines, such as computer science and engineering, to interdisciplinary content, such as human factors, law, ethics, and risk management. These guidelines also suggest key-knowledge areas to be included in a cybersecurity program, such as data security, software security, network security, human security, and organizational security (IEEE Computer Society and ACM, 2017).

3.3. British computer society

The BCS has established and defined accreditation standards and guidelines for cybersecurity programs for higher education. These standards focus on identifying key-knowledge areas of cybersecurity programs (Crick et al., 2019; Irons et al., 2016). The UK's BCS (Irons et al., 2016; UK (H.M) Government, 2016) requires academic institutions to amend cybersecurity programs' curricula to include a practicum component and key-knowledge areas.

3.4. Certification

National Cyber Security Center (NCSC) with partners have initiated across UK academia certification degree programs designed to address the knowledge, skills, and capability requirements for cybersecurity education, products, and services (Nautiyal et al., 2022). Such certification programs include the Certified Cyber Professionals (CCP). This certification program recognizes those who demonstrated their sustainability to apply their skills, knowledge, and expertise in cyber real-world situations.

Several studies has discussed the importance of professional cybersecurity certificates towards overcoming the existing gap on demand cybersecurity skills. For instance, (Marquardson and Elnoshokaty, 2020) analyzed large number of job-listing for cybersecurity professionals and determined that 60% of entry-level jobs in cybersecurity requires computer-related degree while 19% of these jobs requires professional certificates demonstrating certain knowledge, skills, and competencies.

3.5. UAE - Ministry of education

The MoE K-12 Computer Science and Technology Standards was published in 2015 (Ministry of Education- UAE, 2015) and elaborates on a set of guidelines for schools, describing cybersecurity key-learning areas in order to prepare students to pursue graduate degrees in cybersecurity. The standard is divided into four main domains: Digital literacy and Competence, Computational Thinking, Computer Practice and Programming, and Cybersecurity/Safety Ethics. The MoE has adopted and included existing international standards, such as the International Society for Technology in Education (ISTE), and Computer Science Teachers Association (CSTA) standards.

3.6. Other frameworks and concepts

Several studies have proposed frameworks to create, develop, and enhance current practices in both the design and delivery of cybersecurity programs. For instance, a study by Hallett et al. (Hallett et al., 2018) proposed a Cybersecurity Body of Knowledge with the stated aim of providing a common basis to compare various curriculum development frameworks in cybersecurity. Nearly all proposed frameworks are focused on identifying the sets of fundamental knowledge and skills needed to be incorporated in the cybersecurity curricula (Kreider and Almalag, 2019). Several studies reviewed existing cybersecurity and computer science higher education programs' curricula for improvements (Alsmadi and Zarour, 2018; Cabaj et al., 2018; Cao and Ajwa, 2016). Some improvement challenges reported the importance of keeping course material up-to-date and remaining ethical while practicing new skills (Beuran et al., 2016; Santos et al., 2017). Nevertheless, with the goal of enriching individuals' cybersecurity awareness, the study conducted by Przyborski et al. (2019) proposes embedding a compulsory common course for all first-year students across all disciplines. Their evaluation shows promising results (Breitinger et al., 2021).

ENISA perceives the fact that the development of an European Cybersecurity Skills Framework is an integral act that shall shape the Europe's digital future and prosperity (Nurse et al., 2021). A group of professionals were assigned to design the framework with the goal of promoting harmonization in the ecosystem of cybersecurity education, training, and workforce development and to development a common European language in the context of cybersecurity skills.

With the focus on overcoming the cybersecurity skills shortage within EU member states, the underlying objective of the European Cybersecurity Skills Framework is to create a common understanding of the roles, competencies, skills and knowledge utilized by and for individuals, employers and training providers cross the EU member states. Furthermore, the framework serves to support recognition of cybersecurity-related skills and the design of relevant cybersecurity training programs. Hence, the framework is expected to support employment in cybersecurity sectors throughout the Union. The framework's design is articulated based on member state inputs and needs, and therefore, could be restricted to serve the state's digital economy.

In this section, samples of improvement standards and frameworks were reviewed. Our study employs the NICE framework because it adopts the competency-based education method of teaching (Alsmadi and Easttom, 2020).

4. Review of cybersecurity education improvements initiatives

Researchers and academics from all over the world seek to improve and promote cybersecurity education. The results of their work focus on encouraging high school students to pursue careers in cybersecurity, improving existing curricula, and creating an attractive cybersecurity education.

The NCSP is one the driving forces towards designing an effective cybersecurity program. The design paradigm is required to fulfill NCSP goals and requirements. The following are common education requirements found in sample reviewed of world-leading NCSPs:

- **Alignment with NCSP:** Cybersecurity education plays a vital role in the supply of professionals and in the enrichment of an individual's maturity and awareness of cybersecurity. Hence, programs throughout the world should to be in alignment with the NCSP goals and priorities.
- **Dynamic Revision Process:** Cybersecurity programs are required to have a dynamic revision process for their curricula and be able to cope with new and emerging technologies, new forms of cyber threats and attacks, and knowledge of new innovative solutions (Cobb, 2016; Crumpler and Lewis, 2019; Kreider and Almalag, 2019).
- **Workforce Demands on Cybersecurity Skills and Competencies:** Recent studies indicate a shortage in the workforce supply for cybersecurity professionals in terms of numbers and skills (Cobb, 2016; Crumpler and Lewis, 2019; Evans and Reeder, 2010). Cybersecurity curricula should demonstrate their capability to produce skillful cybersecurity professionals in terms of knowledge, skill, and competency.

4.1. Initiatives to attract cybersecurity students

Several initiatives have been made at the national government level to encourage high-school students to pursue cybersecurity education as a future career (Government of Australia, Department of Home Affairs, 2020; Ministry of Public Safety and Emergency

Preparedness of Canada, 2019; UAE - Telecommunication Regulatory Authority, 2019). For instance, the Australian cybersecurity strategic plan (Government of Australia, Department of Home Affairs, 2020) attempts to attract individuals and have them consider cybersecurity as their future profession several initiatives such as: Scholarships, Apprenticeships or apprenticeship-style courses in higher education, Development and delivery of specialist cybersecurity courses for professionals, Re-training initiatives to help existing professionals in other related disciplines transition to the cybersecurity domain, Training or professional development for teachers and board executives through practical partnerships or exchanges with industry figures, and Digital training platforms and students delivered cybersecurity services.

ENISA has recently developed the Cybersecurity Higher Education (CYBERHEAD) program to promote cybersecurity education and to maintain a unique crowd-sourcing database of cybersecurity-related education programs (Nurse et al., 2021).

In addition to various government initiatives, another way to encourage individuals to consider cybersecurity as their future profession is through the creation of activities and competitions. For example, the Pink Elephant Unicorn (PEU), Capture the Flag (CtF), and Collegiate Penetration Testing Competition (CPTC) are examples of famous cybersecurity competitions (Pattanayak et al., 2018; Švábenskỳ et al., 2021). Cheung et al. (2011) and Thomas et al. (2019) investigated the implications of challenge-based learning in the classroom, where challenges and competitions were created to help teach or practice concepts and skills. Once the students were assessed, researchers found that their performance in the classroom had actually improved.

Diversification in instructional and teaching methodologies is an important variable to examine when evaluating the quality of cybersecurity programs. According to the guidelines set by IEEE Computer Society and ACM (2017) and the standards set by National Security Agency and Department of Homeland Security (2020), cybersecurity courses must include practical components in the form of laboratory exercises. These exercises should involve the sufficient tools to properly train students and to practice the application of knowledge in order to develop tangible skills. As an example, China's NCSP emphasizes the importance of having a laboratory environment setup. In line with this, China is planning to establish ten advanced cybersecurity academic institutions installed with cutting-edge technologies and state-of-the-art facilities between 2017–2027 (Daricili and Özdal, 2018).

Zeng et al. (2018) proposed developing virtual and hands-on laboratories for students. Specifically, a web-based virtual platform was designed to conduct cybersecurity data analysis and intelligence. A similar approach was also proposed by Thompson and Irvine (2018), who suggested using virtual environments known as lab-trainers. Studies conducted by Katerattanakul and Kam (2019); Qian et al. (2012); Yuan (2017) emphasized the importance of using hands-on and realistic projects to elevate student competencies in key cybersecurity knowledge and skill domains. In their study, Mislan and Wedge (2016) proposed a similar ideology for their cybersecurity and digital forensics labs. They designed a lab environment that allowed students to assume roles and interact with each other while handling small-scale digital devices. Sharevski et al. (2018) sought to include students from other disciplines in cybersecurity related topics. Namely, they proposed an interdisciplinary course in secure design for cybersecurity students, user interaction design, and visual design. In order to apply the concepts taught in the course, the students were taught to prototype Internet-of-Things (IoT) products, which is another area that is gaining in popularity due to the increased presence of IoT devices and smart things.

Gestwicki and Stumbaugh (2015); Jin et al. (2018); Li and Kulkarni (2016); Olano et al. (2014); Zahed et al. (2019) proposed in their studies game-based learning methods for cybersecurity concepts. These games target students of all ages. The games themselves were developed for both mobile phones and computers and they teach cybersecurity concepts in a simple, easy way that anyone can understand. There are several purposes for these games:

1. To encourage younger students to practice safe digital communication and interactions.
2. To attract students to the cybersecurity field.
3. To offer current cybersecurity students a different, more relaxed and entertaining way of practicing the skills that they learned in class.
4. To enrich individuals' awareness level on cybersecurity and ethics.

Other research studies proposed that students may benefit from exchanging experiences with their peers. Ahmed and Roussev (2018); Govan (2016); Straub (2018) proposed the integration of peer-teaching methods into cybersecurity courses. Straub (2018) and Ahmed and Roussev (2018) used peer-learning as a platform for students to ask questions and discuss class materials together. These labs also included activities for the students to partake in together to learn from each other. For instance, Govan (2016) introduced roles to these lab activities. According to Ahmed and Roussev (2018), 92% of the students that participated in peer-learning believed that discussing the course topics with their classmates helped them understand the material better. A summary of literature and their proposed / studied initiative is depicted in Table 5.

