Education for the Multifaith Community of Cybersecurity

Steven Furnell, Matt Bishop

Education for the multifaith community of cybersecurity

Steven Furnell[1,3][0000-0003-0984-7542] and Matt Bishop[2][0000-0002-7301-7060]

[1] Centre for Security, Communications and Network Research, University of Plymouth, Plymouth, UK
[2] Department of Computer Science, University of California at Davis, Davis, CA, USA
[3] Security Research Institute, Edith Cowan University, Perth, Western Australia
steven.furnell@plymouth.ac.uk; mabishop@ucdavis.edu

Abstract. The demand for cybersecurity professionals is growing. Many cybersecurity academic and training programmes exist to prepare students and professionals for these jobs. The programmes cover many areas of cybersecurity with considerable overlap, but with different emphases. Some are highly technical and cover little non-technical; others do the opposite. Cybersecurity jobs typically require some technical knowledge, an ability to place security problems in a larger context, and an ability to communicate this information effectively and convincingly. The problem with treating technical and non-technical subjects as silos rather than recognizing the two are tightly related and need to be taught together. This paper shows how seven common cybersecurity frameworks and ten masters' courses from the UK and US cover both technical and non-technical content. It examines the balance of technical courses, non-technical courses, and courses that mix both technical and non-technical material. It argues that these topics cannot be siloed, and their balance is critical to meeting the goals of the frameworks and programmes.

Keywords: Certifications, Curricula mapping, Cybersecurity Frameworks, Masters Degrees, Qualifications.

1 Introduction

Over the last two decades, the need for improved cybersecurity has become more visible and more critical. Newspapers report compromises of major vendors and organizations daily; nation-states engage in cyberwarfare by attacking other countries' infrastructure; and attacks increase in sophistication. The damage from these attacks has repercussions throughout societies. As an example, the Equifax compromise exposed tens of millions of credit records, putting their subjects at risk for identity theft and other nefarious purposes [1].

There is no doubt that the profession is suffering from a shortage of qualified and skilled workers. As an example, according to a survey of 267 cybersecurity professionals conducted by Enterprise Strategy Group (ESG) and the Information Systems Security Association (ISSA), three quarters felt that the skills shortage had impacted them in recent years, with a third indicating that it had done so significantly [2]. Similarly,

the latest cybersecurity workforce study from (ISC)[2] reports a global skills gap of 4.07 million, and further suggests that 65% of organisations have a skills shortage, with 51% considering themselves to be at moderate or extreme risk as a result [3].

Reflecting the resultant demand for skilled workers, there has been a growth in both academic programmes and industry certifications targeting the topic area, which should in theory begin to help in offsetting the shortage. However, while there are many education and training options on offer, there is a question of whether the full breadth of the cybersecurity discipline is receiving the attention that it requires.

Cybersecurity spans many technical and non-technical skills, ranging from technical and low-level aspects of computing to human, organizational, and business skills. The latter, often called "soft skills," seem to be considered less important in many communities, even though in practice, they are as important as the former ("hard skills"), and indeed are skills that employers seek when hiring – especially given the need to understand the effects of security problems on the company, not just the technical implications.

The paper examines the balance of technical and non-technical topic coverage that exists within the various cybersecurity topic frameworks and standards that may be guiding academic and industry perspectives, and how this coverage aligns to areas of employer demand in terms of job openings. It then considers how the topic is represented within academic qualifications in cybersecurity, with an assessment of the coverage within a series of Masters degrees from the United Kingdom and the United States. The findings enable a comparison to be made between the coverage in the reference frameworks and market demand, and the focus provided by the academic programmes.

2 Cybersecurity skills – spectrum or silos?

Players within the cybersecurity community often have conflicting perspectives of what cybersecurity actually is, with the consequence that the technical and business camps often cannot relate to each other and are even dismissive. Management often views the technology staff through the lens of the established stereotype of being a group of geeks and nerds who lack the ability to understand and properly communicate the aspects of their work relevant to the business or organization. Technical practitioners often consider the business and human side of cybersecurity to be some sort of sanctuary for those who can no longer keep up with the technology. Such attitudes foster a "them and us" culture within the discipline of cybersecurity. The key argument of this paper is that, to move things forward effectively, it is important to accept that cybersecurity is a multifaith community, and educating accordingly is critical to improving the state of the art and its effectiveness. Some topics are central, some are peripheral, but they are all cybersecurity. In practice, the key needs vary according to the party involved:

- for providers - knowing how education maps to roles; and
- for employers - knowing what is needed to get the job done.

