Working Group D: Cyber Security Culture and Skills

White Paper: Task Force on Cybersecurity Professional Training and Development[1]

Date: 22 March 2019
Editors: Catherine Garcia-van Hoogstraten, Lecturer & Researcher in Data Governance, Cybersecurity and Technology at the Centre of Expertise Cyber Security, The Hague University of Applied Sciences and GFCE Advisory Board member and Laura Bate, Policy Analyst at New America

Data collection methodology

In September 2018 the participants in GFCE's Working Group D (WG D) identified the need for more information on existing programs for cybersecurity awareness and professional education and training. Between October 2018 and February 2019, the Chair and Task Force Leaders of WG D, together with the GFCE Secretariat, devised a questionnaire to which the WG D membership provided input pertaining to current initiatives for promoting cybersecurity awareness, education, professional training and development. This input was collected in the database of initiatives (Annex 1). In addition, this white paper is supplemented by the analysis of secondary sources [2].

Results and Analysis

Of the initiatives received covering both cyber security awareness and cyber security professional education and training programmes:

- 20 initiatives focused specially on professional education and training

---

[1] The 2019 White Paper "Task Force on Cybersecurity Professional Training and Development" was jointly drafted by Catherine Garcia-van Hoogstraten, Lecturer & Researcher in Data Governance, Cybersecurity and Technology at the Centre of Expertise Cyber Security- Cybersecurity for SMEs, The Hague University of Applied Sciences, Task Force Leader and GFCE Advisory Board member and Laura Bate, Policy Analyst New America. We thank the feedback and input of the members of the Working Group D: Cyber Security Culture and Skills.

[2] Open-source data concerning seminal reports linked to key areas of cybersecurity education and skills development. See all forthcoming footnotes.

- 4 initiatives cut across both cyber security awareness and professional education and training
- More government-sponsored than Non-Government Organisations (NGO) - sponsored activities were reported
- Many initiatives showed reliance on public-private partnerships between various combinations of government entities, academia, private sector, professional associations
- More activities with a national focus, rather than with a regional focus, were reported

The main goals of this white paper dealing with the issue of cybersecurity professional training and development are: (1) mapping the challenges and definitional issues around cyber professional training and development; 2) assessing the similarities and differences among the submitted professional education and training initiatives; (3) identifying elements of existing programs that would be useful replicated or adapted to different national contexts, and 4) providing conclusions and guidance in the design of policy aiming at advancing cybersecurity training and workforce development, which is key to the GFCE's promotion of cyber capacity-building among its members and the wider public.

1. Mapping the challenges and definitional issues around cyber professional training and development

The development of global human capital through cybersecurity education and training is a high priority of GFCE members. As reflected in the **Delhi Communiqué on a GFCE Global Agenda for Cyber Capacity Building** the issue is an important aspect of the effort that needs investment from different stakeholders in the global cybersecurity community to drive workforce development. Without an appropriate quality and quantity of cybersecurity personnel, the overall goals of ensuring a basic level of global cybersecurity cannot be met.

Nevertheless, it is important to take note of some of the persistent challenges and definitional issues around cyber professional training and development:

1.1 No shared taxonomy around the cybersecurity workforce:

Across various jurisdictions, there is no shared taxonomy of "typical cyber security roles as well as the knowledge, skills and abilities that underpin them."[3] This challenges leads, on the one hand, "educators and governments to design better programs and initiatives to attract, train and retain workers to the sector."[4] On the other hand, it challenges "industry to identify future talent more easily."[5] Accordingly, it is of crucial importance to identify efforts to standardize the taxonomy around the cybersecurity workforce in a timely fashion.

1.2 The cybersecurity skills shortage

As the Global Cyber Security Capacity Centre and the Center for Strategic and International Studies reported, the cybersecurity skills shortage presents a global "challenge for every industry sector,"[6] with nations across the development spectrum facing resource shortages.[7] A 2018 report by (ISC)² estimates a total of 2.9 million cybersecurity jobs unfilled globally.[8] In this regard,

---

[3] "National Initiative for Cybersecurity Education (NICE) Workforce Framework," AustCyber, Accessed 18 March 2019, https://www.austcyber.com/resources/dashboards/NICE-workforce-framework. This is a detailed breakdown of cyber security work roles. This framework includes: 7 categories of cyber security functions, 33 specialty distinct areas of cyber security work, 52 cyber security work roles comprised of specific knowledge, skills, and abilities required to perform tasks in a work role, tasks activities that could be assigned to a professional working in one of these cybersecurity work roles and knowledge, skills and abilities (KSAs) needed to perform tasks, usually demonstrated through relevant experience or performance-based education and training.