4.2. Initiatives for dynamic revision of cybersecurity curricula

Education programs are required to revise their adherence to accreditation standards (whether national or international) periodically. In fact, nearly all accreditation standards require programs to conduct self-assessment exercises on a yearly basis to demonstrate its effectiveness and capacity to achieve program learning outcomes, as well as to incorporate new and emerging developments to the program curriculum. In comparison to other scientific and engineering disciplines such as mathematics, physics, and mechanical engineering, the cybersecurity discipline is considered to be evolving at a rapid pace (Kreider and Almalag, 2019).

Studies conducted by Alsmadi and Zarour (2018); Beuran et al. (2016); Cabaj et al. (2018); Cao and Ajwa (2016); Kam and Katerattanakul (2014); Luallen and Labruyere (2013); McGettrick (2013); Patterson et al. (2016); Santos et al. (2017); Wei et al. (2016) have reviewed existing cybersecurity and computer science programs to ensure that they include the required material and appropriate courses. Modifications were proposed to cybersecurity programs to keep course modules up-to-date, to ensure that the necessary resources are available and up-to-date, and to introduce new skills (Beuran et al., 2016; Santos et al., 2017).

Cabaj et al. (2018); Harris et al. (2019); Raj and Parrish (2018); Stange et al. (2019); Wei et al. (2016) reviewed several cybersecurity programs offered in different educational institutions to determine their adherence to the accreditation standards set by IEEE Computer Society and ACM (2017); National Security Agency and Department of Homeland Security (2020). Their studies investigated a variety of courses and practical components of cybersecurity curricula that need to be included. Stange et al. (2019) reviewed an accredited program by ACM and Accreditation Board for Engineering and Technology (ABET) called Cyber2yr, which is a cybersecurity program that was proposed for two-year associate degrees. Their study was focused on testing the generalization of accreditation standards for different types of degrees.

Table 5
Summary of methods used to attract individuals to cybersecurity discipline.

Initiative/ Activity	Reference	Main Objective
Government Support	(Daricili and Özdal, 2018; Government of Australia, Department of Home Affairs, 2020; Ministry of Public Safety and Emergency Preparedness of Canada, 2019; The White house, Washington DC, 2018; UAE - Telecommunication Regulatory Authority, 2019; UK (H.M) Government, 2016)	• To provide support for individuals pursuing their future career in cybersecurity • To provide support for research and development in this field. • To provide support for academic institutions and organizations to launch cybersecurity academic and awareness programs.
Competitions	(Cheung et al., 2011; Pattanayak et al., 2018; Thomas et al., 2019)	• To improve competitions and find ways to be more welcoming to those that are interested in cybersecurity as a career.
Different Teaching Methods	(Ahmed and Roussev, 2018; Gestwicki and Stumbaugh, 2015; Govan, 2016; Jin et al., 2018; Katerattanakul and Kam, 2019; Li and Kulkarni, 2016; Mislan and Wedge, 2016; Olano et al., 2014; Qian et al., 2012; Sharevski et al., 2018; Straub, 2018; Thompson and Irvine, 2018; Yuan, 2017; Zahed et al., 2019; Zeng et al., 2018)	• To offer different methods of teaching cybersecurity in addition to the traditional methods to spark interest in newcomers and enhance training for current students.
Curriculum Revision and Improvements	(Alsmadi and Zarour, 2018; Beuran et al., 2016; Cabaj et al., 2018; Cao and Ajwa, 2016; Kam and Katerattanakul, 2014; Luallen and Labruyere, 2013; McGettrick, 2013; Patterson et al., 2016; Santos et al., 2017; Wei et al., 2016)	• To enhance the learning experience for students, as well as help the institution become certified and accredited for cybersecurity education.

The dynamic revision of cybersecurity curriculum is based on multiple influencing factors. The followings are critical influencing factors to consider when revising cybersecurity education and training programs' curricula for improvement:

- NCSP mandates / requirements.
- Labor market demands for cybersecurity skills, knowledge, and competencies in professional cybersecurity workforce.
- New and emerging innovation and research in cybersecurity.
- New and emerging forms of sophisticated cybersecurity threats.
- Evolution in digital information and communication technologies.
- Evolution in cybersecurity education accreditation standards.
- Changing societal expectations (e.g., due to generational culture differences).

An NCSP enforces the improvement of cybersecurity education and awareness programs with the aim of meeting national cyber agendas. Nevertheless, labor market demands and future trends impose the pressure to constantly revise and improve the skill and knowledge requirements of cybersecurity education programs (Gorham, 2019). Emerging innovative cybersecurity knowledge or solutions are also driving factors putting increasing pressure on the need to constantly revise cybersecurity education curricula. For instance, the use and application of blockchain technology in cybersecurity and privacy is an area that needs further attention (Hajizadeh et al., 2020; Maleh et al., 2020). Educating individuals on how cyber threats are conducted and evolving to be more sophisticated is an integral part of cybersecurity education. Studies of new and emerging threats are now essential and should be incorporated into the curricula.

Digital information and telecommunication technologies evolve rapidly, which introduces new aspects to explore and consider for cybersecurity education. For example, new cybersecurity capabilities and challenges are introduced when looking at 6G networks (Gui et al., 2020; Guo et al., 2020). Accreditation standards, and any changes to them, have both a direct and indirect impact on all educational and professional programs curricula. Therefore, cybersecurity programs and credentials must be revised in order to comply with any updates.

4.3. Initiatives for the alignment of cybersecurity knowledge, skills, and competencies

The learning outcomes of cybersecurity education and awareness are incorporated in its curriculum in the form of key-knowledge areas, skill sets, and competencies. Cybersecurity education and awareness programs are required to revise these aspects periodically in order to ensure that their standards meet the labor market demands for the professional cybersecurity workforce. Revision is done regularly to incorporate new or emerging key-knowledge areas, skill sets, and competencies. These revisions are influenced by several factors such as coordinating the cybersecurity curriculum material with the NCSP, as well as adding new trends in digital and information technology, and the latest research and innovation in this discipline. Several frameworks have been proposed to emphasize the factors which influence curriculum design and delivery. Accreditation standards impose mandatory revision cycles of program curricula and self-assessments in order to ensure its efficacy in the goal towards achieving student learning outcomes. For instance, the NICE framework has been designed to provide a lexicon for the cybersecurity workforce (Newhouse et al., 2017; Petersen et al., 2020). ENISA intends to develop a European Cybersecurity Skills Framework to create a common understanding of the relevant roles, competencies, skills and knowledge (Nurse et al., 2021). IEEE and ACM created a joint effort to propose guidelines for defining the structure and fundamental topics to be incorporated into cybersecurity discipline (IEEE Computer Society and ACM, 2017).These guidelines suggest that the key cybersecurity knowledge areas include topics such as data security, software security, network security, human security, and organizational security.

The BCS has proposed accreditation guidelines for professional and academic cybersecurity programs (Irons et al., 2016). These guidelines emphasize important key-knowledge areas in this discipline and require cybersecurity programs to include practical components in their curricula. The UAE's Commission of Academic Accreditation (CAA) new accreditation standard of 2019 has an academic program based on its risk-profile (Commission of Academic Accreditation- Ministry of Education, 2019).

5. Strategy mapping approaches and models

The NCSPs determine a set of strategic goals, objectives, and key-performance indicators towards fulfilling a nation's cybersecurity professional requirements. Therefore, a great part of the responsibility depends on how well cybersecurity education and training programs are aligned with NCSPs and their goals. A pragmatic and systematic process is essential for mapping the high-level cybersecurity strategic goals with cybersecurity programs' curricula to assure adequate maintenance and calibrating the competitively successful growth of the cybersecurity programs for long terms.

To the authors' knowledge, investigating the process of liaising the influencing factors to the revision of cybersecurity curricula has not yet been investigated. Furthermore, there is currently no methodology that is recommended or specifically designed to align and cascade high-level strategic goals to education or training curricula. Thus, in practice, an approach to define required cybersecurity competencies that explicitly links high-level cybersecurity strategic goals and initiatives is needed.

5.1. Balanced scorecard

The Balanced Scorecard (BSC) is one of the most famous methods in strategy mapping and was introduced in the early1990′s (Adamson, 2019; Kopecka, 2015). BSC is used to translate high-level strategic goals into actionable plans. It provides the basis for the development of financial and non-financial BSC measures to monitor strategy execution and performance (Kopecka, 2015). Strategy mapping works as a vehicle to help establishments and individuals interpret the high-level strategic goals and to align their priorities and activities accordingly (Kaplan et al., 2004). Strategy mapping using BSC works by creating a visual representation that demonstrates how to link low-level operational activities to higher-level strategic goals. The BSC has been intensively employed in various domains since it was introduced, as mentioned in (de Almeida Ribeiro et al., 2021; Choong and Islam, 2020; Goldstein, 2020; Moraga et al., 2020; Oliveira et al., 2021; Urquía-Grande et al., 2021).

The BSC interprets strategies based on four perspectives: financial, customer, internal processes, and learning and growth (Adamson, 2019; Kaplan et al., 2004). Generally, the financial and customer perspectives answer the general question: 'What does the business want to accomplish?' while the internal processes, and learning and growth perspectives answer the question 'How does the business plan to accomplish it?' (Adamson, 2019).

Although the BSC is considered to be a mature strategy mapping method, it also has its own deficiencies (Kopecka, 2015). For example, a study conducted by Speckbacher et al. (2003) reported that the BSC method lacks in crucial information, competitive environment and stakeholders orientation. Additionally, the definition of BSC may be unclear and diverse integration may lead to overlooking some crucial issues (Kopecka, 2015). Another study reported that the BSC method's learning and growth perspective does not completely assist organizations in achieving organizational change and strategies (Yee-Ching and Shih-Jen, 1999). In some cases, strategy mapping using the BSC approach requires the integration of other systems or methods to incorporate integral components of planning development, execution, and maintenance. For example, a study conducted by Quezada et al. (2021) proposes the integration of the Analytical Network Process (ANP) to consolidate the implementation of BSC and to generate performance indicators for manufacturing areas within companies. A study conducted by Pakdaman et al. (2021) discussed the benefits of combining BSC with other methods, such as Project Portfolio Management (PPM) and the Analytical Hierarchy Process (AHP) for strategy mapping and prioritization with focus on increasing organizational performance and effectiveness.

