Global Perspectives on Cybersecurity Education for 2030: A Case for a Meta-discipline

Allen Parrish*
Mississippi State University
United States
aparrish@research.msstate.edu

John Impagliazzo†
Hofstra University
United States
john.impagliazzo@hofstra.edu

Rajendra K. Raj†
Rochester Institute of Technology
United States
rkr@cs.rit.edu

Henrique Santos†
Universidade do Minho
Portugal
hsantos@dsi.uminho.pt

Muhammad Rizwan Asghar
The University of Auckland
New Zealand
r.asghar@auckland.ac.nz

Audun Jøsang
University of Oslo
Norway
josang@mn.uio.no

Teresa Pereira
Instituto Politécnico de Viana do Castelo, Portugal
tpereira@esce.ipvc.pt

Eliana Stavrou
University of Central Lancashire
Cyprus
estavrou@uclan.ac.uk

ABSTRACT

Information security has been an area of research and teaching within various computing disciplines in higher education almost since the beginnings of modern computers. The need for security in computing curricula has steadily grown over this period. Recently, with an emerging global crisis, because of the limitations of security within the nascent information technology infrastructure, the field of "cybersecurity" is emerging with international interest and support. Recent evolution of cybersecurity shows that it has begun to take shape as a true academic perspective, as opposed to simply being a training domain for certain specialized jobs. This report starts from the premise that cybersecurity is a "meta-discipline." That is, cybersecurity is used as an aggregate label for a wide variety of similar disciplines, much in the same way that the terms "engineering" and "computing" are commonly used. Thus, cybersecurity should be formally interpreted as a meta-discipline with a variety of disciplinary variants, also characterized through a generic competency model. The intention is that this simple organizational concept will improve the clarity with which the field matures, resulting in improved standards and goals for many different types of cybersecurity programs.

CCS CONCEPTS

• **Social and professional topics** → **Model curricula**; **Computing education**; **Computing education programs**;

KEYWORDS

ITiCSE working group, cybersecurity education, computer security education, information assurance education, global standards.

ACM Reference Format:
Allen Parrish, John Impagliazzo, Rajendra K. Raj, Henrique Santos, Muhammad Rizwan Asghar, Audun Jøsang, Teresa Pereira, and Eliana Stavrou. 2018. Global Perspectives on Cybersecurity Education for 2030: A Case for a Meta-discipline. In *Proceedings of the 23rd Annual ACM Conference on Innovation and Technology in Computer Science Education (ITiCSE Companion '18), July 2–4, 2018, Larnaca, Cyprus.* ACM, New York, NY, USA, 19 pages. https://doi.org/10.1145/3293881.3295778

1 INTRODUCTION

Unfilled cybersecurity positions will number around 3.5 million across the world by 2021 [55]. As a result, many "alternative education" programs have been created, which include certification-based courses, online courses, and other non-traditional approaches to training and education. Some of these programs have been used as alternatives to college, and many high school computing and cybersecurity programs are designed to support career paths that do not involve traditional college attendance. By short-circuiting college, training programs quickly ramp up the size of the cybersecurity workforce, but lack the many benefits of a traditional undergraduate college education [58].

Universities are increasing their offerings at the undergraduate level to develop a qualified cybersecurity workforce in several ways. First, traditional computing programs, such as computer science, are incorporating security content, as illustrated by various model curricula documents [6–8, 43], as well as by recent work by ABET [3], the predominant accreditation body for programs in computing, engineering, engineering technology, and applied and

*Working Group Leader
†Working Group Co-Leader

ITiCSE Companion '18, July 2–4, 2018, Larnaca, Cyprus

ACM ISBN 978-1-4503-6223-8/18/07…$15.00
https://doi.org/10.1145/3293881.3295778

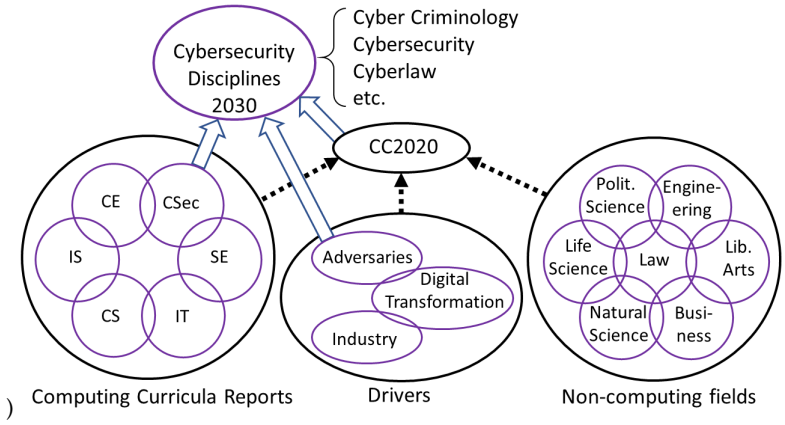


Figure 1: Towards Cybersecurity as a Meta-Discipline

natural science in the United States. In their latest accreditation criteria, ABET now requires coverage of some cybersecurity principles in all undergraduate computing programs. ABET has also created new criteria for cybersecurity and for engineering programs.

Additionally, universities are now offering standalone cybersecurity programs, most often as continuing education in the context of executive education or certificate programs, and sometimes as professional master's programs. They have also begun to offer standalone undergraduate cybersecurity programs of a more traditional format. ABET has recently produced accreditation criteria for undergraduate degree programs in cybersecurity, which will complement existing accreditation criteria for programs in computer science, information systems and information technology.

The above categories of programs are present in universities around the world. While existing academic disciplines evolve to incorporate cybersecurity content, separate degree programs are likely to continue well into the future. How should cybersecurity degrees coexist alongside other degree programs within the modern university? Several different variants of cybersecurity currently exist, for instance, in criminal justice, computer science, information technology or software engineering, while others are included within various degrees in business, law and the various social sciences. Any reasonable cybersecurity education framework thus needs to allow for a wide variation of types of cybersecurity degrees.

Any framework that promotes stability and growth needs to have a unifying basis and be accompanied by a well-understood set of terms and concepts. One definition of cybersecurity is: "a computing-based discipline involving technology, people, information, and processes to enable assured operations in the context of adversaries. It involves the creation, operation, analysis, and testing of secure computer systems. It is an interdisciplinary course of study, including aspects of law, policy, human factors, ethics, and risk management" [30].

The unifying basis for cybersecurity is that it focuses on the "adversarial aspects" of computing, *i.e.,* to study the prevention and detection of threats and the response to attacks. The maturation of the cybersecurity discipline is essential for ensuring that the digital transformation of society becomes sustainable in the long term. This paper proposes that the term "cybersecurity" be used with the specific intent of referring to a broad "meta-discipline" covering a broad spectrum of disciplinary variants, with corresponding bachelor-level programs, as illustrated in Figure 1. It is necessary to understand and manage the adversarial aspects of computing, and to respond to the need for enforcing laws and policies in cyberspace.

Just as Louis Fein's seminal paper in 1959 [23] proposed "computer sciences" as a discipline and as a university organizational unit, a similar proposal and rationale is needed for a terminological and organizational framework for cybersecurity. The proposal of the 'computer sciences' as a disciplinary area was followed by the formation of numerous computer science programs within the 1960s, which was a period of major technological demand. With a unified basis and terminological conceptualization of cybersecurity, more institutions are likely to formalize and accredit their fledgling, ad hoc programs in this space.

Similarly, degree programs in cybersecurity can be blended from concepts across a wide spectrum of disciplines, and depending on the area of emphasis, several substantially different degree programs could take on the "cybersecurity" title or other similarly generic name. Due to the ambiguity associated with the current use of program and degree names, it is useful to distinguish the notion of "big-cybersecurity" from the various individual cybersecurity disciplines. Here, big-cybersecurity is a meta-discipline, or the really broad concept that encompasses several more specific disciplines, much like the way *engineering*, *mathematics*, or *science* are broad meta-disciplines that are made up of many different specific disciplines. The suggestion therefore is that the individual cybersecurity disciplines – termed as "small-cybersecurity" – need different names that directly describe their areas of emphases, *e.g.*, network security, cyber criminology, or secure software development. Disciplines including political science, law, liberal arts and psychology have an impact on different "small-cybersecurity" disciplines. For example, Dawson and Thomson discuss the impact of skills beyond just technical that will have an impact on the future cybersecurity workforce [18].

This report proposes a consistent terminological framework around a vision for cybersecurity education. As such, it clarifies the scope of what is included in a cybersecurity degree and what is part of the field of study in at least two ways by discussing:

(1) The emergence of the various types of cybersecurity degrees, and
(2) The collection of learning competencies that define a boundary around cybersecurity as a descriptor of degree programs.

The remainder of the report is organized as follows. Section 2 is a review of previous efforts to characterize cybersecurity as a discipline. Section 3 is a review of currently active efforts in this area, and Section 4 is a conceptual framework for the future that is organized around the idea of cybersecurity as a family of academic disciplines.

2 PRIOR INVESTIGATIONS OF GLOBAL CYBERSECURITY EDUCATION

This section summarizes prior efforts in global cybersecurity education, based heavily on three ITiCSE working group reports. The first of these reports explored the state of cybersecurity education in 2009 [17]; the second outlined draft curricular guidelines in 2010 [16]; and the third examined cybersecurity education in institutions offering two- and four-year degrees in 2011 [45]. Note that these earlier reports are written in terms of "information assurance," the term commonly used for cybersecurity in that time period.

These three past ITiCSE reports capture the history of cybersecurity education, and as a core set of members participated in each of the three working groups, the reports follow similar formats and provide a three-year sequence, starting with "exploration" to "curricula guidelines" to "information assurance education."

2.1 The ITiCSE 2009 Working Group Report

The 2009 ITiCSE working group explored "the space of various existing information assurance educational standards and guidelines, and how they may serve as a basis for helping to define the field of information assurance" [17]. The group studied the position of security in other areas of computing, for example, computer science within the CS 2008 guidelines [15] and information technology within IT 2008 [33]. Given that few undergraduate computing faculty members in the early 2000s focused on cybersecurity education, the 2009 report treated cybersecurity education as a global issue rather than limited to a single country. Broader curricular recommendations had been made to include security in computer engineering (CE2004), software engineering (SE2004), computer science (CS2008), and information technology (IT2008), discussed in more detail in Section 3.3.

The 2009 report examined the growth of cybersecurity education and training starting in the 1970s when industrial conferences began to provide continuing education courses in cybersecurity topics such as audit and security management, with commercial training programs such as SANS, ISC2, and ISACA came into existence. Additionally, college faculty began to develop and teach coursework on computer security, with full courses emerging by the early 1980s, specific information security journals dedicated to academic research papers emerged. Significant changes occurred in 1987 when the National Computer Security Center (NCSC), of the US National Security Agency (NSA) brought together subject matter experts from government, academia and industry to develop six undergraduate curriculum modules for use by computer science professors [17]. This was the first effort by the US government with an objective to promote and coordinate computer security education. The Cooper et al. report [17] also traces the history of cybersecurity, starting with several efforts of the US governmental agencies and continuing with professional societies such as the International Federation for Information Processing (IFIP) working group WG 11.8, ACM, IEEE, the British Computer Society, and the Australian Computer Society. In 1998, the Centers of Academic Excellence (CAE) [30] in Information Assurance Education (IAE), later renamed Cyber Defense, recognized institutions with significant cybersecurity education programs and encouraged other institutions to develop such offerings. The report also identified the role of government standards and guidelines that helped to improve the quality of Information Assurance (IA) education in the US and other Western countries. For instance, ISO 17024:2003 certified US organizations for use by the US Department of Defense, and the development of the 1998 NIST Special Publication 800-16 as a "living handbook" for training for federal agencies.