The authors have already examined the second point in an accompanying paper that considers the relationship between skills, certifications and roles, recognising that this is what employers will ultimately need to understand when looking to recruit talent that addresses their needs [4]. The focus of the current paper is more towards the first point, considering the extent to which academic programmes are effective in addressing the breadth of the domain.

Training and education clearly need to be aligned to target roles. For example, someone trained to conduct risk assessment cannot be expected to use that training as a basis to do penetration testing. It is interesting that most of the industry and professional certifications have a technical flavour, not least because many of them are geared towards securing a particular product or platform. This provides learners with expertise in a particular area, but not with the breadth required of most cybersecurity specialists.

Table 1 lists the relative importance of different forms of cybersecurity qualifications and experience, according to the $(ISC)^2$ Cybersecurity Workforce Study 2018 [5] (based upon responses from 1,452 cybersecurity professionals from across North America, Latin America, Asia-Pacific and Europe). Looking at the ranking, it is rather notable that degree qualifications are at the bottom of the list. The survey does not comment upon the reason for this, but one might hypothesize that a potential contributor could be that employers have not found current offerings to be delivering graduates with the knowledge and skills that they need. Academic institutions and educators should not necessarily expect anything they do to be able to *change* this, but they at least need to *recognise* it and ensure that their degrees remain relevant.

Table 1. Importance of different types of cyber security qualifications and experience.

Characteristic	Respondents rating as important
Relevant cybersecurity work experience	49%
Knowledge of advanced cybersecurity concepts	47%
Cybersecurity certifications	43%
Extensive cybersecurity work experience	40%
Knowledge of basic cybersecurity concepts	40%
Strong non-technical/soft skills	39%
Cybersecurity qualifications other than certifications or a degree	37%
Knowledge of relevant regulatory practices	37%
Cybersecurity or related graduate degree	21%
Cybersecurity or related undergraduate degree	20%

It is also notable that non-technical skills are rated ahead of most of the qualification-related options, highlighting the fact that those working in cybersecurity are expected to be able to communicate and integrate within the business context. This finding is echoed in a report from Infosec, suggesting the top ten skills that security professionals needed to have in 2018 [6]. Looking at the list below, it clear that soft skills and non-

technical aspects have a significant presence alongside the ones that are clearly technical:

1. Security Analysis
2. Penetration Testing
3. Secure Application Development
4. Incident Response
5. Cloud Security
6. Data Science and Analytics
7. Customer Service
8. Communication
9. Collaboration
10. Curiosity and Passion for Learning

This is not to suggest that it is an either-or situation. The most desirable scenario is to have an effective *combination* of skills, as illustrated the following quotes from two further reports:

> "*Currently, the most-prized hire in a cybersecurity team is a technically proficient individual who also understands business operations and how cybersecurity fits into the greater needs of the enterprise*" [7]

> "*the really good people in the security industry are far more than just technically skilled. Especially in the higher ranks, you will see people who have a good mix of technical and soft skills, which enables them to implement control frameworks that really work*" [8]

This need to look beyond technical ability broadly aligns with earlier work from Dawson and Thomson, who suggest six key traits that the members of the future cyber security workforce are likely to need: systemic thinking, teamwork, continued learning, strong communication ability, a sense of civic duty, and a blend of technical and social skill [9]. This does not devalue the importance of the technical skills. It emphasizes the importance of not seeking them in isolation, because knowing which cybersecurity issues are critical to the functioning of the enterprise, and being able to present cybersecurity issues so that non-computer people can understand them and act appropriately, require the aforementioned blend of technical, social, organizational, and business skills.

In practice the technical and non-technical aspects are not distinct and separated. They overlap, interact and affect each other (e.g. technologies are deployed within a legal and regulatory context; choices are informed by policy and risk assessment; effectiveness is influenced by user education and awareness). So, we need emerging cyber professionals to be taught to think of them holistically and not to regard them as competing views (i.e. recognising that effective cybersecurity benefits from a spectrum of skills rather than placing them within silos).