The application[2] of strategy mapping using BSC and its four perspectives in this study's context has provided high-level action plans which may be considered, in some cases, as business goals. For instance, addressing the students' experience perspective did not determine which competency to include or to maintain but provided cybersecurity improvement curricula action plan. Nevertheless, results obtained from BSC approach are high-level activities. It is considered to be insufficient when determining which cybersecurity professional competencies to consider when revising cybersecurity education and training program's curricula and work towards achieving the cybersecurity strategic goal to supply competent cybersecurity professionals and to create cybersecurity mature society.

5.2. GQM and GQM+strategies

Goal-Question-Metric (GQM) is a systematic and pragmatic method which explicitly integrates high-level goals with models of various perspectives of interest, based on specific needs. In the GQM+Strategies approach, the goals are first defined in an operational and traceable fashion by clarifying them into a set of quantifiable questions that are utilized to elicit information from the models. These questions and models are employed to determine the metrics. The defined metrics are used to specify the data needs to be collected. The models provide a framework which interprets the collected data (Basili et al., 2007). Fig. 2 depicts the various elements of GQM+Strategies model.

Originally, the GQM approach was defined for evaluating defects for a set of projects the NASA Goddard Space Flight Center environment where the application involved a set of case study experiments (Basili and Selby, 1984; Basili and Weiss, 1984; Caldiera and Rombach, 1994). Though it was originally utilized for a specific project in a particular environment, the GQM has been expanded to be used in more contexts. For example, it has been used for quality improvement for software development organizations and paradigms within an organizational framework, as well as for building software competencies to supply to projects (Caldiera and Rombach, 1994).

According to Basili et al. (2007), the GQM approach is limited when it comes to describing goal dependencies and does not ensure the wholeness of goals to constitute a rich set of relationships. On the other hand, the GQM+Strategies leverages the traditional GQM approach (Caldiera and Rombach, 1994). It is designed to identify and utilize the relationships between goals at different levels. It makes strategic goals and corresponding business goals explicit. In addition, it also makes relationships between business goals and related activities explicit (Basili et al., 2007). The GQM+Strategies sequences activities necessary to achieve the strategic goal, which are defined by business goals and enclosed into scenarios. Links identify the business goals that support the strategic goal achievement. The model GQM+Strategies produces provides an organization with mechanisms to interpret how the selected output is consistent with upper levels within an organization. Moreover, links and outcomes ensure that business goals are fulfilled (Basili et al., 2007).

6. An updated GQM+strategis model

In this study's context, we are proposing updates to the GQM+Strategies model to systematically align the improvement

[2] BSC application to align cybersecurity improvement program goals to NCSP is demonstrated in Appendix A.

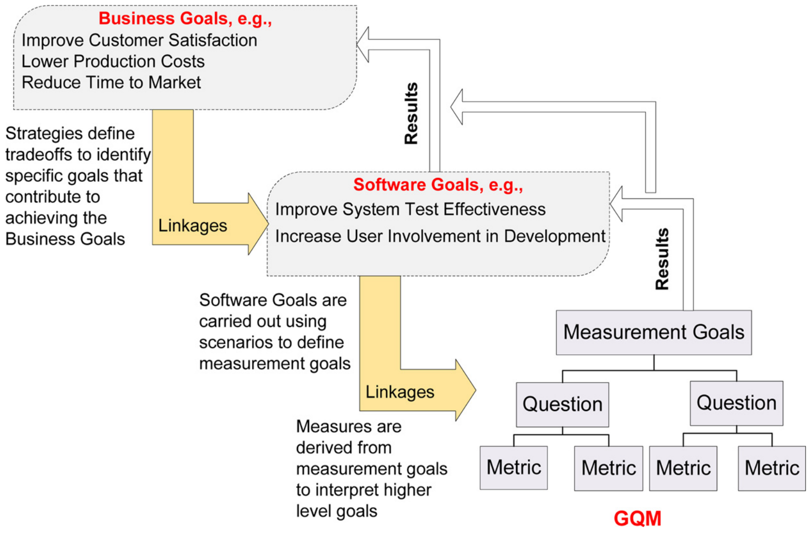
Business Goals, e.g.,
Improve Customer Satisfaction
Lower Production Costs
Reduce Time to Market
Strategies define tradeoffs to identify specific goals that contribute to achieving the Business Goals
Linkages
Results
Software Goals, e.g.,
Improve System Test Effectiveness
Increase User Involvement in Development
Results
Software Goals are carried out using scenarios to define measurement goals
Linkages
Measurement Goals
Question
Question
Measures are derived from measurement goals to interpret higher level goals
Metric
Metric
Metric
Metric
GQM

Fig. 2. GQM+Strategies approach aligning business and project goals to measurement program.

process of cybersecurity education and training curricula to NCSP goals. The newly proposed updated model is called Goal-Question-Outcomes+Strategies (GQO+Strategies). Cybersecurity improvement processes focus on determining the best-fit cybersecurity learning outcomes. The update to GQO+Strategies is made at the quantitative level to produce a systematic alignment that outlines the best-fit learning outcomes instead of metrics. The GQO+Strategies approach is modified while adopting GQM+Strategies peculiarities. It offers cybersecurity education and training providers with meaningful rationale for adequately calibrating best-fit competencies to their curriculum and to have blueprint for justifying/interpreting data at each level of the approach (Basili et al., 2007). Therefore, at each goal level, learning outcomes are defined and linked to the achievement of cybersecurity improvement goals and aligned with cybersecurity strategic goals. Fig. 3 depicts the transformation of the GQM+Strategies approach to GQO+Strategies for the purpose of cybersecurity curricula improvement and alignment with cybersecurity strategic goals integrating NIST-NICE framework for cybersecurity workforce skills and competencies. This study utilizes the UAE's NCSP to derive and align cybersecurity curriculum improvement of the United Arab Emirates University's Master's program in information security.

The GQO+Strategies approach makes the *NCSP goals*, strategies, and corresponding *Cybersecurity Education Improvement* goals explicit. Strategies are formulated that deal with NCSP goals such as supplying cybersecurity professionals, defending from sophisticated cybersecurity threats, and more. The GQO+Strategies approach also makes the relationship between *Cybersecurity Education Improvement* activities and *Curriculum Improvement Goals* explicit. Sequences of activities necessary for accomplishing the goals are defined by the NCSP and embedded into scenarios in order to achieve some cybersecurity education improvement goals. Links are established between each cybersecurity education improvement goals and the NCSP goals it supports. Attached to goals, strategies, and scenarios at each level of the model is the information about the relationships between goals, relevant context factors, and assumptions. The entire model provides NCSP with a mechanism not only to define cybersecurity curriculum improvement consistent with larger, upper level NCSP goals, but also to interpret and roll up the resulting curriculum improvement data at each level. NICE framework was then utilized to select the most appropriate learning outcomes and their competency levels. Finally, GQO+Strategies linkages and curriculum improvement goals in terms of learning outcomes ensure the NCSP goals are fulfilled.

6.1. *GQO+Strategies implementation*

In this section, we explore the potential of applying the updated GQO+Strategies approach to systematically align cybersecurity education and training programs' curriculum improvements to consolidating the achievement of cybersecurity strategic goals. This method is an analytical inspection that focuses specifically on identifying conceptual context for strategic goals, cybersecurity education improvement goals, and curriculum improvement programs as the main influencing factors. It elaborates on the operational context by characterizing the improvement goal with respect to various aspects of the improvement objective to determine the best-fit learning outcomes. Hence, detailing learning outcomes in order to correlate the most appropriate competencies and speciality areas to embrace from a relevant lexicon. Concluded learning outcomes will be therefore used to benchmark against program learning outcomes for improvement.

1. Conceptual level (Goals): Cybersecurity education and training curricula improvement program is defined for a variety of reasons, from various point of view, relative to its environment. Cybersecurity curriculum improvement program output are:
   - Students' learning outcomes.
   - Level of alignment to cybersecurity strategies.
   - Competencies obsolescence.
2. Operational Level: A set of questions to characterize the way to assess the achievement of curriculum improvement goals. Since this study is focused on identifying the most appropriate cybersecurity competencies, questions might be asked in the following formats:
   - What competency do cybersecurity professionals need to acquire in order to ... ?
   - Which competency is best-fit for cybersecurity professionals to acquire to perform ... ?
   - What is the level of the cybersecurity competency cybersecurity professionals need to acquire to successfully achieve, complete, and conduct ... ?
3. Outcomes Level: A set of cybersecurity learning outcomes and speciality areas associated with each question used to characterize the curriculum improvement goal. At this level, the NICE