A variety of industry-based and vendor-specific IA training and certification programs also developed to provide necessary training for personnel in the workforce. Two categories of vendor training and certifications are those that are vendor-specific and those that are vendor-neutral. Vendor-specific IA training addresses specific products and services, whereas vendor-neutral IA training addresses the general IA knowledge areas necessary for a given occupation, *e.g.,* system administrator or systems security certified practitioner. The primary stakeholders in industry-based training were the leads/heads of companies and organizations who were responsible for the success of their organizations, and needed to consider a balance between training and education for their employees and also manage the training costs.

The report also focused on one of the greatest challenges associated with education and training, that is, to determine a success metric that relates to the actual learning that has taken place.

2.2 The ITiCSE 2010 Working Group Report

The 2010 report [16] built on the 2009 report and focused on existing cybersecurity curricula, as well as key government- and industry-oriented cybersecurity education standards and guidelines. By 2010, cybersecurity (then called information assurance) was already viewed as a set of technical and managerial controls designed to ensure the confidentiality, possession of control, integrity, authenticity, availability, and utility of information and information systems. It included measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation.

The 2010 working group took the first steps toward defining educational models for cybersecurity by addressing two specific problems: (a) identification of topics that comprehensively defined cybersecurity, independent of degree program and specific academic discipline, and (b) development of a set of topics and associated student learning outcomes for one cybersecurity subject

to serve as a model for future efforts to define other subjects. To create a Cybersecurity Body of Knowledge (BoK), they distributed an electronic survey to all existing US CAE [57] institutions. The survey was a tool to synthesize varied curricular content of these cybersecurity programs into a single comprehensive set of topic areas to define the space of cybersecurity education. The working group received 33 responses of which 29 were usable for data analysis. The questions included typical demographics as well as two additional questions related to (a) the actual percentage of a course of study covering each of a given set of major topic areas, and (b) the percentage of the course of study that should cover each of these major topic areas. The major topic areas identified were fundamental aspects: cryptography, ethics, policy, digital forensics, access controls, security architecture, network security, risk management, attacks/defenses, operational issues, and secure software design and engineering. The topics listed were sufficient to cover the field.

The working group used the survey findings to help define an all-encompassing cybersecurity BoK. The working group resolved the BoK into 11 major areas and related subjects. In particular, the group concluded that both theory and practice were *defining characteristics* of cybersecurity education, and that the compelling distinguishing feature of cybersecurity, as compared to other disciplines, is the presence of opposing actors or adversaries.

For each of the 11 cybersecurity subject areas, the report also identified the topics and learning outcomes associated with that subject. The purpose was to develop a template for all eleven areas described above. Key principles, common issues, learning outcomes at different Bloom's levels and assessment rubrics were included for each topic. The specific subject chosen for detailed exploration was *secure coding*.

In short, the working group proposed 11 areas that constitute cybersecurity education, with 83 associated subjects. The in-depth coverage of secure coding was set up as a model for descriptions of the other 82 subjects. The group also called for bodies such as ACM to develop and own these curricular guidelines for cybersecurity.

2.3 The ITiCSE 2011 Working Group Report

The 2011 report [45] examined a broad set of undergraduate cybersecurity two- and four-year programs at college levels. Within the US, the group focused on the challenge of articulation between two- and four-year programs; articulation refers to agreements between two-year and four-year programs to allow for smoother transfer of students. The group also looked at cybersecurity programs at international institutions to gain insight into differences between US and non-US cybersecurity programs. Across the board in 2011, as at present, the group noted that consensus about what constitutes cybersecurity education had not been reached, which resulted in bachelor degrees in cybersecurity or related disciplines with widely varying curricula. For US institutions only, the NSA/DHS CAE (for four-year undergraduate, as well as graduate programs) and CAE2Y (for two-year programs) guidance [57] provides some curricular guidance, but not to constrain the breadth and depth of cybersecurity degree programs.

Within the US, community colleges (which offer two-year programs) play a major role in the education of cybersecurity technicians, practitioners and professionals. However, the lack of curricular guidance and standards, as well as program establishment and sustainability, were major challenges. Common two-year cybersecurity degrees included both the associate of science (AS) degree and the associate of applied science (AAS) degree; students graduating with the former often intend to transfer to four-year undergraduate programs while the latter traditionally prepares students to enter the workforce immediately upon graduation. The working group examined the content, context and purpose of 16 associate-degree programs in cybersecurity. Of the approximate 1200 community colleges nationwide, only 13 had received the CAE2Y designation by 2011. Industry-based certifications in AAS degree programs provided an easier path to employment and standardized assessment of prior learning, but made articulation into four-year programs harder, as the skill-based training did not provide educational concepts needed for long-term career growth.

In 2011, most US cybersecurity programs were at the graduate level, but a few full-fledged four-year undergraduate cybersecurity programs were emerging, despite the lack of clarity about what exactly constituted such a program. The working group identified 73 CAE institutions offering bachelor degrees with cybersecurity concentrations or minors. Of these, 42 were housed in computer science, 16 within computer information systems, six are in security departments, five in information technology, four in housed in informatics, three in electrical and computer engineering departments, one in software engineering, and one in criminal justice. The four-year cybersecurity degree programs had names such as information security and assurance (1), cybersecurity (2), information assurance and forensics (2), information technology (1), infrastructure assurance (1), computer science - security track (1), and computer and network security (1). Other than covering network security, introductory security concepts and ethics, it was hard to discern any other commonalities across the nine programs.

The working group considered cybersecurity education at institutions outside the US, where the term "information assurance" is not typically used. Looking at bachelor-level computing security programs, the group compared bachelor-level computing security programs at seven non-US institutions using the list of eleven IA subjects suggested by the 2010 ITiCSE working group (see above), augmented with four additional subjects to reflect non-US programs' needs: fundamental aspects, cryptography, ethics, policy, digital forensics, access control, security architecture, network security, risk management, attacks/defenses, operational issues, secure software design and engineering, computer science, soft skills, practice, project, thesis, and other optional areas. The working group found many similarities among the security programs in coursework on software development, networks, database systems, and operating systems. The programs also had significant differences in terms of the quantity and depth of security-related topics, or the program objectives (preparation for workforce or advanced study).

The bachelor's programs within and outside the US thus revealed commonalities and differences. Degree programs in fields, such as computer engineering, permitted students to pursue concentrations in security, and these degrees were both terminal and continuing. However, the duration of the degree program varied from three to

four years, depending on whether general education was included or not. Ethics was more prevalent in US programs, but often covered as part of general education. All programs worldwide suffered shortcomings in terms of curriculum due to the lack of a common understanding of what defines the cybersecurity discipline or disciplines.

3 CURRENT STATE OF THE WORLD

This section summarizes current cybersecurity education efforts on a global scale. Section 3.1 examines the different frameworks that have been developed for organizing cybersecurity skills and training. Section 3.2 examines different approaches that have been taken by different countries and organizations to increase cybersecurity expertise. Finally, Section 3.3 examines the different curricular standards and guidance, as well as accreditation criteria that have been developed worldwide.

3.1 Cybersecurity Skills, Training and Education Frameworks

This subsection examines the different cybersecurity frameworks that have been developed both within the US and elsewhere for developing skills, providing training and education in cybersecurity.

US National Initiative for Cybersecurity Education (NICE)

NICE [41] is an initiative of the US National Institute of Standards and Technology (NIST), which joins academia, governments and private sector to develop cybersecurity education and training framework. The NIST NICE cybersecurity framework serves as a reference resource for describing and sharing information about cybersecurity work as well as the knowledge, skill, and ability (KSA) needed to complete tasks that strengthen the cybersecurity posture of an organization.

The primary NICE strategic goal is to support employers to plan and guide career development and workforce enhancement, to respond to market needs and to enhance recruitment, hiring, development and retention of cybersecurity talents. The objectives within this strategic goal include the following [40]:

- Identify and analyze data sources to support the identification of the present and future cybersecurity needs.
- Publish and raise awareness of the NICE Framework and encourage its adoption as a reference resource for actions related to cybersecurity workforce, training and education.
- Promote tools to support professionals and contracting managers with recruitment, hiring, development and retention of cybersecurity professionals.
- Promote international collaboration for sharing best practices in cybersecurity career development and workforce planning.

To support organizations in managing roles and responsibilities, the NICE framework encompasses the following core components [40]:

- **Categories** comprise the overarching organizational structure of the NICE Framework. It includes seven categories and with each category composed of specialty areas and work roles. This organizational structure comprises a high-level grouping of common cybersecurity functions based on extensive job analyses, which includes work and workers that share common major functions, regardless of job titles or other occupational conditions.
- **Specialty areas** are distinct areas of cybersecurity work categories. There are 32 specialty areas identified in the National Cybersecurity Workforce Framework, version 2.0 [41]. Each specialty area represents an area of concentrated work, or function, within cybersecurity and related work. In previous versions of the NICE framework, tasks and KSA were associated with each specialty area. Now the KSA and Tasks are associated with the work roles.
- **Work roles** are the most detailed groupings of cybersecurity or cyber-related work, which include baseline knowledge, skills and abilities required to perform a set of tasks. Cybersecurity responsibilities and work roles are grouped into specific classes of categories and specialty areas.
- **Tasks** are specific work activities that combined with other identified tasks, comprise the work in a specific specialty area or work roles.
- **Knowledge, Skills, and Abilities (KSAs)** consist of the required attributes to perform tasks, generally demonstrated through relevant experience or performance-based education and training.

Institute of Information Security Professionals

The Institute of Information Security Professionals (IISP) has published the IISP Skills Framework [29] that specifies a range of competencies that Information Security and Information Assurance Professionals are expected to have to effectively perform their role. This initiative involved collaboration between private and public organizations, academic institutions, and security experts.

The IISP report identifies six levels of skill useful for the assessment of performance. Table 1 provides a summary of the meaning of these levels as expressed in the 2018 IISP report. The six skill levels are used against the ten skill areas specified in the framework, as shown in Table 2. For each skill area, the framework proposes a range of competencies that a professional should possess.

North Atlantic Treaty Organization

In recent years and as a consequence of several security incidents affecting several North Atlantic Treaty Organization (NATO) member states [37], the organization started a dedicated project Multi-National Cyber Defense Education & Training Project (MN CD E&T) [36], framed by its smart defense projects program, to provide NATO and allied nations the education and training necessary to respond to these emerging threats. Even so the project is more focused on defense aspects and despite some prevalent opinions about the singularities of the cyber defense education [19], the model and the process promoted by the project, in particular concerning the skill set and competencies, are very similar to what we could expect from any program to build curricula-related outputs on cybersecurity.