3 Examining coverage within cyber security frameworks

Although there is clear agreement that a range of underlying topics fit within the overall cyber security discipline, there is currently no single source that definitively specifies what the topics are or how they are structured. There are, however, a number of key

sources that describe the information/cyber security discipline (and which in several cases are used to directly inform education and training activities). With this in mind, it is relevant to look at the topic coverage within these, and the extent to which they cover the technical and non-technical perspectives. Table 2 identifies seven such sources, and summarises the categories under which they have grouped their security topics. It should be noted that of these some are formal standards, whereas some bill themselves as frameworks, guidelines and bodies of knowledge. However, for the purposes of this discussion, we will use the term *framework* as the generic label by which to reference them, while further examining the ways in which each elect to classify and divide the overall topic space.

Table 2. A summary of the selected cybersecurity frameworks.

Source	Framework	Description / Coverage
ACM/IEEE/ AIS/IFIP	Cybersecurity Curricula 2017 (CSEC2017) [10]	Produced by the ACM/IEEE/AIS/IFIP Joint Task Force in 2017, the guidelines provide a structure for the cybersecurity discipline, defining its boundaries and outlining key dimensions of a curricular structure. It identifies 8 Knowledge Areas: Data Security; Software Security; Component Security; Connection Security; System Security; Human Security; Organizational Security; Societal Security.
CIISec	Skills Framework v2.4 [11]	The Skills Framework describes the range of competencies expected of Information Security and Information Assurance Professionals in the effective performance of their roles. It is based on 11 Security Disciplines: Information Security Governance and Management; Threat Assessment and Information Risk Management; Implementing Secure Systems; Assurance, Audit, Compliance and Testing; Operational Security Management; Incident Management, Investigation and Digital Forensics; Data Protection, Privacy and Identity Management; Business Resilience; Information Security Research; Management, Leadership, Business and Communications; Contributions to the Information Security Profession and Professional Development.
CyBOK project	Cyber Security Body of Knowledge (CyBOK) [12]	An initiative funded by the UK's National Cyber Security Programme and seeking to codify the foundational and generally recognised knowledge on cyber security. It proposes 19 Knowledge Areas: Risk Management & Governance; Cyber Physical Systems; Law & Regulation; Physical Layer and Telecommunications Security; Human Factors; Secure Software Lifecycle; Privacy & Online Rights; Operating Systems & Virtualisation Security; Ad-

		versarial Behaviours; Malware; Network Security; Security Operations & Incident Management; Cryptography; Software Security; Authentication, Authorisation & Accountability (AAA); Web & Mobile Security; Hardware Security; Distributed Systems Security; Forensics.
$(ISC)^2$	Common Body of Knowledge (CBK) [13]	The CBK is used as the underlying knowledge base for $(ISC)^2$'s series of professional certifications including CISSP, SSCP and CCSP. It identifies 8 domains: Security and Risk Management; Asset Security; Security Architecture and Engineering; Communications and Network Security; Identity and Access Management; Security Assessment and Testing; Security Operations; Software Development Security.
ISO/IEC	27002:2013 - Code of Practice for Information Security Controls [14]	An International Standard designed as a reference for organizations to use in selecting common security controls, as well as offering guidance on their use. It is structured around 14 main clauses: Information Security Policies; Organization of Information Security; Human Resource Security; Asset Management; Access Control; Cryptography; Physical and Environmental Security; Operations Security; Communications Security; Systems Acquisition, Development and Maintenance; Supplier Relationships; Information security Incident Management; Information Security Aspects of Business Continuity Management; Compliance.
NIST	National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework [15]	The NICE Framework aims to provide a common, consistent lexicon that categorizes and describes cybersecurity work, and a reference for describing and sharing information about the knowledge, skills, and abilities involved. It is based upon 7 Categories: Analyze; Collect and Operate; Investigate; Operate and Maintain; Oversee and Govern; Protect and Defend; Securely Provision.
NSA	Centers of Academic Excellence (CAE) Knowledge Units [16]	The Centers of Academic Excellence program identifies four classes of Knowledge Units: *Fundamental* (Cybersecurity Foundations; Cybersecurity Principles; IT Systems Components), *Technical Core* (Basic Cryptography; Basic Networking; Basic Scripting and Programming; Network Defense; Operating Systems Concepts), *Non-Technical Core* (Cyber Threats; Cybersecurity Planning and Management; Policy, Legal, Ethics, and Compliance; Security Program Management; Security Risk Analysis), and *Optional* (spanning 56 further units covering both technical and non-technical aspects of security, as well as more general computing and communications topics). The