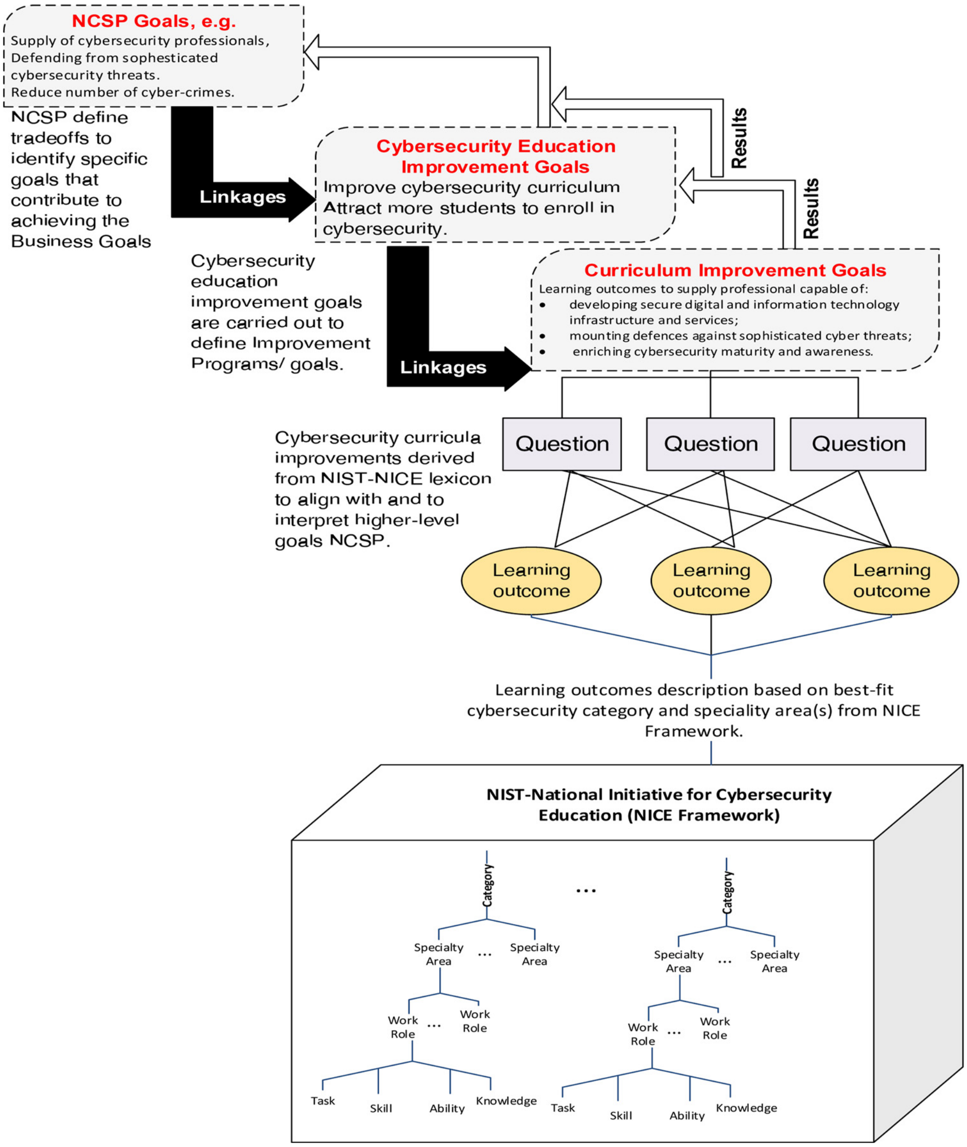
NCSP Goals, e.g.
Supply of cybersecurity professionals,
Defending from sophisticated cybersecurity threats.
Reduce number of cyber-crimes.
NCSP define tradeoffs to identify specific goals that contribute to achieving the Business Goals
Linkages
Results
Cybersecurity Education Improvement Goals
Improve cybersecurity curriculum
Attract more students to enroll in cybersecurity.
Results
Cybersecurity education improvement goals are carried out to define Improvement Programs/ goals.
Linkages
Curriculum Improvement Goals
Learning outcomes to supply professional capable of:
• developing secure digital and information technology infrastructure and services;
• mounting defences against sophisticated cyber threats;
• enriching cybersecurity maturity and awareness.
Cybersecurity curricula improvements derived from NIST-NICE lexicon to align with and to interpret higher-level goals NCSP.
Question
Question
Question
Learning outcome
Learning outcome
Learning outcome
Learning outcomes description based on best-fit cybersecurity category and speciality area(s) from NICE Framework.
NIST-National Initiative for Cybersecurity Education (NICE Framework)
Category
...
Category
Specialty Area
...
Specialty Area
Specialty Area
...
Specialty Area
Work Role
...
Work Role
Work Role
...
Work Role
Task
Skill
Ability
Knowledge
Task
Skill
Ability
Knowledge

Fig. 3. GQO+Strategies approach for cybersecurity education and training curricula improvement and alignment to cybersecurity strategic goals.

framework is utilized to identify best-fit cybersecurity categories and speciality areas. The selection of cybersecurity categories and speciality areas is governed by the systematic alignment of curriculum improvement goals derived from higher-level strategies. Furthermore, it is dependent on the specifications provided in the workforce framework for cybersecurity NICE framework (Petersen et al., 2020).

As a result of examining NCSPs, the following are shared strategic goals which require the supply of professional workforce and the enrichment of individuals' cybersecurity awareness. These strategies will be taken into consideration as cybersecurity education and training programs' curricula improvement program goals.

- **Development** of secure digital and information technology infrastructures and services. This applies to both government and private sectors' critical infrastructures, including its systems, data, and network.
- **Defending** from sophisticated cyber threats by developing appropriate countermeasures to detect and deter cyber threats. This applies to research, development, and innovation in both cybersecurity countermeasures and defense mechanisms. This goal also requires skills in secure operation and maintenance of information technology infrastructure.
- **Enrichment** of individuals' maturity and awareness of cybersecurity and cyber-crime and threats. This applies to awareness programs in both private and national-level organizations.

The GQO+Strategies approach addresses the cybersecurity strategic goals, which are defined as the following:

- **Strategic Goal-1:** *Development of secure digital and information technology infrastructures and services.*
  - **Purpose:** Supply of competent cybersecurity professionals to develop secure and digital critical infrastructures and services.
  - **Issue:** Lack of certain and emerging cybersecurity competencies, advancement in technological solutions, and emerging sophisticated cyber threats.
  - **Sector (theme):** Cybersecurity Education and Training Programs.
  - **Viewpoint:** National Leadership.
- **Strategic Goal-2:** *Defending from sophisticated cyber threats by developing appropriate countermeasures to detect and deter.*

  - **Purpose:** Establishing resilient cyber sovereignty from cyber attacks.
  - **Issue:** Emerging cybersecurity threats with the need for developing countermeasures.
  - **Sector (theme):** Cybersecurity Education and Training Programs.
  - **Viewpoint:** National Leadership.
- **Strategic Goal-3:** *Enrichment of individuals' maturity and awareness of cybersecurity and cyber-crime and threats*.
  - **Purpose:** Reduce cyber-crimes.
  - **Issue:** Enrichment of individuals to combat cyber crimes.
  - **Sector (theme):** Cybersecurity Education and Training Programs.
  - **Viewpoint:** National Leadership.

Business goals can be addressed using the same approach. As defined in the strategic goals, cybersecurity education and training providers are required to align their business goals to achieve the cybersecurity strategic goal and address related issues. The following business goals are just an example, and not an inclusive list, of possible cybersecurity improvement goals. Therefore, education and training providers are not limited to the following cybersecurity improvement business goals:

- **Business Goal-1:** *State-of-the-art cybersecurity education and training program's curricula*.
  - **Purpose:** Emphasizing on the on-demand cybersecurity competencies and to include emerging cybersecurity skills.
  - **Issue:** Updating cybersecurity education program's curricula.
  - **Theme (object):** Cybersecurity Education and Training Programs' Curricula.
  - **Viewpoint:** Cybersecurity Education and Training Providers/Sector.
- **Business Goal-2:** *State-of-the-practice cybersecurity training program's curricula*.
  - **Purpose:** Enrich cybersecurity professionals hands-on capabilities.
  - **Issue:** Revision of cybersecurity hands-on themes curriculum and to introduce state-of-the-practice case studies, experiments, and exercises.
  - **Theme (object):** Cybersecurity Education and Training Programs' Curricula.
  - **Viewpoint:** Cybersecurity Education and Training Providers/Sector.
- **Business Goal-3:** *Cutting-edge facilities and equipment*.
  - **Purpose:** Adopt to new and advanced technology.
  - **Issue:** Coping with technological evolution.
  - **Theme (object):** Cybersecurity Education and Training Programs' Delivery Environment.
  - **Viewpoint:** Cybersecurity Education and Training Providers/Sector.
- **Business Goal-4:** *Cybersecurity research and innovation*.
  - **Purpose:** Pioneer cybersecurity innovation and contribute to its evolution.
  - **Issue:** Participation and exposure to cybersecurity innovation and advanced research.
  - **Theme (object):** Cybersecurity Education and Training Programs.
  - **Viewpoint:** Cybersecurity Education and Training Providers/Sector.

The requirements to achieve NCSP goals are interpreted into business goals. In this study, the business goals are improvements to cybersecurity education and training programs. As a business goal, this will require the establishment of cybersecurity education and training curricula improvement programs. These goals are tackled from various aspects, as described earlier. They are encapsulated by a set questions to identify the best-fit cybersecurity workforce categories and their corresponding speciality areas mapped from the NICE framework. Ideal learning outcomes are then generated based on the description of the matched category from the NICE framework.

Results from implementing GQO+Strategies to determine best-fit cybersecurity competencies to achieve cybersecurity education and training curricula improvement program goals using NICE Framework as a lexicon for cybersecurity workforce competency are illustrated in Table 6.

6.2. Case Study: Utilizing GQO+Strategies to Align UAEU MSc. Program in Information Security Improvement to UAE NCSP

The College of Information Technology at the United Arab Emirates University (UAEU) offers an MSc. degree program in Information Security. The program is designed towards fulfilling growing demands for information technology specialists in the information security discipline (United Arab Emirates University, 2021). The program consists of 30 credit hours in total and is accredited by the UAE's CAA. According to United Arab Emirates University (2021), the MSc. Information Security program focuses on the delivery of six Program Learning Outcomes (PLOs):

1. Apply information security knowledge and effective security strategies and standards.
2. Design effective security solutions based on given requirements.
3. Evaluate in depth enterprise security systems.
4. Execute ethically project work or research that contributes significantly to the information security discipline.
5. Demonstrate advanced oral and written communication skills individually and collectively.
6. Analyze critically emerging information security concepts, models, techniques, and solutions.

Learning outcomes produced from implementing the GQO+Strategies paradigm to align cybersecurity curricula improvement program with cybersecurity strategies are benchmarked against the master program's learning outcomes. Comparing between GQO+Strategies learning outcomes and PLOs, we the program needs improvement in order to align cybersecurity curricula improvement goals with overall cybersecurity strategic goals. For instance, the enrichment goal is not fulfilled in any of the program learning outcomes. Hence, it is expected that graduates of this program will not have the adequate competencies to deliver professional training not awareness programs to individuals. Table 7 shows the bench-marking results.

The benchmarking practice explored some shortcomings in the UAEU master program. It was found that the program offered PLOs that do not cover all cybersecurity workforce categories needed to fulfill the nation's NCSP. For example, a gap analysis study conducted by Crumpler and Lewis (2019) indicated the urgent need for competent cybersecurity professionals to operate and maintain information technology infrastructure securely. This particular set of competencies corresponds to various speciality areas that undergo the 'Operate and Maintain' category of cybersecurity workforce framework. None of the PLOs in the MSc. in Information Security emphasized on or introduced enrichment-related competencies. Thus, this could be considered as another area for improvement. In addition, PLOs delivered by the UAEU master program were found to contribute significantly to defending more than development and neglected enrichment competencies. Some of the learning outcomes of the program are introduced to adhere to national accreditation standards, such as PLO-5. Finally, PLO-6 is found to be generic and does not specifically correspond to any specific cybersecurity workforce competency nor to the identified learning outcomes from GQO+Strategies approach. This learning

Table 6
GQO+Strateiges aApplication using NICE lexicon cybersecurity curricula alignment framework.