[4] Ibid.

[5] Ibid.

[6] *Hacking the Skills Shortage: A Study of the International Shortage of Cybersecurity Skills*, McAfee and Center for Strategic and International Studies, July 2016, https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hacking-skills-shortage.pdf.

[7] "Global Cybersecurity Education Needs Assessment," Global Cyber Security Capacity Centre, University of Oxford, June 2018, https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/Cybersecurity%20Education%20Needs%20Resource%20Paper_0.pdf. They report that in the ASEAN region, the cybersecurity industry faces structural challenges because of its highly fragmented nature. In Africa, there is an ongoing debate around the need for governments and enterprises to provide an enabling environment buoyed by a relevant educational curriculum designed to attract and groom these talents. A survey of higher income nations reports that cybersecurity education was deficient and that high-value skills are in critically short supply, the most scarce being intrusion detection, secure-software development, and attack mitigation.

[8] Cybersecurity Professionals Focus on Developing New Skills as Workforce Gap Widens: (ISC)² Cybersecurity Workforce Study, (ISC)2, 2018, https://www.isc2.org/-/media/ISC2/Research/2018-ISC2-Cybersecurity-Workforce-Study.ashx?la=en&hash=4E09681D0FB51698D9BA6BF13EEABFA48BD17DB0.

De Zan (2019) asserts that "it is not straightforward to distinguish between policies that are trying to increase the pipeline of security professionals (under-supply) from those that are seeking to improve the quality of job candidates (under-skilling)."[9] However, De Zan points out that "one of the correlates of the shortage could be the lack of professional experience of graduates and the absence of entry-level opportunities."[10] Consequently, "policy measures implemented by some governments suggest that the nature and the characteristics of the shortage are still not well understood."[11] There is debate around the types of skills that are required for addressing cybersecurity challenges over the next decades.[12]

1.3 Lack of differentiation between traditional and multidisciplinary cybersecurity professional training and development

The European Union Network and Information Security Agency (ENISA) draws attention to the fact that "education and training in cybersecurity should be a dynamic process because of their continuous evolution nature."[13] Accordingly, ENISA reports that "there is a lack of differentiation between traditional programmes offering fundamental security related curricula and more versatile

[9] Tommaso De Zan, Mind the Gap: The Cyber Security Skills Shortage and Public Policy Interventions, Global Cyber Security Center, Center for Doctoral Training in Cyber Security-University of Oxford, February 2019, https://gcsec.org/wp-content/uploads/2019/02/cyber-ebook-definitivo.pdf. This research relies on secondary data, such as data are extracted mainly from reports such as labor market analysis and "state of profession" surveys, i.e: the ISC Cybersecurity Workforce Study or the Information Systems Audit and Control Association's (ISACA) State of Cybersecurity survey. It also collects official national cyber security policy documents.

[10] Ibid.

[11] Ibid.

[12] See, for example, Laura Bate, *Cybersecurity Workforce Development: A Primer, New America Cybersecurity Initiative,* New America, November 2018, https://www.newamerica.org/cybersecurity-initiative/reports/cybersecurity-workforce-development/.

[13] Claire Vishik and Maritta Heisel, *Cybersecurity Education snapshot for workforce development in the EU,* European Union Agency for Network and Information Security, Network Information Security (NIS) Platform-working group on ICT research and innovation (WG3), September 2015, https://resilience.enisa.europa.eu/nis-platform/shared-documents/wg3-documents/cybersecurity-education-snapshot-for-workforce-development-in-the-eu/view. The focus of this report is on graduate curriculum (higher education and professional level training). Not distinctions are made between beginner or advanced levels of training. The NIS Platform partners established a *EU cybersecurity education database* including a list of available courses and certification programmes linked to Network and Information Security.

cybersecurity[14] programs with multi-disciplinary coverage and multi-faceted training materials."[15] As a consequence, "there are limited vehicles available today to create an all-round skill set in cybersecurity, with expertise in technology and societal issues."[16]

2. Summarizing the initiatives pertaining to Cybersecurity Professional Training and Development in Annex 1

Of the 20 initiatives focused specifically on professional education and training, the majority of the organizations that are carrying out the initiatives are government-driven efforts, including 4 in North America, 2 in Australia, 1 Asia, 1 in the Middle East. In addition, 4 Initiatives were also carried out by International organizations like ITU and regional organizations like the Council of Europe, European Commission or the Organization of American States. Furthermore, 8 initiatives were carried out by public-private partnerships, i.e. government entities, academia, private sector, professional associations.