MN CD E&T used, as a starting point, European Defense Agency (EDA) and NATO specific and related documents characterizing

Table 1: Meanings of Competency Levels

Level	Trait	Meaning	Knowledge	Practice
1	Basic knowledge of principles/follow good user practice (*Knowledge*)	Acquired and can demonstrate basic knowledge associated with a skill		
2	Knowledge and Understanding of basic principles (*Knowledge and Understanding*)	Understands the skill and its application	Demonstrates basic knowledge associated with skill; understands how to apply the skill.	Can explain the principles of the skill and how to apply it; should be aware of recent developments in the skill.
3	Practitioner (*Apply*)	Understands the skill and applies it to basic tasks with *some* supervision.	Acquired a good understanding of the knowledge associated with the skill and how to apply the skill	Has experience in applying the skill to a variety of basic tasks; can work as an effective member of a team; contributes ideas to the application of the skill; has experience in training potential and actual practitioners.
4	Senior Practitioner (*Enable*)	Understands the skill and applies it to basic tasks with *minimal* supervision; normally operates as a member of a team.	Acquired a deep understanding of the knowledge associated with the skill; understands how to apply the skill.	Has experience in applying the skill to a variety of tasks; contributes ideas in the application of the skill; aware of recent developments in the skill; has experience in training Information security professionals in the skill; contributes ideas for technical development.
5	Principal Practitioner (*Advise*)	Understands the skill and applies it to complex tasks with *no* supervision; leads teams in a project; operates at a corporate level.	Acquired a deep understanding of the knowledge associated with the skill; knows how to apply the skill across several projects in different environments.	Has experience in applying the skill to a variety of complex tasks; has significant personal responsibility or autonomy; contributes ideas in the application of the skill; contributes ideas for technical development; has effective leadership and management skills; demonstrates awareness of recent developments in the skill; contributes ideas for technical development.
6	Expert/Lead Practitioner (*Initiate, Enable, Ensure*)	An authority who leads implementation of the skill; is an expert, as acknowledged by peers in the skill.	Same as for level 5.	Has oversight responsibility for overall application of the skill across a range of customers; a subject matter expert within a large organization; leads innovative work to enhance the skill; develops and leads programs of advanced training in the skill.

Table 2: IISP Security Disciplines

Section	Security Discipline
A	Information Security Governance and Management
B	Threat Assessment and Information Risk Management
C	Implementing Secure Systems
D	Assurance: Audit, Compliance and Testing
E	Operational Security Management
F	Incident Management, Investigation and Digital Forensics
G	(Not Used)
H	Business Resilience
I	Information Security Research
J	Management, Leadership, Business and Communications
K	Contributions to the Information Security Profession and Professional Development

target jobs and competencies, but keeping open the possibility to include similar documents (*e.g.,* the NIST models) from other sources both at national and international levels. With that information the project produced a cyber defense competencies and skills specification [31], which was used as a reference to identify a gap analysis over the actual education and training programs. After that first exercise a set of disciplines and/or courses were generated, which will integrate the future NATO cyber academia - replacing the actual NATO Communication and Information Systems School, starting in January 2019, at Oeiras, Portugal. More detailed information can be obtained from the project site [36]. The project includes representatives from several countries/organizations, including military, academic and private sector, and rapidly called the attention of EU that joined NATO in several recent cybersecurity initiatives [28].

The project and the proposed competencies model led to the adoption of four levels of expertise that each course within the curricula provides [31]:

- basic knowledge;
- comprehension and application;
- analysis; and

- synthesis and evaluation.

This characterization closely follows the well-known Bloom's Taxonomy [13] for classification of learning outcomes, but collapses two of the levels. This approach is linked to the hierarchical nature of military organizations, not a justification based on outcomes or specific skills at each level. However, the target job definition and gap analysis appear appropriate to design courses aligned with real-world requirements.

Summary

The frameworks analyzed above converge in several aspects, though they use different approaches. The NATO proposal is more focused on cyber defense, including several specific competencies (namely those concerning defense activities), while the other two are more related to cybersecurity. The NICE framework is more focused on job definition and characterization, while the IISP framework follows an organization more consistent to curricula requirements. Note that the NATO's framework gap analysis process and the level of detail about skills are a useful characterization of cyber defense skills.

3.2 Cybersecurity Strategies

This subsection takes a look at the approaches or strategies that different countries and organizations have taken towards the development of cybersecurity expertise.

European Union

Many countries in Europe have defined a national cybersecurity strategy (NCSS), where the European Union Agency for Network and Information Security (ENISA) provides a good overview [22]. European national strategies typically include objectives for building cybersecurity capabilities, enhancing awareness and for providing cybersecurity education. Some initiatives have emerged in relation to cybersecurity education in general, especially from governmental organizations aimed at certifying cybersecurity courses and at providing guidelines for the subject areas that they expect to be included within the syllabi of cybersecurity modules. These guidelines can also serve as a set of criteria against which cybersecurity courses are certified.

ENISA itself published its first "National Cyber Security Strategy Good Practice Guide" in 2012. The 2016 version of the document analyzes the status of NCSS in the European Union and the European Free Trade Area (EFTA), and is meant to support EU member states in their efforts to develop and update their NCSS [21]. Therefore, the target audience of this guide are public officials and policy makers. The guide also provides useful insights for the stakeholders involved in the life cycle of the strategy, such as private, civil and industry stakeholders.

The ENISA guide presents six steps for the design and development of NCSS:

(1) Set the vision, scope, objectives and priorities
(2) Follow a risk assessment approach
(3) Take stock of existing policies, regulations and capabilities
(4) Set a clear governance structure
(5) Identify and engage stakeholders
(6) Establish trusted information-sharing mechanisms

In addition, the ENISA guide describes fifteen objectives for the implementation of NCSS:

- Develop national cyber contingency plans
- Protect critical information infrastructure
- Organize cyber security exercises
- Establish baseline security measures
- Establish incident reporting mechanisms
- Raise user awareness
- Strengthen training and educational programs
- Establish an incident response capability
- Address cyber crime
- Engage in international cooperation
- Establish a public-private partnership
- Balance security with privacy
- Institutionalize cooperation between public agencies
- Foster R&D
- Provide incentives for the private sector to invest in security measures

The recently enacted general data protection regulation (GDPR) sets strict requirements for adequate security assurance when building and operating ICT solutions. By definition, adequate security assurance is the condition of being compliant with the GDPR requirement of 'privacy by design.' The concept of 'security by design' denotes the elements needed to provide adequate security assurance in general, and typically encompasses the following elements [42, 46]:

- Cybersecurity skills/training for designers, operators and users of IT systems
- Security requirements and specification for planned systems
- Security design and architecture for planned systems
- Secure software and development of systems
- Security testing of systems
- Security in the deployment and continuous operation of systems
- Security management within stakeholder organizations and their partners

Note that skills/training is one of the elements of 'security by design,' which calls for more detailed guidelines for which type of skills/training is needed within the context of GDPR.

Australia

Like other countries, Australia has also released its cybersecurity strategy in 2016 [11]. This strategy focuses on building a smart nation and highlights the issue of current shortfall in the cybersecurity workforce. As stated in the strategy, the issue can only be fixed through investment in long-term cybersecurity education plans for high schools and universities. In the first annual update released in 2017 [12], there are plans for gap identification and collaboration on skills initiatives with international partners, such as New Zealand.

Caelli and Liu state that cybersecurity education is offered at both undergraduate and postgraduate levels by different Australian universities [14]. In particular, cybersecurity is offered as a major or minor, while other universities offer some courses in association with industry organizations in Australia. Their study provides a data repository that could be useful for prospective students and

others, but their analysis shows that the scope of current course work is limited.

Some universities in Australia offer cybersecurity study units instead of a complete degree program. Caelli and Liu [14] considered forty Australian institutions: 17.5% institutions offer full degree programs, 35% institutions offer cybersecurity as a major or minor, 27.5% institutions offer units, and 20% of them are not involved in any cybersecurity education. In terms of course content, they found the main focus to be on network security, with little to no focus on topics including trusted systems, secure application software development, and penetration testing. They highlight the need for a holistic approach in terms of content and suggest focus on national and global standardizations; national and global legal/regulatory requirements in cybersecurity and cyber response; healthcare systems; future trends and technologies including Internet of Things (IoT), cloud computing, network virtualization; trustworthy systems and their evaluation covering common criteria; and others.

Henry [26] views cybersecurity education as multidisciplinary, and identifies gaps in university offerings and presents an education framework for cybersecurity. These gaps were in the context of KSA (Knowledge, Skills, and Abilities), where knowledge refers to understanding of legal aspects of cybersecurity, while skills and abilities cover applying techniques used in cybersecurity exercises. Moreover, there is also a gap when it comes to developing attitude to deal with uncertain cybersecurity situations. He investigates generalist postgraduate degree programs in Australia and concludes that mission-specific and purpose-driven curriculum may better prepare students for addressing skills crisis than generalist degree programs. He concluded that "Many governments still try to initiate a single–non-multidisciplinary–curriculum to solve the cybersecurity and/or skills crisis, which will probably fall short, as discussed above. The multidisciplinary nature of cybersecurity requires multiple different streams. While this is a start for governments, more is required and a focus on the purpose for the cybersecurity education is critical to identify different public policy requirements, career paths and education levels required." Likewise, other research studies [59] also argue that cybersecurity education is an opportunity to address the cybersecurity skills gap properly.

New Zealand

To deal with cybersecurity threats, New Zealand has defined a cybersecurity strategy in 2011 [48]. One of the long-term initiatives of this cybersecurity strategy is to meet the need for cybersecurity professionals in New Zealand and to determine cybersecurity qualifications, training, research and development in collaboration with industry, universities, and other educational and training institutions. Fourie *et al.* [25] state that many tertiary institutions in New Zealand have realized the need for cybersecurity education since the 2011 cybersecurity strategy. Generally, cybersecurity education is in the form of a number of undergraduate and postgraduate courses with cybersecurity content.

According to New Zealand's cybersecurity strategy 2015 [49], one goal in the action plan is to build cybersecurity capabilities. Achieving this goal requires the education and training system for addressing cyber hygiene practices. To this end, several tertiary institutions have already incorporated cybersecurity into their courses and curriculum. One of the main action points to develop cybersecurity capability is the promotion of cybersecurity education by identifying gaps in cybersecurity training.

The first annual report on the implementation of the cybersecurity strategy's action plan [50] mentions that a cybersecurity skills task force has been established to address the shortage of cybersecurity skills. This task force has representatives from industry, academia, and education. One main outcome of this task force is expected to be improved understanding of cybersecurity training at different levels in education including primary, secondary, and tertiary. A proposal has been made for developing a diploma in cybersecurity of level 6, per New Zealand qualifications framework (NZQF) standards by 2017.

A draft diploma in cybersecurity [38] has been designed to produce graduates capable of applying cybersecurity skills, knowledge, and practice and to work per professional standards independently and in teams. This diploma requires 120 credits that include 90 credits for technical skills and 30 for core skills. The technical skills cover identification of assets and stakeholders (10 credits), analyzing technologies (15 credits), risk assessment (20 credits), determining controls (25 credits), incident handling (15 credits), analyzing legal, and privacy and ethical impacts (5 credits). The core skills include behaving responsibly (10 credits), communication and soft skills (10 credits), and project management (10 credits).

Several master's programs are offered in New Zealand. A master of professional studies in digital security program is offered by the University of Auckland [10]. Victoria University of Wellington also offers a master of computer science with an option to choose cybersecurity courses.

Summary

A substantial number of countries have already developed and published a cybersecurity strategy, after recent evidence related to cybersecurity incidents, the assumption of the high impact of those incidents and the evidence of a shortage of professionals in this (rapidly) emerging area.

In 2018, the Canadian National Cyber Security Strategy recognized the role of science, technology, engineering, and mathematics (STEM) and the need for Canadian graduates to to specialize in the skills needed to address the increasing demand for cyber security jobs [47]. The 2016 National Occupational Classification can be used to find a listing of a variety of cybersecurity related job positions, for example, informatics security analyst, informatics security consultant, internet security analyst, systems security analyst, systems security planner, intelligence analyst, intelligence officer and intelligence operator [32]. However, there is no developed cybersecurity education framework such as the US Centers for Academic Excellence [34] or the NIST NICE Framework [39].