Goal	Questions	Learning Outcomes	NICE Framework	
			Categories	Speciality Areas
Development of secure digital and information technology infrastructures and services	What are the knowledge, skills, and competencies required to developed secure constitutes of information technology critical infrastructure?	Create secure information technology solutions	Securely Provision	• Risk Management • Software Development • Systems Architecture • Systems Development • Systems Requirements Planning • Technology Research and Development • Testing and Evaluation
			Operate and Maintain	• System Analysis
Defending from sophisticated cyber threats	What does the cybersecurity professional workforce need to know and do in order to identify, classify, detect, and govern security to withstand sophisticated cyber threats?	Manage, lead, direct, develop or advocate effective conduct of cybersecurity work.	Oversee and Govern	• Cybersecurity Management • Executive Cyber leadership • Legal advise and advocacy • Program/Project Management and Acquisition • Strategic Planning and Policy • Training, Education, and Awareness
		Evaluate threats to IT systems and/or networks and mitigate them.	Protect and Defend	• Cyber Defense Analysis • Cyber Defense Infrastructure Support • Incident Response • Vulnerability Assessment and Management
		Perform a highly-specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence	Analyze	• All-Source Analysis • Exploitation Analysis • Language Analysis • Threat Analysis
	What does the cybersecurity professional workforce need to learn in order to defend and deter sophisticated cyber threats?	Supports specialized denial and deception operations and collection of cybersecurity information that may be used to develop intelligence	Collect and Operate	• Collection Operations • Cyber Operations • Cyber Operational Planning
		Investigates cybersecurity events or crimes related to IT systems, networks, and digital evidence	Investigate	• Cyber Investigation • Digital Forensics
	What cybersecurity competencies are required for operating information technology infrastructure securely?	Provide necessary operational and administration skills to ensure efficient and effective IT system performance and security	Operate and Maintain	• Data Administration • Knowledge Management • Network Administration
			Collect and Operate	• Collection Operations • Cyber Operations • Cyber Operational Planning
	What cybersecurity competencies are required for securely maintaining information technology infrastructures?	Provide adequate maintenance skills and competencies necessary to ensure efficient and effective IT system performance and security	Operate and Maintain	• Customer Services and Technical Support • Network Services • System Analysis
Enrichment of Individuals' Cybersecurity Maturity and Awareness	What are cybersecurity education, teaching, and training delivery knowledge, skill sets, and competencies required for enriching the awareness and maturity for individuals?	Conducts training of personnel within pertinent subject domain. Develops, plans, coordinates, delivers and/or evaluates training courses, methods, and techniques as appropriate.	Oversee and Governance	• Training, Education, and Awareness
		Addresses problems; installs, configures, troubleshoots, and provides maintenance and training in response to customer requirements or inquiries. Provide initial incident information to the Incident Response (IR) Specialty.	Operate and Maintain	• Customer Services and Technical Support
	What are the cybersecurity key-knowledge areas, skill sets, and competencies individuals must acquire to combat cybercrimes and attacks?	Consolidation of the creation of cyber ecosystem	Multiple categories and speciality areas	• Several key-knowledge areas, skill sets, and competencies that might be selected from the beginners or intermediate levels from various categories and speciality areas.

Table 7
GOQ+Strategies learning application to improve cybersecurity program.

UAEU - MSc. Information Security PLOs	Knowledge level (Blooms Taxonomy)	GQO+Strategies Cybersecurity Learning Outcomes	Category	NICE-Capability Indicator	Improvement Goal
1- Apply information security knowledge and effective security strategies and standards	Apply	Manage, lead, direct, develop and/or advocate effective conduct of cybersecurity work.	Oversee & Govern	Intermediate	Defending
2- Design effective security solutions based on given requirements.	Create	Create secure information technology solutions	Securely Provision	Advanced	Development
3- Evaluate in-depth enterprise security systems	Evaluate	Perform highly-specialized reviews and evaluation of incoming cybersecurity information to determine its usefulness for intelligence	Analyze	Advanced	Defending
		Supports specialized denial and deception operations and collections of cybersecurity information that may be used to develop intelligence	Collect & Operate	Advanced	Defending
		Evaluate threats to IT systems and/or networks and mitigate them.	Protect & Defend	Advanced	Defending
		Investigates cybersecurity events or crimes related to IT systems, networks, and digital evidence	Investigate	Advanced	Defending
4- Execute ethically project work or research that contributes significantly to the information security discipline.	Create	Create secure information technology solutions.	Securely Provision	Advanced	Development
5- Demonstrate advanced oral and written communication skills individually and collectively	Apply	Not Applicable	Not Applicable	Not Applicable	Not Applicable
6- Analyze critically emerging information security concepts, models, techniques, and solutions.	Analyze	Not Applicable	Not Applicable	Not Applicable	Not Applicable
Not Applicable	Not Applicable	Provide necessary operational and administrative skills to ensure efficient and effective IT system performance and security	Operate and Maintain	Advanced	Defending
Not Applicable	Not Applicable	Provide adequate maintenance skills and competencies necessary to ensure efficient and effective IT system performance and security	Operate and Maintain	Advanced	Defending
Not Applicable	Not Applicable	Addresses problems, and installs, configures, troubleshoots, and provides maintenance and training in response to customer requirements or inquiries. Provide initial incident information to the Incident Response (IR) specialty.	Operate and Maintain	Advanced	Enrichment
Not Applicable	Not Applicable	Conducts training of personnel within pertinent subject domains. Develops, plans, coordinates, delivers and/or evaluates training courses, methods, and techniques as appropriate.	Oversee and Governance	Advanced	Enrichment

outcome was placed to assure dynamic compliance and to cope with new and emerging UAE-NCSP mandates.

7. Discussion

The NICE framework elaborates on various cybersecurity workforce competency categories and specialty areas, as well as their corresponding knowledge, skill sets, and level (Daimi and Francia III, 2020; Dawson et al., 2019; Petersen et al., 2020). Three main levels were determined according to cybersecurity workforce proficiency or capability indicators: Beginner, Intermediate, and Advanced.

The development of secure digital and information technology infrastructures and services is identified as one of the cybersecurity improvement program goals. This goal was characterized by a set of questions and contributes to the supply of professional cybersecurity competencies by enabling them to develop, operate, and maintain critical infrastructures and services securely. Identifying adequate learning outcomes to include in cybersecurity education and training program curricula is the final stage of this process. At this point, detailed learning outcomes mapped to their corresponding cybersecurity workforce framework categories and speciality areas are illustrated and become more specific. The underlying objective of this paradigm is to ease the process of mapping the high-level cybersecurity strategic goals to the improvement initiatives of cybersecurity education and training using cybersecurity workforce lexica. Hence, consolidating the achievement of the NCSP.

Similarly, being able to defend against cyber threats by developing appropriate countermeasures to detect and deter them is a key characteristic on its own. Therefore, defence-related cybersecurity speciality areas are considered as the second strategic goal. Due to its significant influences, this goal was the subject of our study and the basis for revising cybersecurity education and training programs' curricula for improvement.

Enrichment of individuals awareness to create a mature society to withstand against cybercrimes and cyberattacks is vital to national sustainability and the establishment of a cyber ecosystem. This strategic goal influences the design of cybersecurity education and training programs significantly. For instance, learning outcomes consolidating the achievement of this strategic goal shall enable cybersecurity to:

- Assuring that skills are acquired for cybersecurity education, teaching, teaching methods evaluation, and training delivery.
- Defining the set and level of key-knowledge areas, skill sets, and competencies required to withstand and combat cybersecurity crimes and attacks.
- Continuously evolving cybersecurity awareness programs for effectiveness and updates.

We have found that the achievement of cybersecurity strategic goals for the enrichment of individuals and communities maturity and awareness on cyber crime and attacks requires mapping various key-knowledge areas, skills sets, and competencies from multiple categories and speciality areas. More importantly, by studying the levels of these aspects for mature awareness on cyber crime and attacks, we recommended training providers to refer to the NICE framework capabilities indicator to select the most appropriate level for cybersecurity learners.

8. Conclusions

In this paper, we reviewed a sample of NCSPs from world-leading countries from different regions around the world: US, UK, EU, Russian Federation, China, Australia, ASEAN, UAE, and Switzerland. Observations from the review include the lack of professionally trained cybersecurity specialists and the need to design cybersecurity programs that align with international best practices. We also reviewed cybersecurity education improvement initiatives and efforts for attracting students, dynamic revisions of cybersecurity curricula, and the consolidation of achievements of national cybersecurity strategic goals. These achievements were reviewed by aligning cybersecurity education curricula improvement initiatives.

We then proposed a GQO+Strategies paradigm that draws upon the NICE framework and Blooms' taxonomy, and demonstrated how it can be applied using the MSc. in Information Security program at the UAEU as a case study. Implementing this paradigm has shown that our method is effective when determining areas of improvement for an academic cybersecurity program.

Declaration of Competing Interest

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

CRediT authorship contribution statement

Saleh AlDaajeh: Conceptualization, Methodology, Writing – original draft. **Heba Saleous:** Conceptualization, Methodology, Writing – original draft. **Saed Alrabaee:** Supervision, Writing – original draft. **Ezedin Barka:** Writing – review & editing. **Frank Breitinger:** Writing – review & editing. **Kim-Kwang Raymond Choo:** Writing – review & editing.

Appendix A. BSC Application on NCSP Alignment with Cybersecurity Curricula Improvement

This study is primarily focused on the academic context, in particular, improving cybersecurity education and training programs' curricula by aligning it to national cybersecurity strategy. Hence, support the achievement of NCSP. Each of the BSC perspectives will be addressed by a set of questions amended to the context of this study. Figure A.4 depicts the BSC approach and its four perspectives (Kaplan et al., 2004).

The question addressing the finance perspective of the cybersecurity strategic maps would be 'How a cybersecurity program success is measured by stakeholders?'. This would include any activity that contributes to the financial growth/sustainability within and outside the academic/training institution. The primary customer in this context is the cybersecurity learner / students. In this case, the question to address the second perspective - customer's perspective - would be 'What values does the cybersecurity program provide to learners' experiences?'.