2.1. Similarities between the initiatives:

The initiatives all shared few core similarities. The more salient is that the main aim of most these initiatives is a) to lower and mitigate the cybersecurity workforce gaps and b) not limited to formal education, but also includes badging, upskilling and reskilling. To a lesser degree, initiatives are c) addressing the issue of increasing the number of women and minorities in cybersecurity. Another similarity is that d)

[14] Moreover, the "soft definition of the 'science of cybersecurity' has led to great diversity in training and curricula impeding the creation of common context and core knowledge." (Source: Vishik and Heisel, 2015) For instance, ENISA "adopted a definition of cybersecurity that comprises a wide range of relevant topics...from cryptography, computer, information and network security to privacy, security economics, or legal, regulatory, and policy frameworks." (Source: Vishik and Heisel, 2015)
[15] Vishik and Heisel, 2015.
[16] Ibid.

many of the initiatives showed reliance on public-private partnerships between various combinations of government entities, academia, private sector, professional associations, potentially to make these initiatives sustainable over time.

2.2. Differences between the initiatives:

In many ways, the data is more clearly described by its differences than its similarities. While all reported initiatives center around professional education and training, interpretations of what that means vary by circumstance. The initiatives reported differ even in the fundamental issues they aim to address. Accordingly, it is no surprise to find that shape, target, sponsorship, and many other factors vary by programme. This section does not present an exhaustive list of these features, but rather highlights several differences that significantly distinguish initiatives from one another.

Government involvement: Of the data collected, about three-quarters of the initiatives focused on cyber security professional training and education specifically, and another quarter were classified both as cyber security awareness and professional training and education initiatives.[17] About three-fifths of these are government-led, and the rest are led by non-governmental organisations (NGOs) or intergovernmental organisations (IGOs).

However, this high-level differentiation breaks down upon inspection. Rather than a simple binary distinction, the initiatives exhibit a range of different levels of government involvement, and most exhibit some blending of government support with non-profit organisations, academic institutions, and private sector companies. Some relationships are funding based (i.e. grants and contracts),

[17] Another set of initiatives were focused specifically on cybersecurity awareness. These are discussed in a separate white paper by the GFCE's Working Group D, Task Force on Cybersecurity Awareness.

others are joint efforts, and still others are coalitions among a range of actors. Examples of different partnership arrangements from the collected data include:

- The Women in Cybersecurity (WiCyS) conference started with a government-funded grant to a university, which was then additionally supported by a range of organisations, particularly including private companies.
- Singapore's Skills Framework for Infocomm Technology was "Jointly developed by SkillsFuture Singapore (SSG), Workforce Singapore (WSG), and the Info-communications Media Development Authority (IMDA), together with industry associations, education institutions, training providers, organisations and unions."[18]
- The Digital Skills Coalition is a European Commission initiative, but is lead by a governing board that represents a wide range of stakeholders from different sectors.[19]

While initiatives are often spearheaded by either a government or non-government entity, they are not wholly one category or the other because--in a variety of ways--they blend resources from both.

Intended demographic: Not only do programmes vary in terms of the demographics they are intended to impact (e.g. women, policymakers, children), they also vary in terms of the specificity of those efforts. For example, Cyber Shikshaa is a programme based in India to teach cyber security skills to female engineering graduates ages 21 to 26 in certain cities.[20] The programme has a very specific definition of the demographic it intends to impact. On the opposite end of the spectrum, Australia's Cyber Smart Nation initiative includes a series of programmes designed to impact a much broader population--not just

[18] "Skills Framework for Infocomm Technology: What Is It?," SkillsFuture, Accessed 18 March 2019, https://www.skillsfuture.sg/skills-framework/ict.
[19] "The Governing Board of the Digital Skills and Jobs Coalition," The European Commission, Accessed 18 March 2019, https://ec.europa.eu/digital-single-market/en/governing-board-digital-skills-and-jobs-coalition.
[20] "Cyber Shikshaa," DSCI, Accessed 18 March 2019, https://www.dsci.in/cyber-shikshaa/.

women, but also universities, the tertiary sector, and ultimately, the whole nation.[21] These two programmes illustrate not just the different demographics, but the range of differences in scope and scale in defining what demographic the programme will impact.