At the EU level, developing such a strategy was mandated for all members, with all cybersecurity strategies looking generally similar in terms of cybersecurity education and training. However, there are differences in levels of detail and inked action plans, with some countries leading in initiatives for establishing different levels of cybersecurity courses.

3.3 Standards and Curricular Guidelines

This subsection explores some initiatives to set up standards and provide curricular guidance in two countries: the United Kingdom and the United States, as well as other attempts by professional computer societies and accreditation organizations.

United Kingdom

One governmental initiative worth mentioning is that of the UK government which has established the National Cybersecurity Centre (NCSC) that certifies bachelor and master degrees in cybersecurity and closely related fields, using IISP's skills framework Institute of Information Security Professionals [29]. At the bachelor level, the scheme [54] certifies degrees in:

- Computer science for cybersecurity. This category involves degrees that are addressing underpinning computer science relevant to cybersecurity.
- Computer science and cybersecurity. This category concerns degrees that provide a general, broad foundation in cybersecurity.
- Computer science and digital forensics. Degrees considered in this category provide a foundation in digital forensics.

For each degree pathway, there are indicative topics that one would expect to find within the syllabus of bachelor-level modules. For all degree pathways, there are common computer science subject areas that students should learn. These include:algorithms and complexity; architecture and organization; discrete structures; programming languages; software development fundamentals; software engineering; systems fundamentals; security fundamentals; networks; operating systems; human-computer interaction; information management; secure programming; low level techniques and tools; systems programming; embedded systems; social issues and professional practice.

For a computer science and cybersecurity degree, the program should cover the following areas: information security management; information risk management; implementing secure systems; information assurance methodologies and testing; operational security management; incident management; audit, assurance and review; business continuity management; information systems research; and professional skills.

The following subject areas are considered essential for a computer science and digital forensics degree. They include: foundations of digital forensics; digital Forensic analysis; digital Forensic practice; application of digital forensics; legal process; information security; and evidence handling and management.

Initiatives from industry associations provide other guidelines, promoting specific cybersecurity skill competencies. For example, the Tech Partnership is a network of UK employers that collaborate to identify the skills needed for the UK digital economy. One objective of the partnership is to improve the quality of digital skills training and education by setting apprenticeship standards and developing degree apprenticeship programs to meet employers' needs. To this end, the partnership has published standards related to information security [52] that indicate the competencies, knowledge and understanding that a person should have, depending on the years of experience (0-2, 3-5, 6-9, 10+). The standards fall under the following categories: information security governance; risk assessment and management; secure development and security architecture; security testing; secure operations management, vulnerability assessments, and identity and access management; intrusion detection, incident investigation and management, and digital forensics; audit, compliance and assurance; and business resilience.

Another initiative is taken by the assessment and qualification alliance (AQA) that provides academic and vocational qualifications taught in UK and international schools and colleges. In the context of cybersecurity, they have published advanced technical qualifications [9], built in collaboration with employers and professional bodies. The alliance specifies the following two qualifications. The *Foundation Technical Level IT: Cybersecurity* qualification is made up of four mandatory units. These include: fundamental principles of computing; communication technologies; developing and maintaining computer networks; and network threats and vulnerabilities.

The *Technical Level IT: Cybersecurity and Security Administration* qualification is made up of seven mandatory units and two optional units (one of which must be studied): fundamental principles of computing; communication technologies; developing and maintaining computer networks; network threats and vulnerabilities; mathematics for computing; network and cybersecurity administration; managing identity and access to systems; programming for networking and security (optional unit); and computer forensic investigation (optional unit)

United States

This subsection on the efforts in the United States is heavily adapted from a recent presentation made by two of the authors, along with Edward Sobiesk, Joseph J. Ekstrom, Andrew Hall and Shannon Gorman [44]. Within the USA, cybersecurity curriculum development and evolution has been influenced by several sources. First, ACM and the IEEE Computer Society published the Computing Curricula series with an overview volume called CC2005 [24] that references separate volumes for each of the recognized computing disciplines:

- IS2010 (Information Systems) [5]
- CS2013 (Computer Science) [6]
- SE2014 (Software Engineering) [43]
- CE2016 (Computer Engineering) [7]
- IT2017 (Information Technology) [8]

A sixth volume was recently published for cybersecurity called CSEC2017 [30], and the CC2005 [24] is currently in revision with the next version to be released as CC2020.

The National Security Agency (NSA) and Department of Homeland Security (DHS) support cybersecurity education in colleges and universities within the US via the National Centers of Academic Excellence in Cyber Defense (CAE-2Y for 2-year colleges, CAE-CDE for 4-year colleges, and CAE-R for research universities) designation. Depending on its type, each institution must successfully map its curriculum to the core Knowledge Units (KUs), optional KUs, and focus areas [34]. These designations ensure an appropriate cybersecurity curriculum is available within the institution. However, these programs do not require an institution to assess and evaluate formally the graduates that have achieved their degree's learning outcomes.

Complementing the CAE-CD effort are the national centers of academic excellence (CAE) for cyber-operations programs [35] in support of the presidential national initiative for cybersecurity education (NICE) [39] to increase the number of cybersecurity trained professionals. Unlike the CAE-CD effort, the CAE-cyber-operations designates a student as having completely satisfied all of the mandatory knowledge unit requirements and at least four of the optional knowledge units in terms of their transcript or degree. Only a small number of institutions have achieved the CAE-cyber-operations certification.

Accreditation and Curricular Guidelines

We now examine efforts in accrediting cybersecurity programs, based on curricular guidelines provided by various professional computing societies including the ACM and IEEE Computer Society.

ABET is a US-based international organization dedicated to disciplinary accreditation in computing, engineering, engineering technology and applied and natural sciences. ABET is organized around the concept of commissions, where each commission is responsible for accrediting programs with common themes. ABET has commissions for each of the aforementioned themes: computing accreditation commission (CAC), engineering accreditation commission (EAC), engineering technology accreditation commission (ETAC), and applied and natural science accreditation commission (ANSAC).

Each commission has a set of general criteria that are required to be met for all programs accredited by that commission, along with more specific program criteria that programs of various disciplines must meet. Recently the CAC general criteria were enhanced to include a significant cybersecurity curricular requirement for all computing programs. CAC currently accredits programs in computer science (CS), information systems (IS) and information technology (IT). That is, CAC has a set of general criteria for all programs and then a separate set of program criteria for each of CS, IS and IT. ABET cybersecurity program criteria [2] were recently published in draft form for execution within CAC as a fourth type of computing program, in addition to CS, IS and IT. Similar ABET activities have taken place under the EAC for cybersecurity engineering programs.

These efforts fall into two categories. The category 1 effort represents approaches that integrate cybersecurity content with existing computing-based disciplines, while the category 2 effort represents the creation of a stand-alone discipline for cybersecurity. The category 1 effort has been prevalent in US-based education for more than twenty years, while the category 2 effort is emerging as a new movement. These two approaches are detailed as follows.

Category 1: Integration with Existing Computing Programs. The ACM/IEEE-CS curriculum volumes have generally evolved to incorporate cybersecurity concepts within each of the latest versions that include the following:

- ***Computer Engineering (CE2016):*** CE2016 [7] defines the terms: knowledge area, knowledge unit, core learning outcomes, and elective learning outcomes. CE2016 then describes 12 recommended knowledge areas, with information security as one of them. In particular, CE2016 explicitly describes 20 hours of cybersecurity content, which is recommended for inclusion across the curriculum. Cybersecurity is also suggested as a potential area of emphasis, or a trade-off, when learning requisite design skills that need to occur throughout the entire CE curriculum) [7].
- ***Computer Science (CS2013):*** CS2013 [6] provides an overall taxonomy for the discipline consisting of knowledge areas (KAs), knowledge units (KUs), topics and learning outcomes (LOs). For security, CS2013 recommends 9 lesson hours of concepts where the depth is unique to information assurance and security and an additional 63.5 lesson hours of information assurance and security content that is "integrated into other knowledge areas that reflect naturally implied or specified topics with a strong role in security concepts and topics" [6]. These integrated CS cybersecurity curricular recommendations are mostly technical material that apply to the aspect of the curriculum being covered.
- ***Information Systems (IS2010):*** IS2010 [5] uses courses for its organization, with a BoK extracted into an appendix. There are seven core courses and seven sample elective courses enumerated. Topics and learning outcomes are listed in the course outlines. Although the IS BoK appendix does not explicitly mention security when listing recommended knowledge areas, security recommendations are included in six of the seven sample core courses, and security is the main theme for two of the sample elective courses. Note that IS2010 is the oldest of the current curriculum volumes, and is now almost ten years old.
- ***Information Technology (IT2017):*** IT2017 [8] includes a set of core information technology domains and supplemental information technology domains with subdomains. IT2017 recommends the cybersecurity content occupy approximately 10% of the IT curriculum, with most of the material covered throughout the curriculum instead of just in one course. In fact, due to the robustness of cybersecurity in information technology as presented in the IT2017 report, one can make the case that any IT degree program could be viewed as a cybersecurity program [20].
- ***Software Engineering (SE2014):*** SE2014 [43] provides a knowledge area, knowledge unit, topic hierarchy with topics tagged with the expected level of coverage (knowledge, comprehension, or application), which correspond to Bloom's cognitive domain taxonomy simplified to three levels. Security is one of SE2014's ten recommended knowledge areas, and SE2014 includes 20 hours of explicitly recommended security content. In a manner similar to CS2013, however, SE2014 clarifies that the "relatively small number of hours assigned to the software quality (QUA) and security (SEC) knowledge units reflects that these areas represent cross-cutting concerns that are closely linked to topics in other knowledge units. They have been identified separately to increase their visibility and to recognize their importance across the entire extent of the software engineering discipline" [43].

The above curricular reports demonstrate a general increase in cybersecurity content as the disciplines have evolved. ABET has supported this evolution by adding EAC program criteria for cybersecurity engineering programs and adding a CAC requirement

to the general criteria for all computing programs, which requires the inclusion of "principles and practices for secure computing" within the curriculum [1]. The revised criteria have not yet been deployed, and so they have not yet impacted the content of accredited computing programs in the large. Evaluating the effect of ABET's actions on cybersecurity education will be an important area for future examination and research.

Regarding the impact of the CAE program on the integration of cybersecurity content into existing programs, we note that of 162 NSA CAE institutions, only 36 offered degrees in 2016 classified as "information security" based on required reporting to the US Department of Education Integrated postsecondary education data system (IPEDS) [56]. This means that most of the effect of CAE has been on infusing non-information security programs with cybersecurity content.

Category 2: Standalone Cybersecurity Programs. As noted above, the five longstanding ACM/IEEE-CS curriculum volumes have supported the integration of cybersecurity concepts into existing computing disciplines. The integration approach has been complemented by ABET and NSA/DHS CAE. However, many recent efforts have also supported the development of standalone cybersecurity programs.

Notably, the recently published CSEC2017 [30] primarily lays a foundation for standalone cybersecurity programs. "The CSEC2017 curricular volume will be the leading resource of comprehensive cybersecurity curricular content for global academic institutions seeking to develop a broad range of cybersecurity offerings at the post-secondary level". The CSEC2017 report presents a "model" of cybersecurity that consists of three parts: knowledge areas, cross-cutting concepts and a set of disciplinary lenses [30].

Parrish et al. [44] discuss how the CSEC2017 disciplinary lens permits existing computing disciplines to absorb security content within the desired discipline [44]. A "mixed disciplinary" lens helps to capture cybersecurity in the context of a "computing + X" interdisciplinary combination, *e.g.*, cybersecurity in the context of bioinformatics. While CSEC2017 allows cybersecurity concepts to be contextualized, the vision of CSEC2017 permits cybersecurity to be a separate, standalone discipline with different "flavors" of degrees.