The third perspective 'internal processes' refers to the core-business processes of the program, and operational excellence; establishing an unique education and training environment; adequately delivering proposed outcomes; and compliance with national and international accreditation standards. The question addressing the third perspective 'internal processes' would be asked as 'What core business processes does cybersecurity education and training programs have to be good at?'. The fourth perspective of the strategy mapping BSC is the 'knowledge and growth'. Knowledge and growth of cybersecurity education and training program would be addressed by asking the question 'What knowledge management practices to implement and professional development activities that would contribute to the development and optimization of the cybersecurity program?'. Tables A.8, A.9, A.10, and A.11 illustrate an application example for mapping cybersecurity strategies to cybersecurity education and training programs using the BSC

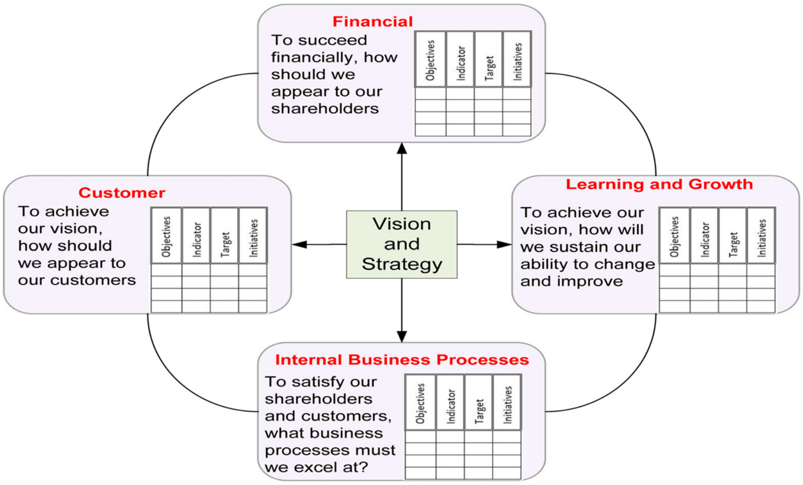
Financial
To succeed financially, how should we appear to our shareholders
Objectives
Indicator
Target
Initiatives
Customer
To achieve our vision, how should we appear to our customers
Objectives
Indicator
Target
Initiatives
Vision and Strategy
Learning and Growth
To achieve our vision, how will we sustain our ability to change and improve
Objectives
Indicator
Target
Initiatives
Internal Business Processes
To satisfy our shareholders and customers, what business processes must we excel at?
Objectives
Indicator
Target
Initiatives

Fig. A1. BSC and its four perspectives: Alignment of strategic goals to business activities.

Table A1
BSC application on aligning cybersecurity strategies to cybersecurity education program: Finance perspective.

Strategy Definition	Institute Academic Expectations	Academic Objectives	Specific Deliverable
Activities that would contribute to financial gain	• Program committees influencing financial gain. • Grants and scholarships • Research proposals in cybersecurity domains • Student capacity and retention rates • International students recruitment • Balanced work-load among faculty members • Alignment with national cybersecurity agenda	• Maximize involvement in committees influencing financial growth/sustainability of organization (e.g. research committee, recruitment committee).	• Industry and research committee • National research and development support for cybersecurity • Research proposals in cybersecurity domains • International students recruitment improvement program • Industrial partnerships and external fund • Organizing and hosting international events

Table A2
BSC application on aligning cybersecurity strategies to cybersecurity education program: Students' experience perspective.

Strategy Definition	Institute Academic Expectations	Academic Objectives	Specific Deliverable
Refers to the value proposition for students' experience	• Students involvement in cybersecurity research activities • State-of-the-art practice experiences in cybersecurity discipline. • Students' enrichment programs	• Curricula revision to align to NCSP • Student professional development programs • Student participation in research and scholarly activities	• State-of-the-art curriculum • Cutting-edge facilities and IT laboratories • Student publications, conferences, clubs, and journals

Table A3
BSC application on aligning cybersecurity strategies to cybersecurity education program: Internal processes perspective.

Strategy Definition	Institute Academic Expectations	Academic Objectives	Specific Deliverable
Refers to the 'core business' processes of cybersecurity program and operational excellence, building education and training delivery, or research platform through innovations	• New courses and revision of learning outcomes • New teaching and delivery techniques, methods, and approaches • Program self-evaluation techniques, methods, and approaches • Faculty teaching load distribution and planning • New assessment and progress evaluation tools	• Complying with accreditation standards • Implementing a faculty promotion policy and system • Program self-evaluation techniques, methods, and approaches • Faculty involvement in curricula improvement initiatives	• Faculty members contribution to cybersecurity course delivery. • Foundation courses are allocated to novice faculty members. • Rotate faculty members on different program services committees • Faculty professional development and support programs.

Table A4
BSC application on aligning cybersecurity strategies to cybersecurity education program: Knowledge and growth perspective.

Strategy Definition	Institute Academic Expectations	Academic Objectives	Specific Deliverable
Activities that shall contribute to the development and optimization of cybersecurity program delivery, research, and professional development	• Cybersecurity program knowledge management policies and system • Automated tools and systems for knowledge sharing, storing, and retrieval • Encourage faculty members' collaboration in research projects • Support faculty members to organize and bid for international conferences • Internal clubs and publications	• Data and information management systems • Faculty conferences, journal publications, training and professional workshops • Knowledge sharing, ethics, rules, and regulations • Support faculty members to organize and bid for international conferences. • Internal clubs and publications.	• Emerging teaching methods using technology (e.g., virtual distance teaching). • Faculty orientation on Intellectual property laws and regulations. • Knowledge management system improvement program.

four perspectives: finance, students' experience, Internal Processes and knowledge and growth respectively.

References

Adamson, K., 2019. Strategy mapping: An essential tool for new academic faculty - faculty focus | higher ed teaching & learning. https://www.facultyfocus.com/articles/faculty-development/strategy-mapping-an-essential-tool-for-new-academic-faculty/. (Accessed on 07/21/2021).

Ahmed, I., Roussev, V., 2018. Peer instruction teaching methodology for cybersecurity education. IEEE Security & Privacy 16 (4), 88–91.

de Almeida Ribeiro, J., Ladeira, M.B., de Faria, A.F., Barbosa, M.W., 2021. A reference model for science and technology parks strategic performance management: an emerging economy perspective. J. Eng. Tech. Manage. 59, 101612.

Alsmadi, I., Easttom, C., 2020. The NICE Cyber Security Framework. Springer.

Alsmadi, I., Zarour, M., 2018. Cybersecurity programs in saudi arabia: Issues and recommendations. In: 2018 1st International Conference on Computer Applications & Information Security (ICCAIS). IEEE, pp. 1–5.

Basili, V., Heidrich, J., Lindvall, M., Munch, J., Regardie, M., Trendowicz, A., 2007. Gqm+ strategies–aligning business strategies with software measurement. In: First International Symposium on Empirical Software Engineering and Measurement (ESEM 2007). IEEE, pp. 488–490.

Basili, V.R., Selby, R.W., 1984. Data collection and analysis in software research and management. Proceedings of the American Statistical Association and Biomeasure Society 13–16.

Basili, V.R., Weiss, D.M., 1984. A methodology for collecting valid software engineering data. IEEE Trans. Software Eng. 728–738.

Beuran, R., Chinen, K.-i., Tan, Y., Shinoda, Y., 2016. Towards effective cybersecurity education and training. Technical Report. Japan Advanced Institute of Science and Technology.

Booz, H.Allen, 2017. The 2017 (isc) 2 global information security workforce study. Center for Cyber safety and Education ISC2.

Breitinger, F., Tully-Doyle, R., Przyborski, K., Beck, L., Harichandran, R.S., 2021. First year students' experience in a Cyber World course–an evaluation. Education and Information Technologies 26 (1), 1069–1087.

Cabaj, K., Domingos, D., Kotulski, Z., Respício, A., 2018. Cybersecurity education: evolution of the discipline and analysis of master programs. Computers & Security 75, 24–35.

Caldiera, V.R.B.G., Rombach, H.D., 1994. The goal question metric approach. Encyclopedia of software engineering 528–532.

Cao, P.Y., Ajwa, I.A., 2016. Enhancing computational science curriculum at liberal arts institutions: a case study in the context of cybersecurity. Procedia Comput Sci 80, 1940–1946.

Cheung, R.S., Cohen, J.P., Lo, H.Z., Elia, F., 2011. Challenge based learning in cybersecurity education. In: Proceedings of the International Conference on Security and Management (SAM). The Steering Committee of The World Congress in Computer Science, Computer Ọ, p. 1.

Choong, K.K., Islam, S.M., 2020. A new approach to performance measurement using standards: a case of translating strategy to operations. Operations Management Research 13 (3), 137–170.

Cobb, S., 2016. Mind this gap: Criminal hacking and the global cybersecurity skills shortage, a critical analysis. In: Virus Bulletin Conference, pp. 1–8.

Commission of Academic Accreditation- Ministry of Education, 2019. Standards for Institutional Licensure and Program Accreditation in UAE December 2019. 2020 (accessed May 9, 2020).

Crick, T., Davenport, J.H., Irons, A., Prickett, T., 2019. A uk case study on cybersecurity education and accreditation. arXiv preprint arXiv:1906.09584.

Crumpler, W., Lewis, J.A., 2019. Cybersecurity Workforce Gap. Center for Strategic and International Studies (CSIS).

Daimi, K., Francia III, G., 2020. Innovations in Cybersecurity Education. Springer.

Daricili, A.B., Özdal, B., 2018. Analysis of the cyber security strategies of people's republic of china. Security Strategies Journal 14 (28).

Dawson, M., Taveras, P., Taylor, D., 2019. Applying software assurance and cybersecurity nice job tasks through secure software engineering labs. Procedia Comput Sci 164, 301–312.

De Inovação, S.P., 2018. Overview of Cybersecurity Status in ASEAN and the EU. 2018. Technical Report. European Union Horizon's 2020 Research and Innovation Program.

ENISA, 2020. The European Union agency for cybersecurity. [Online]. Available at: https://www.enisa.europa.eu/about-enisa.

Evans, K., Reeder, F., 2010. A human capital crisis in cybersecurity: Technical proficiency matters. CSIS.

Federal IT Steering Unit (FITSU), 2018. National strategy for the protection of Switzerland against cyber risks 2018–2022. [Online]. Available at: https://www.ncsc.admin.ch/dam/ncsc/en/dokumente/strategie/Nationale_Strategie_Schutz_Schweiz_vor_Cyber-Risiken_NCS_2018-22_EN.pdf.download.pdf/Nationale_Strategie_Schutz_Schweiz_vor_Cyber-Risiken_NCS_2018-22_EN.pdf.