Knowledge Units are then used within designated specialisations for Cyber Defence Education (CAE-CDE), Cyber Defence Research (CAE-R) and Cyber Operations (CAE-CO). All designations require the Fundamental units to be covered, and various percentages and combinations of the others.

The frameworks present various views of what cyber looks like. While they are not necessarily *competing* views, they are not entirely *consistent* either (particularly when looking into their various categories in more detail). However, here we consider how the broad areas map onto the technical and non-technical perspectives of cybersecurity. Fig. 1 demonstrates the proportion of coverage allocated to technical and non-technical aspects of cybersecurity, based upon a classification of the top-level topic categories listed in Table 2. In some cases, the topics covered a mix of technical and non-technical aspects (such as the *Adversarial Behaviours* Knowledge Area within CyBOK, and the *Operate and Maintain* category within the NICE Framework). The CIISec Skills Framework is unique in having a discipline that seemed to be a non-cybersecurity topic (namely *Management, Leadership, Business and Communications*, which nonetheless remains relevant *within* cybersecurity as it relates to the much-needed soft skills). The entry depicting the Knowledge Units from the NSA's Center of Academic Excellence is only considering the split of coverage amongst Fundamental and Core units, as it is felt that representing the optional units could give a misleading impression (given that they will be taken in significantly different combinations and many have a non-security focus).

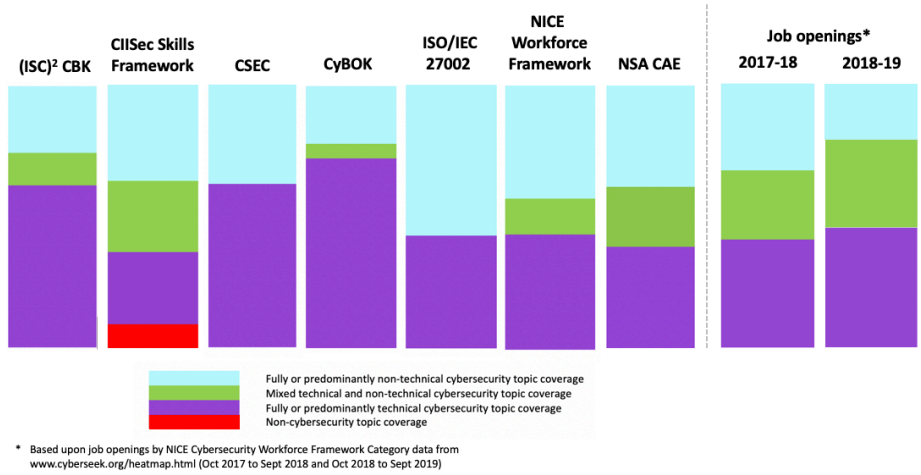

Fig. 1. Topic coverage within alternative cybersecurity frameworks.

The representation in the figure does not take account how large or extensive each category is, and these can decompose in rather different ways. For example, in ISO/IEC 27002, the non-technical clause of *Organization of Information Security* has seven underlying controls, whereas the largely technically focused *Access Control* clause is

home to fourteen associated controls. Similarly, within the CIISec Skills Framework, the discipline of Information Security Governance and Management hosts seven underlying skills groups, whereas Implementing Secure Systems has just three. Nonetheless, it was considered most appropriate to keep the focus at the high-level categories on the basis that each of the frameworks selected these to represent their main structure (and so presumably considered the resulting categories to be of broadly equal merit and importance within cybersecurity as a whole, regardless of the number of underlying points within them).