CSEC2017 has been reinforced by the introduction of ABET accreditation criteria for cybersecurity degree programs [1]. As of the time of this writing, there are now four cybersecurity programs that have been accredited under these criteria, with several other cybersecurity programs anticipated to apply for this accreditation.

Parrish et al. [44] also note that the number of US institutions offering cybersecurity degrees has shown a remarkable 100% increase in the total number over the five-year period from 2012 to 2016 [56]. The number of degrees has been slowly rising, with 13 new institutions beginning to offer cybersecurity degrees during this period. However, as both cybersecurity degrees and institutions are fairly low, substantial growth is needed in both degrees and institutions to meet workforce needs [44].

The standalone approach requires an identifiable "community" for institutions that have adopted the standalone program approach. While several of these institutions are part of the CAE community and most are part of the cybersecurity community writ large, there is still the need for greater collaboration and information sharing that is unique to the standalone program institutions. These institutions will share similar concerns regarding program approval, accreditation, hiring of cybersecurity faculty, developing an academic research community and generally establishing a disciplinary identity. The creation and use of open source data, similar to that used in the Taulbee survey for computing [60], will enable cybersecurity programs to calibrate their resources to accommodate the marketplace and assess strengths, weaknesses, opportunities and threats. The need for a cybersecurity professional community and underlying academic discipline was also recently identified [51].

4 FUTURE CYBERSECURITY DYNAMICS

This section presents three significant aspects related to the future dynamics of cybersecurity. One addresses proposed framework for cybersecurity education. The second addresses the meaning of a competency-based approach in education. The third outlines how minimal competencies in cybersecurity can be described for the 2030s.

4.1 A Framework for Cybersecurity Education

As a framework to discuss cybersecurity education, we propose two overall approaches. The first approach is to augment traditional computing programs with cybersecurity content. This "integration method" is supported by, and in many cases the result of, the addition of significant cybersecurity content into all five of the longstanding ACM/IEEE-CS detailed curriculum volumes that contain recommendations for computer engineering, computer science, information systems, information technology, and software engineering. Alternatively, institutions are also developing brand new standalone cybersecurity programs. This latter approach attacks the workforce development gap directly by educating graduates who are credentialed as cybersecurity professionals. This "standalone method" is being energized by the recent publication of the ACM/IEEE-CS detailed curriculum volume for cybersecurity called CSEC2017 [30]. It is useful to consider several questions in the context of this framework:

(1) Are we seeing the integration method result in new degree programs or are we simply seeing changes in existing programs?
(2) Does the standalone method result in (fundamentally) one new type of degree program or several?
(3) Is cybersecurity a subset of computing or is it orthogonal to it?
(4) Is it possible to identify the participants in the cybersecurity educational community?
(5) Is it more useful to think of cybersecurity as degree program(s), discipline(s) or both?

We first consider why these questions are important and some fundamentals that are raised by the questions.

Question 1: Integration = New Degree Programs? When security concepts are integrated with CS, IS, IT, SE and CE, are the degree programs that result fundamentally a new thing? We note that there are three different things possibly happening. First, disciplinary curriculum models are increasingly integrating more security concepts

with the fundamentals in each of the disciplines. Each of the recent curriculum models (CS2013, IT2017, SE2014 and CE2016) added security to the curriculum content [4]. ABET recently followed suit by now requiring security as a fundamental concept that must be taught in any computing program [1]. So it can definitely be argued that newer versions of each of the computing disciplines will require more security content than in the past.

It can also be argued that many existing degree programs in CS, IS, IT, SE and CE are adding variants and concentrations that are security specific. This is frequently accomplished by within existing programs' flexibility to specify a set of security courses as a track or a concentration. Such approaches have been common in most fields and do not represent anything particularly new and fundamentally different—except that the number of such concentrations is believed to be increasing.

Third, there are new degree programs being created in security that are clearly descended from individual programs in CS, IS, IT, SE or CE. These new programs are perhaps called "cybersecurity" or perhaps other names that more directly reflect specializations of existing degree programs ("secure software systems" or "network security") but are hyper-specializations of existing programs. These are distinguished from tracks or specializations within existing programs by the amount of cybersecurity content and the degree to which content from the original ancestor program is retained. This type of program is indeed something "new and different" and there are challenges with creating such programs. To wit, is it possible to develop cybersecurity content without "base" content from the ancestor discipline? The more cybersecurity content that is included, the less content is possible from the base discipline. How can the new thing be covered without fully covering the old? In most cases, the cybersecurity content requires a depth of understanding within the cognate discipline.

Question 2: Standalone = One degree or several? Several varieties of standalone degrees can be conceptualized, all of which could be called cybersecurity. Obviously, degrees may be specializations of any of the existing computing degree programs, as noted above. Standalone degrees may also be more crosscutting. For example, the US Naval Academy has a degree program called "cyber operations" – which is based on the principles of offensive and defensive cyber operations. This degree program integrates concepts from computer science, computer engineering, systems engineering and political science.

As stated earlier, cybersecurity degree programs can be and have been blended from concepts across a wide spectrum of disciplines. The emphasis area, e.g., networking or cyber criminology, can lead to substantially different degree programs, all named with a "cybersecurity" title or other similarly generic name, but representing "small-cybersecurity." The broader notion of "big-cybersecurity" is the meta-discipline, as shown in Figure 1.

Question 3: Subset of Computing? While certain notions of cybersecurity could be argued to be computing disciplines, big-cybersecurity appears to include content and disciplinary components that go beyond computing. CSEC2017 [30], which defines curriculum content for big-cybersecurity, includes a substantial amount of social science content. Some specific cybersecurity disciplines could be viewed as computing disciplines, but others are clearly not computing (*e.g.*, cyber criminology).

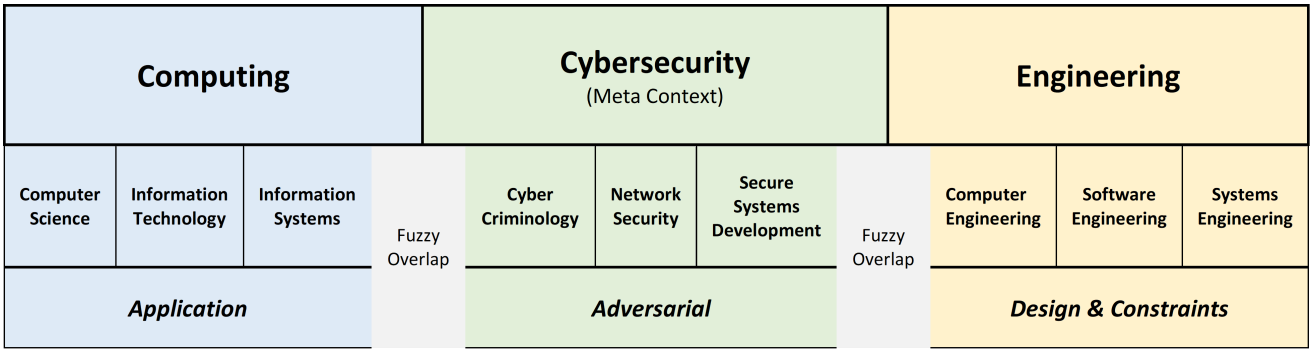
This notion of big-cybersecurity may become confusing when ABET defines *computing* or *engineering* accreditation criteria for cybersecurity, which effectively define requirements for a curriculum or degree program in cybersecurity - as if cybersecurity were a specific computing discipline. This does not reflect the broad notion of big-cybersecurity that is defined in CSEC2017, but it is rather a much more restricted notion of cybersecurity that is simply one variant within a broad spectrum of variants (that also happens to be a computing discipline as well).

Figure 2 shows the broad notion of big-cybersecurity alongside the more restricted version of small-cybersecurity that could be a subset of both big-cybersecurity and computing or big-cybersecurity and engineering. While there may be a significant number of computing-oriented or engineering-oriented cybersecurity programs, it is not the same as the big-cybersecurity that is reflected by CSEC2017 or by many discussions within the educational community. The authors suggest that the community use cybersecurity to mean big-cybersecurity and other words be used for small-cybersecurity notions and for other variants.

Question 4: Cybersecurity Educational Community? For cybersecurity to grow as an entity, it needs to be possible to identify the community of educational practitioners. This appears to be a difficult problem because "cybersecurity" is an amorphous term to begin with. However, an inclusive approach would suggest that the scope of the community goes beyond simply the computing community. In particular, IEEE-CS and ACM do not have SIGs that capture this community. To really obtain maximum intellectual synergy from this community, there needs to be a professional society. There also needs to be a formal identification process for community stakeholders, and open source data captured to reflect potential stakeholders within the community.

Question 5: Degree Programs, Disciplines or Both? We claim that it is time to look at cybersecurity as a meta-discipline with a BoK, educational programs, a supply of PhD graduates to become faculty members, and a community of educational practice. This will enable a more fundamentals-driven approach to designing curricula, and a more long-lasting, durable base of knowledge and competencies. The risk of this approach is that the field could "go out of business" if there are technical solutions that emerge that defeat the adversary and generally eliminate insecurity of systems. Should that time come, it may be that there is no longer a need for degree programs or bodies of knowledge (or any of the other trappings of a community). As such a future is by no means certain and given the intervening international crisis in the area coupled with the lack of human resources, we believe that the risk of taking a disciplinary approach is outweighed by the downside risk of not taking such an approach.

These questions require addressing in the context of current educational efforts in different parts of the world. By framing this discussion of worldwide efforts in terms of these questions, educators can assess how current efforts may affect these questions over the next ten years. The current efforts seem to point toward an



)

Figure 2: Breadth of Cybersecurity

emerging cybersecurity meta-discipline – or field of study – that encompasses technology, engineering, computing, and social science components. This would result in a variety of different types of degree programs framed within existing disciplines or within new disciplines. The next subsection contains information surrounding the competency model that is useful to frame the cybersecurity meta-discipline just discussed.

4.2 Cybersecurity Competencies for 2030

It is a challenge to determine what cybersecurity might be in the future. Recent documents such as the one produced by the IISP [29], the CSEC2017 report [30], and other related publications focus on current cybersecurity efforts. They serve as useful references for the current situation. For example, the CSEC2017 report identifies eight areas of cybersecurity that include data, software, component, connection, system, human, organizational, and societal areas. The 2018 IISP report illustrates ten active security skills as already shown in Table 2.

The narrative that follows addresses the vision of the authors on the future of cybersecurity, particularly as it might appear in 2030. The approach taken is that cybersecurity should be a component of all bachelor degree programs, including programs beyond computing. This multidisciplinary approach underscores the importance of basic cybersecurity exposure whether it occurs in engineering, science, business, or philosophy. An educated global community should have a minimal exposure to cybersecurity. The only difference is the level of that exposure.

Competency and its Meaning

In modern literature, we have witnessed an influx of the word "competency" used in a variety of contexts. Unfortunately, in some/many cases people use it loosely as a current "buzz word" without pertinent meaning. However, some groups have formed concrete meanings for competency. For example, the Software Engineering Competency Model (2014) [27] states that competency is:

> The demonstrated ability to perform work activities at a stated competency level, which is one of five increasing levels of ability to perform an activity denoted as technician, entry-level practitioner, practitioner, technical leader, or senior software engineer.

In essence, this definition suggests that competency is some combination of knowledge, skill, and ability. The MSIS2016 document [53] states:

> Competencies represent a dynamic combination of cognitive and meta-cognitive skills, demonstration of knowledge and understanding, interpersonal, intellectual and practical skills, and ethical values.