Focus on cyber security: Not all reported programmes focused on cyber security specifically. Or, interpreted differently, the data showed variations in what respondents understood "cyber security" to mean. Some programmes focused on developing skills in cyber security specifically, while others addressed the broader topic of digital skills. Still others considered subsets of the larger topic of cyber security, for example cyber crime.

Scope of mission: Some initiatives were fairly narrowly defined, outlining a single, specific training programme or tool. For example, the Collegiate Cyber Defense Competition is an annual capture-the-flag competition in the United States. At over 230 colleges and universities participating, the programme is fairly large in terms of number of participants.[22] Despite its size, in terms of the scope of what the initiative is intended to do, its mission is fairly narrowly defined: it is a capture-the-flag competition. Conversely, other initiatives serve as a platform for subsidiary projects, and are quite broad in terms of what the are intended to do. For example, Cyber New Brunswick's Cybersecurity Skills and Workforce Development Programme offers a range of initiatives and resources. They even have a mascot, "Cybear" the protective mother black bear.[23]

---

[21] "A Cyber Smart Nation," Australian Government, Department of Homeland Affairs, Accessed 18 March 2019, https://cybersecuritystrategy.homeaffairs.gov.au/cyber-smart-nation.

[22] "Cyber Cinderella story, Underdog U of Virginia wins NCCDC college cyber championships," Raytheon, Accessed 18 March 2019, https://www.raytheon.com/news/feature/cyber-cinderella-story?WT.mc_id=facebook_socialmedia_N/A&utm_source=facebook&utm_medium=organic&utm_campaign=N/A&linkId=50638608.

[23] "Planning for Our Online Future," CyberNB, Accessed 18 March 2019, https://cybernb.ca/en/workforce-development/k-12/.

It is also worth noting that among the programmes reported, two are build-outs of an existing program. AustCyber, for example, has developed a dashboard to make the NICE Cybersecurity Workforce Framework more visually digestible.[24] Such programmes have a two-part goal: the first is essentially identical to the intended goal of the initiative upon which it iterates. In the case of AustCyber's dashboard, this primary goal is establishing a taxonomy for cyber security jobs, just as the Framework does. But there is an implicit second goal of increasing its utility--making the Framework easier to use through a more intuitive presentation.

Through such examples, it is apparent that the initiatives reported vary not only in their intended goal, but in the scope of that goal. Some project goals were narrowly defined; whereas others were very broad, serving as a platform to enable a range of subsidiary projects. Others had more than one goal underpinning the overall project.

3. Identifying key elements a national program should include in order to address the challenges

Apart from their shared goal of filling cyber security jobs, the initiatives identified in this study vary widely. Between the heterogeneity inherent to cyber security jobs and the enormous (and growing) number of open jobs, this variety is an important feature. The global cyber security community will require a wide variety of solutions to address the challenge. Moreover, these programmes evolved to address a diversity of local, regional, and global contexts. Between the range of goals, demographics, cultural influences, resources, and challenges, there can be no consistent recipe to provide professional education and training in cyber security.

[24] "National Initiative for Cybersecurity Education (NICE) Workforce Framework," AustCyber, Accessed 18 March 2019, https://www.austcyber.com/resources/dashboards/NICE-workforce-framework.

Accordingly, the various features of programmes encountered through this effort do not define specific recommendations on what policymakers should implement in their own national context. Instead, the programmes show the various dimensions and spectrums along which new efforts can range. Therefore, this study does not suggest the right answers for policymakers to use in implementing their programmes, but rather, the elements for them to consider.

Define the need: The first step in the creation of a new programme is identifying the goal of that programme. As this project shows, the desired outcome of a new programme can be as broad as a series of initiatives designed to work in concert to build connectivity between educators and employers, or it can be as narrow as a single line of effort intended to boost the participation of a particular demographic in the workforce. In either case, being explicit about that goal will help to identify where a new programme fits into the larger ecosystem of existing programmes.

Identify available resources: The varying structures of the initiatives reported show how those initiatives drew on a range of resources, including financial support, endorsement by authorities, platforms and execution from other partners, and many others. In designing new programmes, a first consideration should be what resources are available, and which organisations can supply those resources.

In other words, consider what partners are in a position to contribute to the effort, and how an initiative could be structured to make best use of those resources. A governing board in the model of the the Digital Skills Coalition[25] can provide expertise. Partnership with government offices may make sense for either resources (for example, the grants that supported the development of the WiCyS conference) or for official endorsement, as in the National Centers of Academic Excellence in

[25] "The Governing Board of the Digital Skills and Jobs Coalition," The European Commission, Accessed 18 March 2019, https://ec.europa.eu/digital-single-market/en/governing-board-digital-skills-and-jobs-coalition.