Gestwicki, P., Stumbaugh, K., 2015. Observations and opportunities in cybersecurity education game design. In: 2015 Computer Games: AI, Animation, Mobile, Multimedia, Educational and Serious Games (CGAMES). IEEE, pp. 131–137.

Ghafir, I., Saleem, J., Hammoudeh, M., Faour, H., Prenosil, V., Jaf, S., Jabbar, S., Baker, T., 2018. Security threats to critical infrastructure: the human factor. J Supercomput 74 (10), 4986–5002.

Goldstein, J.C., 2020. Strategy maps: the middle management perspective. Journal of Business Strategy.

Gorham, M., 2019. Internet Crime Report - Annual Report 2019. Technical Report. Federal Bureau of Investigation (FBI-IC3), USA.

Govan, M., 2016. The application of peer teaching in digital forensics education. Higher Education Pedagogies 1 (1), 57–63.

Government of Australia, Department of Home Affairs, 2020. Australia cyber security strategy 2020. [Online]. Available at: https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf.

Gui, G., Liu, M., Tang, F., Kato, N., Adachi, F., 2020. 6G: Opening new horizons for integration of comfort, security and intelligence. IEEE Wireless Commun..

Guo, L., Ye, J., Du, L., 2020. Cyber-physical security of energy-efficient powertrain system in hybrid electric vehicles against sophisticated cyber-attacks. IEEE Trans. Transp. Electrif..

Hajizadeh, M., Afraz, N., Ruffini, M., Bauschert, T., 2020. Collaborative cyber attack defense in SDN networks using blockchain technology. In: 2020 6th IEEE Conference on Network Softwarization (NetSoft). IEEE, pp. 487–492.

Hakak, S., Khan, W.Z., Imran, M., Choo, K.R., Shoaib, M., 2020. Have you been a victim of covid-19-related cyber incidents? survey, taxonomy, and mitigation strategies. IEEE Access 8, 124134–124144.

Hallett, J., Larson, R., Rashid, A., 2018. Mirror, mirror, on the wall: what are we teaching them all? characterising the focus of cybersecurity curricular frameworks. 2018 USENIX Workshop on Advances in Security Education ASE 18).

Haney, J.M., Lutters, W.G., 2021. Cybersecurity advocates: discovering the characteristics and skills of an emergent role. Information & Computer Security.

Harris, M.A., et al., 2019. Using bloom's and webb's taxonomies to integrate emerging cybersecurity topics into a computic curriculum. Journal of Information Systems Education 26 (3), 4.

Herjavec, 2019. 2019 official annual cybercrime report.

HM-Government - The Rt Hon Steve Barclay MP Chancellor of the Duchy of Lancaster and Minister for the Cabinet Office, 2022. Uk national cyber strategy 2022–2025. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1053023/national-cyber-strategy-amend.pdf. (Accessed on 03/20/2022).

Hranický, R., Breitinger, F., Ryšavý, O., Sheppard, J., Schaedler, F., Morgenstern, H., Malik, S., 2021. What do incident response practitioners need to know? a skillmap for the years ahead. Forensic Science International: Digital Investigation 37, 301184. doi:10.1016/j.fsidi.2021.301184. https://www.sciencedirect.com/science/article/pii/S2666281721000925

IEEE Computer Society, ACM, 2017. Cybersecurity curricula 2017: Curriculum guidelines for post-secondary degree programs in cybersecurity.

Irons, A., Savage, N., Maple, C., Davies, A., Turley, L., 2016. Cybersecurity learning. [Online]. Available at: https://www.bcs.org/content-hub/cybersecurity-learning/.

Jin, G., Tu, M., Kim, T.-H., Heffron, J., White, J., 2018. Evaluation of game-based learning in cybersecurity education for high school students. Journal of Education and Learning (EduLearn) 12 (1), 150–158.

Kam, H.-J., Katerattanakul, P., 2014. Diversifying cybersecurity education: A non-technical approach to technical studies. In: 2014 IEEE Frontiers in Education Conference (FIE) Proceedings. IEEE, pp. 1–4.

Kaplan, R.S., Kaplan, R.E., Norton, D.P., Davenport, T.H., Norton, D.P., et al., 2004. Strategy maps: Converting intangible assets into tangible outcomes. Harvard Business Press.

Katerattanakul, P., Kam, H.-J., 2019. Enhancing student learning in cybersecurity education using an out-of-class learning approach. Journal of Information Technology Education: Innovations in Practice 18 (1), 29–47.

Kopecka, N., 2015. The balanced scorecard implementation, integrated approach and the quality of its measurement. Procedia Economics and Finance 25, 59–69.

Kreider, C., Almalag, M., 2019. A framework for cybersecurity gap analysis in higher education. SAIS 2019 Proceedings 6.

Li, C., Kulkarni, M.R., 2016. Survey of cybersecurity education through gamification. 2016 ASEE Annual Conference & Exposition.

Lilly, B., Cheravitch, J., 2020. The past, present, and future of Russia's cyber strategy and forces. In: 2020 12th International Conference on Cyber Conflict (CyCon), Vol. 1300. IEEE, pp. 129–155.

Luallen, M.E., Labruyere, J.-P., 2013. Developing a critical infrastructure and control systems cybersecurity curriculum. In: 2013 46th Hawaii International Conference on System Sciences. IEEE, pp. 1782–1791.

Maleh, Y., Shojafar, M., Alazab, M., Romdhani, I., 2020. Blockchain for cybersecurity and privacy: architectures, challenges, and applications. CRC Press.

Marquardson, J., Elnoshokaty, A., 2020. Skills, certifications, or degrees: what companies demand for entry-level cybersecurity jobs. Information Systems Education Journal 18 (1), 22–28.

McGettrick, A., 2013. Toward effective cybersecurity education. IEEE Security & Privacy 11 (6), 66–68.

Ministry of Education- UAE, 2015. Ministry of Education: K-12 Computer Science and Technology Standards. Accessed October 9, 2020.

Ministry of Public Safety and Emergency Preparedness of Canada, 2019. National cyber security action plan 2019–2024 of canada. [Online]. Available at: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg-2019/ntnl-cbr-scrt-strtg-2019-en.pdf.

Mislan, R.P., Wedge, T., 2016. Designing laboratories for small scale digital device forensics. Annual ADFSL Conference on Digital Forensics, Security, and Law.

Moraga, J.A., Quezada, L.E., Palominos, P.I., Oddershede, A.M., Silva, H.A., 2020. A quantitative methodology to enhance a strategy map. Int. J. Prod. Econ. 219, 43–53.

National Security Agency, Department of Homeland Security, 2020. National centers of academic excellence in cyber defense education program (CAE-CDE): Criteria for measurement - bachelor, master, and doctoral level.

Nautiyal, L., Rashid, A., Hallett, J., Shreeve, B., K, M., E, C., H, C., 2022. The united kingdoms cyber security degree certification program: a cyber security body of knowledge case study. IEEE Security Privacy 20 (1), 87–95. doi:10.1109/MSEC.2021.3127845.

NeSmith, B., 2018. Council post: The cybersecurity talent gap is an industry crisis. [Online]. Available at: https://www.forbes.com/sites/forbestechcouncil/?sh=70d45011649b.

Newhouse, W., Keith, S., Scribner, B., Witte, G., 2017. National initiative for cybersecurity education (nice) cybersecurity workforce framework. [Online]. Available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf.

Nurse, J.R., Adamos, K., Grammatopoulos, A., Di Franco, F., 2021. Addressing the eu cybersecurity skills shortage and gap through higher education. European Union Agency for Cybersecurity (ENISA) Report.

Olano, M., Sherman, A., Oliva, L., Cox, R., Firestone, D., Kubik, O., Patil, M., Seymour, J., Sohn, I., Thomas, D., 2014. Securityempire: development and evaluation of a digital game to promote cybersecurity education. 2014 USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE 14).

Oliveira, C., Martins, A., Camilleri, M.A., Jayantilal, S., 2021. Using the balanced scorecard for strategic communication and performance management. In: Strategic Corporate Communication in the Digital Age. Emerald Publishing Limited, pp. 78–87.

Pakdaman, M., Abbasi, A., Sankaran, S., 2021. Translating organisational strategies to projects using balanced scorecard and AHP: a case study. International Journal of Project Organisation and Management 13 (2), 111–134.

Pattanayak, A., Best, D.M., Sanner, D., Smith, J., 2018. Advancing cybersecurity education: pink elephant unicorn. In: Proceedings of the Fifth Cybersecurity Symposium, pp. 1–7.

Patterson, W., Winston, C.E., Fleming, L., 2016. Behavioral cybersecurity: a needed aspect of the security curriculum. In: SoutheastCon 2016. IEEE, pp. 1–7.

Petersen, R., Santos, D., Smith, M., Witte, G., 2020. Workforce Framework for Cybersecurity (NICE Framework). Technical Report. National Institute of Standards and Technology.

Pranggono, B., Arabo, A., 2020. Covid-19 pandemic cybersecurity issues. Internet Technology Letters.

Przyborski, K., Breitinger, F., Beck, L., Harichandran, R.S., 2019. 'Cyber-World' as a theme for a university-wide first-year common course. 2019 ASEE Annual Conference & Exposition (Presented at Cyber Technology) https://peer.asee.org/31923.

Qian, K., Lo, C.-T.D., Guo, M., Bhattacharya, P., Yang, L., 2012. Mobile security labware with smart devices for cybersecurity education. In: IEEE 2nd Integrated STEM Education Conference. IEEE, pp. 1–3.

Quezada, L.E., Aguilera, D.E., Palominos, P.I., Oddershede, A.M., 2021. An anp model to generate performance indicators for manufacturing firms under a balanced scorecard approach. Eng. Manage. J. 1–15.

Raj, R.K., Parrish, A., 2018. Toward standards in undergraduate cybersecurity education in 2018. Computer (Long Beach Calif) 51 (2), 72–75.

Sabillon, R., 1993. Cyber Security Auditing, Assurance, and Awareness Through CSAM and CATRAM. IGI Global Information Science, USA.

Santos, H., Pereira, T., Mendes, I., 2017. Challenges and reflections in designing cyber security curriculum. In: 2017 IEEE World Engineering Education Conference (EDUNINE). IEEE, pp. 47–51.