The IT2017 report has formulated a constructive and canonical definition of competency based on pedagogical theory and use in multiple professions of practice such as medicine. Contrasting competency with learning outcomes, the IT2017 report states that:

> Learning outcomes are written statements of what a learner is expected to know and be able to demonstrate at the end of a learning unit (or cohesive set of units, course module, entire course, or full program) [8].

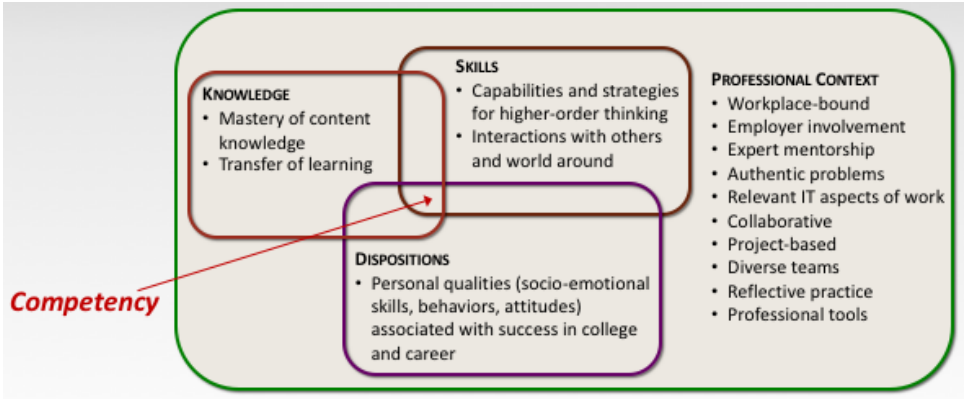
The report also states:

> Competence refers to the performance standards associated with a profession or membership to a licensing organization. Assessing some level of performance in the workplace is often used as a competence measure, which means measuring aspects of the job at which a person is competent [8].

Thus, the essential difference between a competency and a learning outcome is that the focus of competency is on performance in professional context [8], namely that:

Competency = Knowledge + Technical Skill + Human Disposition

Knowledge is simply not sufficient to become a successful practicing professional in cybersecurity. In industry, for example, technical skill and human disposition are often more important than just knowledge. Figure 3 illustrates this understanding in an information technology context, where the intersection of the triple–knowledge, skills, and disposition–describes the intended competency.



)

Figure 3: Illustration of competency for information technology

Table 3: Domains of "cybersecurity"

Tag	Domain	Components
A	Governance	Policy, Strategy, Compliance, Standardization
B	Risk Management	Threat modeling, Asset evaluation, Mitigation, Vulnerabilities
C	Constraints	Legal (including regulatory), Ethical, Organizational, Political, Privacy
D	Controls	Administrative, Physical, Technical

4.3 Cybersecurity Competency Domains

By most accounts, the three essential pillars of security are confidentiality, integrity, and availability (CIA). All security methods, approaches, or systems must possess these attributes, whether a brick-and-mortar structure or a computer network. One would not trust any security system that lacks any one of these principles. Naturally, all bachelor programs in the cybersecurity meta-discipline must include a study of these pillars.

For the field of cybersecurity and its related academic programs, the authors have generated four domains that are endogenous to the field. That is, any cybersecurity program (*e.g.*, cyber criminology, network security, secure software development) must have competencies related to these four domains, which are governance, risk management, constraints, and controls. Table 3 identifies the four domains and their related components.

Table 4: Action Verb Suggestions

Level	Action Verbs <A-verb>
1	Define, Describe, Draw, Identify, Label, List, Locate, Memorize, Name, Recite, Recognize, Select, State, Write
2	Change, Confirm, Explain, Express, Illustrate, Incorporate, Match, Monitor, Paraphrase, Present, Provide, Restate, Transform
3	Apply, Assist, Change, Choose, Classify, Collect, Conduct, Contribute, Convey, Develop, Discover, Draft, Dramatize, Draw, Interpret, Maintain, Make, Model, Modify, Paint, Perform, Prepare, Present, Produce, Report, Show, Undertake, Use, Write
4	Analyze, Apply, Categorize, Classify, Compare, Construct, Contrast, Contribute, Control, Deliver, Design, Differentiate, Distinguish, Examine, Implement, Infer, Incorporate, Investigate, Operate, Oversee, Point-out, Research, Select, Separate, Share, Subdivide, Supervise, Support, Survey, Take-apart, Use
5	Analyze, Append, Assess, Combine, Communicate, Construct, Create, Develop, Design, Encourage, Formulate, Hypothesize, Invent, Lead, Manage, Organize, Originate, Plan, Produce, Role-Play, What-if
6	Advise, Apprise, Assess, Audit, Authorize, Compare, Coordinate, Criticize, Critique, Decide, Develop, Direct, Evaluate, Influence, Judge, Persuade, Recommend, Relate, Solve, Summarize, Weigh

Action Verbs

The IISP report suggests six levels of skills useful for the assessment of practitioner performance. Table 1 had provided a summary of the meaning of these levels. Table 4 presents some suggestions for action verbs taken from the 2018 IISP report and other sources. The action verbs listed in this table have similarities to the well-known Bloom's Taxonomy [13]. Each IISP level seems to focus on the cybersecurity expertise associated with that level, not whether the different IISP levels can be ranked in terms of learning.

The listing represents only suggestions for verb use and does not portray an exhaustive collection of *action verbs* suitable for cybersecurity competencies. One must take the action verbs in context. For example, to develop a program to do a search for a name in a database is quite different than to develop a program

for a flight control system. In the first case, it is a level 1 or level 2 activity; in the second case, it would be a level 5 or level 6 activity.

In reality, a recent graduate from a bachelor program in cybersecurity would not have the capacity or the ability to engage in activities at level 5 or level 6. These graduates are just starting their professional careers and their typical ages are likely to be the early twenties. Thus, for this purpose, we would only consider levels 1 through 4 from the IISP scale.

Building Competencies

It is possible now to build competencies for all cybersecurity disciplines by using the elements from Tables 3 and 4 according to the string concatenation algorithm:

<A-verb> <D-phrase>

where <A-verb> is an action verb used at an indicated level as in Table 4 and where <D-phrase> is a domain phrase assembled from the components in Table 3. The choice of the action verb associated with the domain phrase depends on the level of the expected competence.

Example 1.
A competency of a recent graduate from a bachelor program in business administration working for a government agency could be:
Explain the content of a security policy of a contract with a vendor.
Here, <A-verb> = "Explain" derives from level 1 and <Dphrase> derives from Tag A.

Example 2.
A competency of a recent graduate from a bachelor program in computer engineering working for a security company could be:
Develop a program to mitigate vulnerabilities on a computer system.
In this case, <A-verb> = "Develop" derives from level 3 and <Dphrase> derives from Tag B.

Example 3.
A competency of a recent graduate from a bachelor program in cybersecurity working for a security technology company could be:
Design a control interface for a computer system.
Here, <A-verb> = "Design" derives from level 4 and <Dphrase> derives from Tag D.

Cybersecurity Models

It is now possible to develop models for cybersecurity. Recall that the four domains tagged A, B, C, and D represent minimal, generic parts of full bachelor programs that contain one or more cybersecurity components. For example, a university may have a general education specification whereby all students must take a module or course typically titled "Introduction to Cybersecurity" as a graduation requirement. Thus, students specializing in mathematics, philosophy, engineering, art, computing, or journalism must have some exposure to cybersecurity. In this case, all students regardless of their specialty will all have some level of exposure to the four domains (A,B,C,D) at least at level 1. We would expect a philosophy specialist to cover these areas at level 1 or occasionally at level 2. On the other hand, we would expect students enrolled in a cybersecurity degree program to have expertise in the four domains at level 3 or level 4.

It is now possible to generate models of minimal competencies in cybersecurity for any bachelor program. We do this by combining (1) the full set of domains with their related components, and (2) the associated levels relative to the specialty or curriculum. The following models illustrate how to do this.

We begin by creating competencies for a given bachelor program following the process already specified. That is, for each component of each domain, produce a competency at the expected level for the program. For the four domain areas, there are a total of sixteen components. Therefore, there will be sixteen minimal competencies for any given program.

To illustrate this model, we then form a table listing the four domains with their components in the first column and the levels in the next four columns. As already mentioned, it is not necessary to list all six levels from the 2018 IISP report because recent graduates from bachelor programs would not have the capacity to engage at the fifth and sixth levels. The resulting matrix acts as a snapshot of the minimal competency model. Table entries reflect the fact that a recent graduate with competency at level N has obviously achieved a competency at level N-1 for N = 2, 3, or 4.

Category 1: Information Technology Program with a Cybersecurity Track.
We begin by constructing competencies for this program according to the string concatenation algorithm already discussed. Since students in this program are information technology specialists (not cybersecurity specialists), we would not expect high levels of expertise. The sixteen competencies appear in Table 5.

We now construct a table graph according to the process mentioned. A typical "snapshot" for such a program is as shown in Table 6. The table illustrates the expected levels of competency for each of the sixteen domains. Note that the ... denote the actual constructed values.

Category 2: Cybersecurity Bachelor Program.
As before, we begin by constructing competencies for this program according to the string concatenation process already discussed. Since students in this program are cybersecurity specialists, we would expect relatively high levels of expertise. The sixteen competencies appear in Table 7.

We now construct a table graph according to the process mentioned. A typical "snapshot" for such a program is as shown in Table 8. The table illustrates the expected levels of competency for each of the sixteen domains. Again, note that the ... denote the actual constructed values.

Competencies for the 2030s

We can use the concatenation algorithm coupled with the examples and models to construct cybersecurity competencies for the future. That is, the algorithmic process developed is a "living process" that provides a framework for dynamically developing competencies in cybersecurity that may vary over time.

The authors believe that the cybersecurity competencies stated herein found in the Models 1 and 2 competency tables provide two such cybersecurity cases. Obviously, there are many possibilities

Table 5: Competencies for Model 1

Domain	Competency Example
GOVERNANCE	
Policy	Write a summary of an organizational information security policy for a supervisor.
Strategy	Recognize strategic plans of a corporate division.
Compliance	Describe the compliance requirements of an organization.
Standardization	Paraphrase and explain security standards to a group of peers.
RISK MANAGEMENT	
Threat modeling	Explain the security threats that may compromise corporate assets.
Asset evaluation	Illustrate to a team the asset value characterization of a corporate unit considering its use.
Mitigation	Describe security countermeasures to mitigate identified risks to a government unit.
Vulnerability	State an asset's vulnerabilities in a presentation.
CONSTRAINTS	
Legal	Describe applicable laws, statutes, and regulatory documents to a set of peers.
Ethical	List existing ethical codes of conduct for a company.
Organizational	Restate baseline system security requirements in accordance with applicable security policy
Privacy	Incorporate privacy laws or regulations in main system requirements
Political	Describe to a corporate unit the different sensibilities of all stakeholders concerning system specification and design.
CONTROLS	
Administrative	Monitor and maintain server configuration by providing incident response and business continuity for a local institution.
Physical	Describe physical risks associated with critical assets in a security report.
Technical	Provide adequate access controls based on principles of least privilege and need-to-know for a local company.