Cybersecurity. Identifying the resources needed, therefore, becomes a major driver of the structure and partnerships of new initiatives.

Research existing tools: Many survey respondents cited budgetary limitations as a central challenge for professional education and training programmes. Given these budget constraints, and limited resources more generally, making good use of the tools that have already been developed is an especially promising option. Before beginning a new programme, a critical question should be whether or not something similar already exists. If so, can it be adapted to meet the new specific context? Can a chapter of an existing organisation be established internationally? Can a tool be implemented in a new location?

Seek out collaborators: Several of the submitted initiatives listed multiple entities as being the lead or owner of the initiative. When creating a new programme, identifying potential collaborators can help launch the effort by providing access to resources and tools (see above) as well as knowledge and subject matter expertise. Collaboration in local or regional settings helps develop a strong pipeline, contributing to the sustainability of a cyber security workforce. Further, this activity facilitates and stimulates the sharing of information, which can lead to determining successful approaches and best practices.

4. Providing conclusions and guidance in the design of policy aiming at advancing cybersecurity training and workforce development

Notably, the data collected does not measure programme effectiveness. Rather, it catalogues what exists. As such, the limit of this paper is that cannot define the policies that shape *effective* programmes in professional education and training. With that said, observers can still find important policy implications within the data collected.

Growing and utilising an international community of practice:

Perhaps foremost, the study makes clear that a robust and growing community of practice exists internationally in cyber security professional education and training. Stakeholders across the globe demonstrate a clear interest in working innovatively to find programmes that fill cyber security jobs.

This widespread interest suggests recommendations for the GFCE and for GFCE members, respectively. First, the survey returned sufficient data to make clear that there is value in continued work of this type. Whether conducted by the GFCE or other organisations, studying and building connectivity among this community of practice offers the opportunity of improving the state of cyber security globally. Second, there is a growing body of expertise in cyber security professional education and training. GFCE members that are interested in developing their own programmes have an excellent consultative resource in the programmes and programme sponsors reported herein.

Cultivating a Domestic Ecosystem:

Taking a step back and looking at the data not as a series of individual programmes, but rather as the outline of a trend, a prevailing observation is that cyber security professional education and training programmes are not operating in isolation. Most are part of a larger ecosystem, each working in a different way to fill cyber security jobs. Therefore, the implications for policymakers are not simply that governments should create a national programme for professional education and training. Rather, policymakers should seek to create an environment in which a community of such programmes can emerge, grow, and thrive. This ecosystem allows for variance based on context and also encourages innovation in programmes that are steered by individual champions or supporting organisations.

Certain elements derived from the data can help policymakers build an ecosystem aimed at advancing cyber security training and workforce development. At the base

of these are prioritising workforce development as a core requirement for a healthy domestic cyber security capability and normalising the notion that it is everyone's job to help contribute to better cyber security. Policymakers can also develop mechanisms that help identify areas of critical need and barriers to success. Being able to address these barriers as well as provide systems and processes that encourage information sharing within domestic and international constructs helps facilitate ecosystem growth.

Noting these as a basis, policymakers can encourage stakeholders to build specific programmes and efforts through a range of activities. Piloting or operating an activity in public sector workplaces can help build buy-in from others and provides a testbed for gauging future success. Funding the development of programmes by external partners through grants and contracts spurs growth and can provide a sense of community and ownership so that there is no single point of failure. Policymakers can also serve as a convenor of these partners and other stakeholders in order to foster this sense of community and build an ongoing conversation.

Recommendations for Future Work:

This study is an important first step in better understanding professional education and training programmes in cyber security internationally. There are certainly ways in which this work may be strengthened and carried forward.

One such advancement would be to broaden the reach of the survey. The current work noted a lack of programmes in certain regions like Latin America and East Asia. However, it is unclear whether this result is because there are not many programmes in those regions or because the survey did not connect with programmes in those regions. Because WG D members circulated the survey and were often the respondents reporting programmes, it is likely that the study incurred some sample bias because members are more likely to know about programmes in their own area. Future work could seek to extend the reach of the survey.

A second opportunity to further the work started by WG D is to establish a means of measuring programme effectiveness. This study returns data on what exists, but not necessarily what works. It may be easy to conclude that if a programme continues to be active and grow, there are lessons to be taken from it. However, programme continuation may not be an especially adequate proxy for programmatic effectiveness. Future research could seek evaluate what works in growing a robust cyber security workforce.

Annex 1: Database of initiatives