Sapolu, K., Haruna, S., Koyabe, M., Tambeayuk, F., Rigoni, A., Obiso, M., Weisser, C., Ciglic, K., Kaska, K., Silfversten, E., Satola, D., Sergeant, S., Barayre, C., 2018. Guide to developing a national cybersecurity strategy: Strategic engagement in cybersecurity. Technical Report. International Telecommunication Union.

Sharevski, F., Trowbridge, A., Westbrook, J., 2018. Novel approach for cybersecurity workforce development: a course in secure design. In: 2018 IEEE Integrated STEM Education Conference (ISEC). IEEE, pp. 175–180.

Shoemaker, D., Davidson, D., Conklin, A., 2017. Toward a discipline of cyber security: some parallels with the development of software engineering education. EDPACS 56 (5–6), 12–20.

Speckbacher, G., Bischof, J., Pfeiffer, T., 2003. A descriptive analysis on the implementation of balanced scorecards in german-speaking countries. Management accounting research 14 (4), 361–388.

Stange, M., Tang, C., Tucker, C., Servine, C., Geissler, M., 2019. Cybersecurity associate degree program curriculum. In: 2019 IEEE International Symposium on Technologies for Homeland Security (HST). IEEE, pp. 1–5.

Straub, J., 2018. Assessment of the educational benefits produced by peer learning activities in cybersecurity. 126th Annual Conference & Exposition.

Švábenskỳ, V., Čeleda, P., Vykopal, J., Brišáková, S., 2021. Cybersecurity knowledge and skills taught in capture the flag challenges. Computers & Security 102, 102154.

The White house, Washington DC, 2018. National cyber strategy of the united states of america. [Online]. Available at: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

Thomas, L.J., Balders, M., Countney, Z., Zhong, C., Yao, J., Xu, C., 2019. Cybersecurity education: From beginners to advanced players in cybersecurity competitions. In: 2019 IEEE International Conference on Intelligence and Security Informatics (ISI). IEEE, pp. 149–151.

Thompson, M.F., Irvine, C.E., 2018. Individualizing cybersecurity lab exercises with labtainers. IEEE Security & Privacy 16 (2), 91–95.

Trilling, R., 2018. Creating a new academic discipline: Cybersecurity management education. In: Proceedings of the 19th Annual SIG Conference on Information Technology Education, pp. 78–83.

UAE - Telecommunication Regulatory Authority, 2019. UAE national cybersecurity strategy 2019. [Online]. Available at: https://u.ae/en/about-the-uae/strategies-initiatives-and-awards/federal-governments-strategies-and-plans/national-cybersecurity-strategy-2019.

UK (H.M) Government, 2016. National cybersecurity strategy 2016–2021. [Online]. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf.

United Arab Emirates University, 2021. Master of science in information security. https://www.uaeu.ac.ae/en/catalog/graduate/programs/master-of-science-in-information-security.shtml. (Accessed on 08/01/2021).

United Nations Institute for Disarmament Research, 2017. Cyber Policy Portal - Russian Federation. Technical Report. United Nations Institute for Disarmament Research.

Urquía-Grande, E., Lorain, M.-A., Rautiainen, A.I., Cano-Montero, E.I., 2021. Balance with logic-measuring the performance and sustainable development efforts of an npo in rural ethiopia. Eval Program Plann 87, 101944.

Wei, W., Mann, A., Sha, K., Yang, T.A., 2016. Design and implementation of a multi–facet hierarchical cybersecurity education framework. In: 2016 IEEE Conference on Intelligence and Security Informatics (ISI). IEEE, pp. 273–278.

Yee-Ching, L. C., Shih-Jen, K. H., 1999. The use of balanced scorecard in canadian hospitals.

Yuan, D., 2017. Design and develop hands on cyber-security curriculum and laboratory. In: 2017 Computing Conference. IEEE, pp. 1176–1179.

Zahed, B.T., White, G., Quarles, J., 2019. Play it safe: An educational cyber safety game for children in elementary school. In: 2019 11th International Conference on Virtual Worlds and Games for Serious Applications (VS-Games). IEEE, pp. 1–4.

Zeng, Z., Deng, Y., Hsiao, I., Huang, D., Chung, C.-J., 2018. Improving student learning performance in a virtual hands-on lab system in cybersecurity education. In: 2018 IEEE Frontiers in Education Conference (FIE). IEEE, pp. 1–5.

Saleh H. AlDa'ajeh received the B.S. degree in computer science from University of Petra, Amman, Jordan, in 2007 and his MSc. degree in software engineering from the Blekinge Institute of Technology, Karlskrona, Sweden, in 2010. He is currently pursuing the Ph.D. degree in Information Security at the United Arab Emirates University, College of Information Technology, AlAin, UAE. From 2010 to 2016, he worked as a senior lecturer and curriculum developer for the Information Security Engineering Technology department, AD Polytechnic, Abu Dhabi, UAE. His research interest are in the areas of Information security with focus on Reverse Engineering, Reliability of Internet of Things, and Dependability Engineering in safety-critical systems. Saleh AlDaajeh is an IEEE member.

Heba Saleous (PhD Student - Information Systems and Security) holds a B.Sc. in Computer Engineering from the American University of Sharjah in the United Arab Emirates (UAE) and an M.Sc. in Information Security from the UAE University. She is currently an Information Security PhD candidate in UAE University under the supervision of Dr. Marton Gergely. Her research interests include digital forensics, malware, network security, security policies, and cybersecurity education. She is currently working to improve digital forensics education.

Saed Alrabaee is currently an Assistant Professor at the department of Information Systems and Security in UAEU. Prior to joining UAEU, Dr. Alrabaee was a visiting assistant professor at the department of Electrical and Computer Engineering and Computer Science at the University of New Haven (UNH), US. He is also a permanent research scientist at the Security Research Center, CIISE, Concordia University, Canada. Dr. Alrabaee holds a Ph.D. degree in information system engineering from Concordia University in Montreal, Canada. His research and development activities and interests focus on the broad area of reverse engineering, including, binary authorship attribution and characterization, and malware investigation. In this domain, Dr Saed has published more than 30 articles in top tier journals and in prestigious conferences.

Ezedin Barka is currently an Associate Professor at the United Arab Emirate University. He received his Ph.D. in Information Technology from George Mason University, Fairfax, VA in 2002, where he was a member of the Laboratory for Information Security Technology (LIST). His current research interests include Access Control, where he published a number of papers addressing delegation of rights using RBAC. Other research areas include Digital Rights Management (DRM), Large-scale security architectures and models, Trust management, Security in UAVs, and Network "Wired & Wireless" and distributed systems security. Dr. Barka has published over 50 Journals and conference papers. Dr. Barka is an IEEE member, member of the IEEE Communications Society and member of the IEEE Communications & Information Security Technical Committee (CISTC). He serves on the technical program committees of many international IEEE conferences such as ACSAC, GLOBECOM, ICC, WIMOB, and WCNC. In addition, he has been a reviewer for several international journals and conferences.

Frank Breitinger is an Associate Professor for Digital Forensic Science at the University of Lausanne (CH). Before, he was an Assistant Professor at the Hilti Chair for Data and Application Security of the University Liechtenstein (6/2019 to 4/2021) and at the University of New Haven (CT, US; 08/2014 to 08/2019) where he also acted as the co-director of the University of New Haven Cyber Forensics Research and Education Group (UNHcFREG,https://eur03.safelinks.protection.outlook.com/?url=http%3A%2F%2Fwww.unhcfreg.com%2F&amp;data=04%7C01%7Csalrabaee%40uaeu.ac.ae%7C0b50cffd6b22460011cb08d8f9e660c0%7C97a92b044c8743419b08d8051ef8dce2%7C0%7C0%7C637534116383041468%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C2000&amp;sdata=L2ar8afDe9yKuKKAktrVplGhiWo1Skb%2BoDc%2BTfg2gJE%3D&amp;reserved=0). His teaching and research interests are cybersecurity and digital forensics. Additional information about him and his work is on his website (https://eur03.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.fbreitinger.de%2F&amp;data=04%7C01%7Csalrabaee%40uaeu.ac.ae%7C0b50cffd6b22460011cb08d8f9e660c0%7C97a92b044c8743419b08d8051ef8dce2%7C0%7C0%7C637534116383041468%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C2000&amp;sdata=nabqC8DaZUYZ%2F04R44qJQdI54e3D8NKk5M9VkAtzopk%3D&amp;reserved=0).

Kim-Kwang Raymond Choo received the Ph.D. in Information Security in 2006 from Queensland University of Technology, Australia. He currently holds the Cloud Technology Endowed Professorship at The University of Texas at San Antonio (UTSA). He serves as the Department Editor of IEEE Transactions on Engineering Management, and the Associate Editor of IEEE Transactions on Dependable and Secure Computing, and IEEE Transactions on Big Data. He is an ACM Distinguished Speaker and IEEE Computer Society Distinguished Visitor (2021 - 2023), and included in Web of Science's Highly Cited Researcher in the field of Cross-Field - 2020. He is named the Cybersecurity Educator of the Year - APAC (Cybersecurity Excellence Awards are produced in cooperation with the Information Security Community on LinkedIn) in 2016, and in 2015 he and his team won the Digital Forensics Research Challenge organized by Germany's University of Erlangen-Nuremberg. He is the recipient of the 2019 IEEE Technical Committee on Scalable Computing Award for Excellence in Scalable Computing (Middle Career Researcher), the 2018 UTSA College of Business Col. Jean Piccione and Lt. Col. Philip Piccione Endowed Research Award for Tenured Faculty, the British Computer Society's 2019 Wilkes Award Runner-up, the 2014 Highly Commended Award by the Australia New Zealand Policing Advisory Agency, the Fulbright Scholarship in 2009, the 2008 Australia Day Achievement Medallion, and the British Computer Society's Wilkes Award in 2008. He has also received best paper awards from the IEEE Consumer Electronics Magazine for 2020, EURASIP Journal on Wireless Communications and Networking in 2019, IEEE TrustCom 2018, and ESORICS 2015; the Korea Information Processing Society's Journal of Information Processing Systems (JIPS) Outstanding Research Award (Most-cited Paper) for 2020 and Survey Paper Award (Gold) in 2019; the IEEE Blockchain 2019 Outstanding Paper Award; and Best Student Paper Awards from Inscrypt 2019 and ACISP 2005.