Table 6: Snapshot of Model 1

Domain	L1	L2	L3	L4
GOVERNANCE				
Policy	…			
Strategy	…			
Compliance	…			
Standardization	…	…		
RISK MANAGEMENT				
Threat modeling	…	…		
Asset evaluation	…	…		
Mitigation	…			
Vulnerability	…	…		
CONSTRAINTS				
Legal	…			
Ethical	…			
Organizational	…	…		
Privacy	…	…		
Political	…			
CONTROLS				
Administrative	…	…		
Physical	…			
Technical	…	…		

based on the curriculum at hand and the four levels of action verbs. As before, for degree programs that may require a general education requirement in cybersecurity, the sixteen components of the four domains, competencies would likely be mostly at level 1. Basically, there are sixty-four (16 components * 4 levels) possible competency models derivable from the process mentioned with an infinite number of competency statements. The competencies provided for Models 1 and 2 are the authors' initial attempt to provide guidance to this important area.

5 CONCLUSIONS

This report has focused on defining a vision for a discipline of cybersecurity that consists of fundamental, enduring content. Our prediction is that many different types of programs will emerge over the next ten years - to the point that it is not possible to define cybersecurity as a single discipline, but as a family of disciplines. As such, we have coined the term big-cybersecurity to denote the family of disciplines such as the study of digital, technology-based systems in the face of an adversary.

This paper has reviewed the history of the overall cybersecurity area and how it has evolved from viewing computer security as an augmentation of existing disciplines, to a fairly broad spectrum of independent disciplines that constitute the cybersecurity as a meta-discipline. The authors have provided an overall meta-disciplinary framework for cybersecurity and have characterized cybersecurity in terms of an abstract set of competencies.

This paper represents the beginning of a meta-disciplinary view of cybersecurity driven by the need to provide guidance to higher education when implementing cybersecurity programs. The overall educational ecosystem must scale-up to meet extraordinary workforce demands and international crises associated with the

Table 7: Competencies for Model 2

Domain	Competency Example
GOVERNANCE	
Policy	Develop policy, programs, and guidelines for implementation within an enterprise.
Strategy	Describe strategic plans for security defense for a government agency.
Compliance	Design the security compliance processes and audit controls for an external services organization.
Standardization	Prepare an impact (costs and benefits) report of recent changes made to standards and procedures of an organization.
RISK MANAGEMENT	
Threat modeling	Implement a threat and target analysis of a computer network defense (CND) information and production of threat information within an enterprise.
Asset evaluation	Track and classify the status of protected information assets within a company.
Mitigation	Perform an information security risk assessment and write a plan for security countermeasures to mitigate identified risks within a corporation.
Vulnerability	Perform vulnerability assessments of relevant technology focus areas for a government agency.
CONSTRAINTS	
Legal	Transform applicable laws, statutes, and regulatory documents into one integrated policy for a government agency.
Ethical	Modify existing ethical codes of conduct for a company.
Organizational	Explain an enterprise system security context, a preliminary system security concept of operations, and present baseline system security requirements in accordance with applicable security requirements.
Privacy	Incorporate privacy requirements in organization's security policy.
Political	Describe to a group of peers the different sensibilities of all stakeholders concerning an organization's security policy.
CONTROLS	
Administrative	Design and document a systems administration security operating procedure for a small organization.
Physical	Classify security requirements specific to a security environment for an organization to maintain a critical systems lifecycle.
Technical	Oversee and make recommendations regarding configuration management of a governmental unit.

Table 8: Snapshot of Model 2

Domain	L1	L2	L3	L4
GOVERNANCE				
Policy	…	…	…	
Strategy	…			
Compliance	…	…	…	
Standardization	…	…	…	
RISK MANAGEMENT				
Threat modeling	…	…	…	…
Asset evaluation	…	…	…	
Mitigation	…	…	…	
Vulnerability	…	…	…	
CONSTRAINTS				
Legal	…	…		
Ethical	…	…	…	
Organizational	…	…		
Privacy	…	…		
Political	…			
CONTROLS				
Administrative	…	…	…	…
Physical	…	…	…	…
Technical	…	…	…	…

fragility of global information technology infrastructure. Cybersecurity must be part of a mainstream in higher education and not relegated to the corner of boutique programs. The cost to society of not having the capacity to meet emerging cybersecurity challenges is simply too high.

A WORKING GROUP PARTICIPANTS

Allen Parrish (leader) is Associate Vice President for Research and Professor of Computer Science and Engineering at Mississippi State University, USA. He was previously Professor and Chair of Cyber Science at The United States Naval Academy, and faculty at The University of Alabama in various roles, including Founding Director of the Center for Advanced Public Safety. Active in computer science and cybersecurity education, Dr. Parrish coauthored the CSEC 2017 report [30] and has held several volunteer and leadership roles in computing accreditation with CSAB and ABET.

John Impagliazzo (co-leader) is Professor Emeritus at Hofstra University, USA, and is a steering committee member of CC2020. He chaired the committee that produced the 2016 computer engineering curricular report (CE2016). Dr. Impagliazzo was a principal co-author of the CE2004 report, an active member of the CC2005 project, and a member of the executive committee for information

technology (IT2017). He is an IEEE Fellow, an IEEE Life Member, an ACM Distinguished Educator, and a CSAB Fellow.

Rajendra K. Raj (co-leader) is Professor of Computer Science at the Rochester Institute of Technology, USA. Interested in cybersecurity education, he helped launch RIT's MS in computer security in 2004, and found its Computing Security department in 2012. Dr. Raj co-led the recent effort to revise ABET's accreditation criteria for computing programs and create the new cybersecurity criteria. He was previously a software project manager and vice president in information technology at Morgan Stanley & Co.

Henrique M. D. Santos (co-leader) is Associate Professor of Information Systems at the University of Minho, Portugal, and conducts research in and lectures on information security and computer architecture at the ALGORITMI Research Centre. He is president of a national technical committee for information system security standardization, president of the Portuguese Association for Data Protection and vice president for IEEE Education Society conferences and workshops. Dr. Santos advises civil, governmental and military organizations about information security.

Muhammad Rizwan Asghar (member) is Senior Lecturer in the Department of Computer Science at The University of Auckland, New Zealand, where he received the Dean's Award for Teaching Excellence in 2018. His research in cybersecurity education includes the investigation of novel ways of teaching and learning cybersecurity. He received his PhD and MSc in Information Security Technology from the University of Trento, Italy in 2013 and TU/e, The Netherlands in 2009, respectively.

Audun Jøsang (member) is Professor in cybersecurity at the University of Oslo. With an MS in Information Security from Royal Holloway College, University of London, and a PhD from NTNU in Norway, Dr. Jøsang previously was Associate Professor at QUT in Australia, a telecommunications engineer for Alcatel in Belgium and Telenor in Norway. His research covers cybersecurity threat intelligence, trusted computing, identity and access management, and reasoning under uncertainty. Dr. Jøsang has been the Norwegian national representative to IFIP TC-11.

Teresa Pereira (member) is Adjunct Professor at Instituto Politécnico de Viana do Castelo, Portugal for ICT and information security. Her research at the ALGORITMI Research Centre focuses on Information Security, Cybersecurity and Cyberdefense Education. She is also member of the IS joint task group of CC2020 project and of the Multinational Cyber Defence Education and Training Project (MN CD E&T) NATO Smart Defence Project.

Eliana Stavrou (member) is Lecturer in the Computing Department at UCLan Cyprus and Course Leader for MSc Cybersecurity. She has a strong interest in cybersecurity education and capabilities development. Dr. Stavrou leads and delivers specialized cybersecurity training workshops to diverse audiences, e.g., policy makers, IT personnel, and young people. She is also Oxford Martin Associate at the Global Cyber Security Capacity Centre, UK, and a member of several committees organizing Penetration Testing Competitions.

ACKNOWLEDGMENTS

This work builds on prior efforts in computing and cybersecurity education including CSEC2017. The team acknowledges support provided by the US National Science Foundation under Award No. DGE-1433736; and COMPETE: POCI-01-0145-FEDER-007043 and FCT–Fundacao para a Ciencia e Tecnologia within the Project Scope: UID/CEC/00319/2013 and research grant FCT SFRH/BD/84939/2012. Vítor J. Sá at the Universidade Católica Portuguesa also contributed to early discussions. The team also acknowledges the support of ACM.

Parrish and Raj acknowledge Edward Sobiesk, Joseph J. Ekstrom, Jean R.S. Blair, David Gibson, Harry Reif, Steven Lingafelt and many others for innumerable discussions on cybersecurity education. In particular, they have co-authored multiple publications with Sobiesk and Ekstrom, whose ideas and words have helped to shape some sections of this paper.

REFERENCES

[1] ABET, Inc. 2017. Criteria for Accrediting Computing Programs, Effective for Review During the 2019-20 Accreditation Cycle. http://www.abet.org/wp-content/uploads/2017/12/C001-18-19-CAC-Criteria-Version-2.0-11-29-17-FINAL.pdf, Accessed November 06, 2018.

[2] ABET, Inc. 2017. Proposed Accreditation Criteria for Cybersecurity Academic Programs. http://www.abet.org/wp-content/uploads/2018/02/C001-18-19-CAC-Criteria-Version-2.0-updated-02-12-18.pdf, Accessed November 06, 2018.

[3] ABET, Inc. 2018. ABET Web site. urlhttp://abet.org, Accessed November 06, 2018.

[4] ACM. 2018. ACM Education Curriculum Recommendations. http://www.acm.org/education/curricula-recommendations, Accessed 29 June, 2018.

[5] ACM/AIS Task Group on Information Systems Curricula. 2010. *Information Systems 2010.* Technical Report. ACM Press. https://www.acm.org/binaries/content/assets/education/curricula-recommendations/cc2005-march06final.pdf, Accessed November 06, 2018.

[6] ACM/IEEE-CS Joint Task Force on Computing Curricula. 2013. *Computer Science Curricula 2013.* Technical Report. ACM Press and IEEE Computer Society Press. https://doi.org/10.1145/2534860 Accessed Novemner 06, 2018.

[7] ACM/IEEE-CS Task Group on Computer Engineering Curricula. 2016. *Computer Engineering Curricula 2016.* Technical Report. ACM Press and IEEE Computer Society Press. https://doi.org/10.1145/3025098 https://dx.doi.org/10.1145/30325098, Accessed November 06, 2018.

[8] ACM/IEEE-CS Task Group on Information Technology Curricula. 2017. *Information Technology Curricula 2017.* Technical Report. ACM Press and IEEE Computer Society Press. https://doi.org/10.1145/3173161 https://dl.acm.org/citation.cfm?id=3173161, Accessed November 06, 2018.

[9] AQA. 2016. Tech-level IT: Cyber Security. http://www.aqa.org.uk/subjects/computer-science-and-it/tech-level/it-cyber-security-2016, Accessed November 06, 2018.

[10] Muhammad Rizwan Asghar and Andrew Luxton-Reilly. 2018. Teaching Cyber Security Using Competitive Software Obfuscation and Reverse Engineering Activities. In *Proceedings of the 49th ACM Technical Symposium on Computer Science Education.* ACM, 179–184.

[11] Australian Government. 2016. Australia's Cyber Security Strategy: Enabling innovation, growth & prosperity. https://cybersecuritystrategy.pmc.gov.au/assets/img/PMC-Cyber-Strategy.pdf Accessed: June 14, 2018.

[12] Australian Government. 2017. Australia's Cyber Security Strategy: Enabling innovation, growth & prosperity, First Annual Update 2017. https://cybersecuritystrategy.pmc.gov.au/cyber-security-strategy-first-annual-update-2017.pdf Accessed: June 14, 2018.

[13] Benjamin S Bloom et al. 1956. Taxonomy of educational objectives. Vol. 1: Cognitive domain. *New York: McKay* (1956), 20–24.

[14] William J Caelli and Vicky Liu. 2018. Cybersecurity education at formal university level: An Australian perspective. In *Journal for the Colloquium for Information Systems Security Education*, Vol. 5. CISSE, 26–44.