The goals of the cybersecurity frameworks lead to differences in emphasis. The CSEC2017 and arguably CyBOK frameworks are intended for academic education, and the others are for professional certification or training. The academic frameworks tend not to mix technical and non-technical subjects, as these are generally seen as separate courses. Hence, in Figure 1, these have little to no green. ISO/IEC 27002, a code of practice, also makes the same delineation. The professional certification and training frameworks, on the other hand, mix technical and non-technical aspects of cybersecurity, because practitioners must take into account the non-technical needs when designing and implementing technical controls.

The frameworks offer a point of reference for other activities to map against, including academic courses, professional certifications, and training programmes. Indeed, in some cases this is specifically what they exist to provide, with the CSEC guidelines offering a framework specifically for undergraduate academic curricula and the $(ISC)^2$ CBK being used as the reference point for $ISC)^2$'s own certifications. Meanwhile, other frameworks have a more general purpose, but can still be applied in this context. For example, Hallett et al. [17] have mapped other security frameworks to CyBOK and indicated its potential as a reference point for curricular mapping. Similarly, the national certification programme for academic degrees operated by the UK's National Cyber Security Centre has been using an adapted version of the CIISec framework as the basis for mapping programme coverage [18].

4 Examining coverage within academic degrees

Having looked at the overall composition of the various guiding frameworks that reflect and inform the way we understand cybersecurity, it is interesting to apply the same high-level mapping exercise to the content of academic degrees. With the in mind, we have taken a sample of Masters programmes offered by a range of UK and US universities, and then examined the breakdown of taught module/unit topics offered within each of them. We considered Masters programmes rather than Bachelors degrees because the former are expected to have a more cyber-specific coverage, whereas undergraduate programmes and other earlier-stage qualifications are expected to include a fair volume of more general computing/IT content, which would complicate the task of seeing how security is addressed. In addition, in the Masters, all topics are being covered at the same academic level, whereas attempting to fairly assess undergraduate degrees would also involve some consideration of the years of study at which different security topics were being introduced.

We examined two broad categories of topic coverage within cybersecurity. *Technical cybersecurity* covers material such as system, device, and network security, plus a range of underlying technical mechanisms that support computing and networking. For example, penetration testing, digital forensic analysis, cryptography, authentication, and access control fall into this category. Meanwhile, *non-technical cybersecurity* focuses on the managerial, human, legal, and physical protection. Issues such as risk assessment, business continuity planning, development of security policies, delivery of security awareness training, and cyberlaw fall into this category.

Looking firstly at the UK market, there are more than 100 cybersecurity-related Masters programmes, and the investigation specifically focused upon those titled 'Cyber Security' (as opposed to any more specific - and typically technical - variants such as forensics, network security or ethical hacking). We are looking at a set of programmes that all claim to offer coverage across the discipline as a whole. The sample used here was drawn from a range of universities around the UK (spanning different levels of teaching versus research intensity), with a mix of newer and more established programmes, and nothing inherent within the sample would be expected to skew the results.

The coverage of the degrees was assessed based upon publicly available information from websites (which varied from titles only, to summary paragraphs, to more detailed lists of underlying topic coverage). In terms of content, some programmes include a broad range of options that allow candidates to choose their own route and coverage balance through the selection of electives. Equally, there are some cases in which the syllabus is fully mandated, or the extent of optionality is limited. All also offer substantial project modules, but these are excluded from the assessment as the specifics of their focus will vary depending upon candidates' preferences or topics made available by academic supervisors.

The overall findings are summarised in Fig. 2. It is clear that the situation is generally far less balanced than amongst the frameworks discussed earlier. With one exception, the non-technical aspect of cyber appears to receive little treatment. In programme 5, half of the content is based around more generic computing and network material rather than anything security specific; the rest predominantly cover cybersecurity topics. While it is accepted that wider computing knowledge in areas such as programming, operating systems, and networking can legitimately be relevant in the context of supporting cybersecurity (as well as requiring security aspects to be considered in such areas), this level of coverage seems excessive in a degree claiming to be specifically about cyber. The relevance of the content to employer needs is questionable. Indeed, comparing the spread of job openings illustrated in Fig. 1 to this raises the question of whether the resulting graduates will have topic knowledge and skills that are market-aligned.

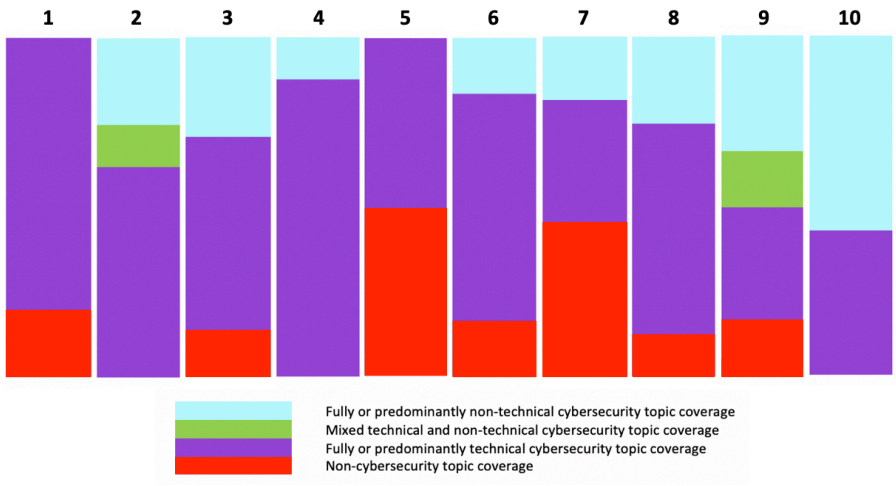

Fig. 2. Topic coverage of ten 'MSc Cyber Security' degree programmes in the UK

There is also the question of how and where the courses deliver the soft skills that employers say they need and rate highly. At first glance, there appears to be little direct attention to these aspects. As these are postgraduate courses, these skills will have been promoted and developed during earlier study. Additionally, there is a good chance that in many cases they will be embedded within other modules, with elements such as group work, presentation and writing skills being a specific part of the assessed activities.

Looking at the wider UK cybersecurity degree market and the specialisms represented, the volume of digital forensics degree programmes seems to outstrip the apparent demand for the 'Investigate' strand of the workforce framework. Meanwhile, other topic specialisations that arguably address market need are less represented within degree programme titles, possibly because universities do not consider them to be sufficiently attractive to students coming *into* the process (e.g. 'risk and governance' is not as applicant friendly as 'ethical hacking').

We also looked at a sample consisting of ten Masters programmes in US universities. As with the UK, there is a plethora of such programmes. We again chose ones with the words "Cyber Security" as opposed to anything more general or more specific. This allowed us to compare the breakdown of the programmes with the breakdown of the UK programmes.

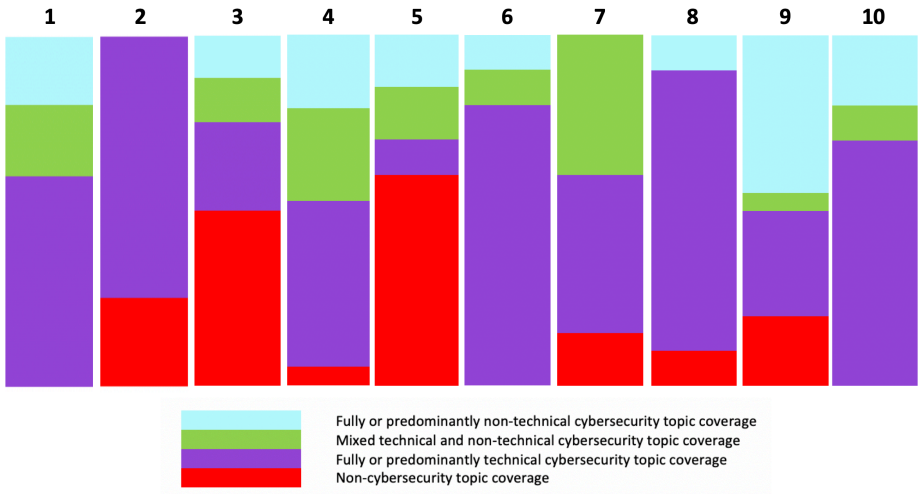

Fig. 3. Topic coverage of ten 'MSc Cyber Security' degree programmes in the US

The programmes have both required courses and electives. Only one school prescribes all courses; the rest allow students to select from among the electives, sometimes with the approval of their advisor. The ratios in Fig. 3 include all required courses and electives except those that could not be properly categorized. For example, a capstone project could be very technical or focus on the use of the technology; hence, it could not be assigned to one category.