[15] Lillian Cassel, Alan Clements, Gordon Davies, Mark Guzdial, Renée McCauley, Andrew McGettrick, Bob Sloan, Larry Snyder, Paul Tymann, and Bruce W. Weide. 2008. *Computer Science Curriculum 2008: An Interim Revision of CS 2001.* Technical Report. New York, NY, USA.

[16] Stephen Cooper, Christine Nickell, Lance C. Pérez, Brenda Oldfield, Joel Brynielsson, Asim Gencer Gökce, Elizabeth K. Hawthorne, Karl J. Klee, Andrea Lawrence, and Susanne Wetzel. 2010. Towards Information Assurance (IA) Curricular Guidelines. In *Proceedings of the 2010 ITiCSE Working Group Reports (ITiCSE-WGR '10).* ACM, New York, NY, USA, 49–64. https://doi.org/10.1145/1971681.1971686

[17] Stephen Cooper, Christine Nickell, Victor Piotrowski, Brenda Oldfield, Ali Abdallah, Matt Bishop, Bill Caelli, Melissa Dark, E. K. Hawthorne, Lance Hoffman,

Lance C. Pérez, Charles Pfleeger, Richard Raines, Corey Schou, and Joel Brynielsson. 2010. An Exploration of the Current State of Information Assurance Education. *SIGCSE Bull.* 41, 4 (Jan. 2010), 109–125. https://doi.org/10.1145/1709424.1709457

[18] Jessica Dawson and Robert Thomson. 2018. The Future Cybersecurity Workforce: Going Beyond Technical Skills for Successful Cyber Performance. *Frontiers in Psychology* 9 (2018), 744. https://doi.org/10.3389/fpsyg.2018.00744

[19] Jan den Berg, Jacqueline Van Zoggel, Mireille Snels, Mark Van Leeuwen, Sergei Boeke, Leo van de Koppen, Jan der Lubbe, Bibi den Berg, and Tony De Bos. 2014. On (the Emergence of) Cyber Security Science and its Challenges for Cyber Security Education. In *The NATO IST-122 Cyber Security Science and Engineering Symposium*.

[20] Joseph J. Ekstrom, Barry M. Lunt, Allen Parrish, Rajendra K. Raj, and Edward Sobiesk. 2017. Information Technology As a Cyber Science. In *Proceedings of the 18th Annual Conference on Information Technology Education (SIGITE '17)*. ACM, New York, NY, USA, 33–37. https://doi.org/10.1145/3125659.3125697

[21] ENISA. 2016. NCSS Good Practice Guide. https://www.enisa.europa.eu/publications/ncss-good-practice-guide, Accessed November 06, 2018.

[22] ENISA. 2018. National Cyber Security Strategies. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/

[23] Louis Fein. 1959. The Role of the University in computers, data processing and related fields.

[24] Joint Task Force for Computing Curricula 2005. 2005. *Computing Curricula 2005: The Overview Report.* Technical Report. ACM Press and IEEE Computer Society Press. https://www.acm.org/binaries/content/assets/education/curricula-recommendations/cc2005-march06final.pdf, Accessed November 06, 2018.

[25] Leon Fourie, Shaoning Pang, Tamsin Kingston, Hinne Hettema, Paul Watters, and Hossein Sarrafzadeh. 2014. The global cyber security workforce: an ongoing human capital crisis. (2014).

[26] Adam P Henry. 2017. Mastering the cyber security skills crisis: realigning educational outcomes to industry requirements. (2017).

[27] IEEE Computer Society. 2014. *Software Engineering Competency Model.* IEEE Press. Paperback ISBN-10: 0-7695-5373-7.

[28] Luukas K Ilves, Timothy J Evans, Frank J Cilluffo, and Alec A Nadeau. 2016. European Union and NATO global cybersecurity challenges: a way forward. *Prism: a Journal of the Center for Complex Operations* 6, 2 (2016), 126.

[29] Institute of Information Security Professionals. 2018. IISP Skills Framework. https://www.iisp.org/iisp/About_Us/Our_Frameworks/Our_Skills_Framework/iispv2/Accreditation/Our_Skills_Framework.aspx?hkey=e77a6f03-9498-423e-aa7b-585381290ec4, Accessed November 06, 2018.

[30] Joint Task Force on Cybersecurity Education. 2018. Cybersecurity Curricula 2017, Version 1.0. ACM, IEEE Computer Society, AIS SIGSEC, and IFIPS WG 11.8. , Accessed November 06, 2018.

[31] Allard Kernkamp and Josine van de Ven. 2017. MNCDE&T Cyber Defense Competencies. http://academiamilitar.pt/images/site_images/Eventos/3rd_Conference/Day_1/CD_Competency_Framework_and_Training_needs_-_Allard_Kernkamp_and_Josine.pdf Accessed November 06, 2018.

[32] Labour Market Information Directorate, Government of Canada. 2016. National Occupational Classification 2016. http://noc.esdc.gc.ca/English/noc/welcome.aspx?ver=16, Accessed November 06, 2018.

[33] Barry Lunt, Joseph Ekstrom, Sandra Gorka, Greg Hislop, Reza Kamali, Eydie Lawson, Richard LeBlanc, Jacob Miller, and Han Reichgelt. 2008. *Curriculum Guidelines for Undergraduate Degree Programs in Information Technology.* Technical Report. New York, NY, USA.

[34] National Security Agency College of Cyber. [n. d.]. National Centers of Academic Excellence for Cyber Defense. https://www.iad.gov/nietp/CAERequirements.cfm, Accessed November 06, 2018.

[35] National Security Agency College of Cyber. [n. d.]. National Centers of Academic Excellence for Cyber Operations. https://www.nsa.gov/resources/students-educators/centers-academic-excellence/cae-co-fundamental/index.shtml, Accessed November 06, 2018.

[36] NATO. 2018. Multinational Cyber Defence Education and Training Project (MN CD E&T). http://mncdet.wixsite.com/mncdet-nato Accessed November 06, 2018.

[37] NATO Review. 2018. The history of cyber attacks - a timeline. https://www.nato.int/docu/review/2013/cyber/timeline/en/index.htm, Accessed November 06, 2018.

[38] New Zealand Qualifications Authority (NZQA). 2017. Draft NZ Diploma in Cybersecurity (Level 6) 120 Credits. http://www.nzqa.govt.nz/assets/qualifications-and-standards/qualifications/ICT-quals-review/Security-and-Testing/NZ-Dip-Cybersecurity-L6-Nov2017-AtD.doc Accessed November 06, 2018.

[39] William Newhouse, Stephanie Keith, Benjamin Scribner, and Greg Witte. 2012. National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. US National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-181, Accessed November 06, 2018.

[40] William Newhouse, Stephanie Keith, Benjamin Scribner, and Greg Witte. 2017. National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. *NIST Special Publication* 800 (2017), 181.

[41] NIST. 2017. National Initiative for Cybersecurity Education, National Cybersecurity Workforce Framework. https://www.nist.gov/file/359261 Accessed November 06, 2018.

[42] The Norwegian Data Protection Authority. 2017. Software development with Data Protection by Design and by Default. https://www.datatilsynet.no/en/regulations-and-tools/guidelines/data-protection-by-design-and-by-default/

[43] ACM/IEEE-CS Task Group on Software Engineering Curricula. 2014. Software Engineering 2014.

[44] Allen Parrish, Rajendra Raj, Edward Sobiesk, Andrew Hall, J.J. Ekstrom, and Shannon Gorman. 2018. The Evolution of Cybersecurity Education in Four-Year Undergraduate Programs. In *22nd Colloquium for Information Systems Security Education (CISSE 2018)*. CISSE.

[45] Lance C. Pérez, Stephen Cooper, Elizabeth K. Hawthorne, Susanne Wetzel, Joel Brynielsson, Asim Gencer Gökce, John Impagliazzo, Youry Khmelevsky, Karl Klee, Margaret Leary, Amelia Philips, Norbert Pohlmann, Blair Taylor, and Shambhu Upadhyaya. 2011. Information Assurance Education in Two- and Four-year Institutions. In *Proceedings of the 16th Annual Conference Reports on Innovation and Technology in Computer Science Education - Working Group Reports (ITiCSE-WGR '11)*. ACM, New York, NY, USA, 39–53. https://doi.org/10.1145/2078856.2078860

[46] PRIPARE Project. 2016. PRIPARE Handbook: Privacy and Security by Design Methodology. http://pripareproject.eu/wp-content/uploads/2013/11/PRIPARE-Methodology-Handbook-Final-Feb-24-2016.pdf

[47] Public Safety Canada. 2018. National Cyber Security Strategy: Canada's Vision for Security and Prosperity in the Digital Age. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/index-en.aspx, Accessed November 06, 2018.

[48] Security and Intelligence Group (SIG). 2011. New Zealand's Cyber Security Strategy 2011. https://www.dpmc.govt.nz/publications/new-zealands-cyber-security-strategy-2011, Accessed November 06, 2018.

[49] Security and Intelligence Group (SIG). 2015. New Zealand's Cyber Security Strategy 2015: Action Plan. https://www.dpmc.govt.nz/sites/default/files/2017-03/nz-cyber-security-action-plan-december-2015.pdf, Accessed November 06, 2018.

[50] Security and Intelligence Group (SIG). 2016. New Zealand's Cyber Security Strategy 2016: Action Plan Annual Report. https://www.dpmc.govt.nz/sites/default/files/2017-06/nzcss-action-plan-annual-report-2016.pdf Accessed November 06, 2018.

[51] F. Spidalieri and S. Kern. 2014. Professionalizing Cybersecurity: A Path to Universal Standards and Status. *Pell Center for International Relations and Public Policy* (August 2014).

[52] The Tech Partnership. 2016. Information Security Standards. https://www.thetechpartnership.com/standards-and-quality/it-industry-standards/it-professional-standards/information-security/, Accessed November 06, 2018.

[53] Heikki Topi. 2017. IS EDUCATION: MSIS 2016: Guidance and Inspiration for Master's Programs in Information Systems. *ACM Inroads* 8, 2 (May 2017), 27–28. https://doi.org/10.1145/3078307

[54] UK National Cyber Security Centre. 2017. Certification of Bachelors' Degrees in Cyber Security. https://www.ncsc.gov.uk/content/files/protected_files/article_files/Certification-Bachelors-2_0-20171214.pdf, Accessed November 06, 2018.

[55] US Bureau of Labor Statistics. 2016-âĂŞ2017. Occupational Outlook Handbook: Information Security Analysts. US Department of Labor. http://www.bls.gov/ooh/computer-and-inforrnation-technology/information-security-analysis.html, Accessed November 06, 2018.

[56] US Department of Education. 2018. Integrated Postsecondary Education Data System. https://nces.ed.gov/ipeds, Accessed November 06, 2018.

[57] US National Security Agency and the Department of Homeland Security. 2018. Centers of Academic Excellence in Cybersecurity. https://www.nsa.gov/resources/educators/centers-academic-excellence Accessed November 06, 2018.

[58] US President's Council of Advisors on Science and Technology. 2012. Engage to Excel: Producing One Million Additional College Graduates with Degrees in Science, Technology, Engineering, and Mathematics. http://files.eric.ed.gov/fulltext/ED541511.pdf, Accessed November 06, 2018.

[59] Rebecca Vogel et al. 2016. Closing the cybersecurity skills gap. *Salus Journal* 4, 2 (2016), 32.

[60] S. Zweben and B. Bizot. 2010. 2016 Taulbee Survey. *Computing Research News* 29, 5 (May 2010).