Four of the US universities had multiple tracks. The tracks in universities 2 and 6 were all technical. University 7 had an interdisciplinary track and a technical track; we used the interdisciplinary one. University 9 had 3 tracks, each of which prescribed some courses and constrained how the electives could be selected. It also had an untracked degree. Because of the myriad of possible combinations, we used all courses to compute the statistics.

Of the ten universities, eight were R1 (doctoral programme – very high research activity), one was R2 (doctoral programme – high research activity), and one was M1 (Masters programme – larger programme) under the Carnegie Classifications. Eight were DHS/NSA Centers of Academic Excellence, seven having CAE-CD (education) classification, five with CAE-R (research) and two with CAE-CO (cyberoperations) classifications; six institutions had more than one such classification [19]. Six were public institutions; the rest were private not-for-profit institutions. Considering the entire university, one had fewer than 10,000 students; four had between 10,000 and 245,999 students, and the remainder had at least 25,000 students [20]. Information on the number of students in each Masters programme was not available.

The results show an overarching focus on technology. Of the ten programmes, only one has more than 20% of the courses being primarily non-technical. That programme is focused on risk management, which explains the predominance of non-technical cybersecurity-related courses. Three of the programmes have a fifth of the courses being

primarily non-technical. One is from a school of information science, which is traditionally broader than programmes in computer science. The other is an interdisciplinary track degree, which would be expected to be broader than a strictly technical degree.

The others are primarily technical, and the courses fall into two groups: those directly related to cybersecurity (such as courses on cryptography and network security) and those that are not (such as courses on compilers and operating systems). Except for the three schools mentioned above, these courses account for over 70% of the curriculum. Further, the number of technical courses is greater than the number of mixed technical, non-technical courses in all but 2 of the schools, sometimes by a large percentage. One of those universities focuses on public policy, while the second figure comes from a school where interdisciplinary work is emphasized.

The mixture of technical and non-technical cybersecurity elements in a Masters course is necessary to show that cybersecurity is not solely a technical endeavour. This work used a sampling of 20 university programmes (10 from the UK and 10 from the US) to examine whether this was commonly done. A more comprehensive study would shed further light on how widespread this confluence of technical and non-technical material in cybersecurity programmes is. Such a study would lead to a deeper understanding of how the two should be integrated to meet the particular goals of the academic programme. A major point of this study was to show how widely varied the focus of a programme called “Cyber Security” can be, and a more comprehensive study would undoubtedly provide more details on the extent of the variation.

5 Conclusions

Multiple frameworks provide structure for the field of cybersecurity. These frameworks each take a slightly different view of what constitutes the field of cybersecurity. As the frameworks were developed for different purposes, and in different cultures, none can be definitive. Nevertheless, the overlap among them is striking.

Frameworks have two uses. The first is to provide a basis for asserting that a certification or an academic programme meets the desired goals. The content of the courses is mapped into the framework's topics, and from that the educators can determine gaps in coverage, or places where more (or less) depth of coverage is required. The second is to provide a basis for comparison. If two programmes are mapped into the same framework, the differences in them will show up as inconsistencies in the coverage of the framework's topics.

Which framework to choose is driven by the needs of the students, the practitioners, and the employers. They are all fit for various purposes -- but the evaluator, students, teachers, and institutions need to be clear on what their purpose is. The same cannot be said for the MSc degree programmes that were examined. In these cases, some include far less balanced coverage of cybersecurity than others. Given that they are called programmes in "cybersecurity", often by exactly the same names, both candidates and employers must understand how this coverage positions graduates for entry into the job market.

Recognising the need for balanced coverage is not enough. It is also necessary to recognise how the programmes and frameworks balance the technical and non-technical topics needed by cybersecurity practitioners, managers, and policy setters.

Acknowledgements. Matt Bishop gratefully acknowledges the support of grants DGE-1303211 and DGE-1934279 from the National Science Foundation to the University of California at Davis. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

References

1. Berghel, H. (2017). "Equifax and the Latest Round of Identity Theft Roulette", *IEEE Computer* 50(12) pp.72–76. doi: 10.1109/MC.2017.4451227.
2. Oltsik, J. (2019). *The Life and Times of Cybersecurity Professionals 2018*. Research Report. Enterprise Strategy Group and Information Systems Security Associate, April 2019. https://www.esg-global.com/hubfs/pdf/ESG-ISSA-Research-Report-Life-of-Cybersecurity-Professionals-Apr-2019.pdf.
3. $(ISC)^2$. (2019). *Strategies for Building and Growing Strong Cybersecurity Teams: (ISC)2 Cybersecurity Workforce Study, 2019*. https://www.isc2.org/-/media/ISC2/Research/2019-Cybersecurity-Workforce-Study/ISC2-Cybersecurity-Workforce-Study-2019.ashx.
4. Furnell, S. and Bishop, M. (2020). "Addressing cybersecurity skills: The spectrum not the silo", *Computer Fraud & Security*, February 2020.
5. $(ISC)^2$. (2018). *Cybersecurity Professionals Focus on Developing New Skills as Workforce Gap Widens: $(ISC)^2$ Cybersecurity Workforce Study 2018*. https://www.isc2.org/-/media/ISC2/Research/2018-ISC2-Cybersecurity-Workforce-Study.ashx.
6. Infosec. (2018). "Top 10 Skills Security Professionals Need to Have in 2018", 17 August 2018. https://resources.infosecinstitute.com/top-10-skills-security-professionals-need-to-have-in-2018/#gref
7. ISACA. (2019). *State of Cybersecurity 2019 - Part 1: Current Trends in Workforce Development*. https://cybersecurity.isaca.org/state-of-cybersecurity
8. Symantec. (2019). *High Alert: Tackling Cyber Security Overload in 2019*. Symantec Corporation. https://resource.elq.symantec.com/LP=7421
9. Dawson, J. and Thomson, R. (2018). "The Future Cybersecurity Workforce: Going Beyond Technical Skills for Successful Cyber Performance", *Frontiers in Psychology*, 12 June 2018. https://www.frontiersin.org/articles/10.3389/fpsyg.2018.00744/full
10. CSEC2017 Joint Task Force. (2017). *Cybersecurity Curricula 2017 – Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity*. Version 1.0 Report 31 December 2017. Association for Computing Machinery (ACM), IEEE Computer Society (IEEE-CS), Association for Information Systems Special Interest Group on Information Security and Privacy (AIS SIGSEC) and International Federation for Information Processing Technical Committee on Information Security Education (IFIP WG 11.8). https://cybered.hosting.acm.org/wp-content/uploads/2018/02/newcover_csec2017.pdf
11. CIISec. (2019). *CIISec Skills Framework,* Version 2.4, Chartered Institute of Information Security, November 2019. https://www.ciisec.org/CIISEC/Resources/Capability_Methodology/Skills_Framework/CIISEC/Resources/Skills_Framework.aspx

12. Rashid, A., Chivers, H., Danezis, G., Lupu, E. and Martin, A. (2019). *The Cyber Security Body of Knowledge*. Version 1.0, 31 October 2019. https://www.cybok.org/media/downloads/cybok_version_1.0.pdf
13. (ISC)². (2019). *The (ISC)² CBK*. https://www.isc2.org/Certifications/CBK (accessed 1 April 2020).
14. ISO/IEC. (2013). *Information technology — Security techniques — Code of practice for information security controls*. International Standard ISO/IEC 27002. Second edition 2013-10-01. International Organization for Standardization and International Electrotechnical Commission.
15. Newhouse, B., Keith, S., Scriber, B. and Witte. G. (2017). *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework*. NIST Special Publication 800-181. August 2017. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf
16. NSA. (2019). *CAE-CD 2020 Knowledge Units*. CAE Requirements and Resources. http://www.iad.gov/NIETP/documents/Requirements/CAE-CD_2020_Knowledge_Units.pdf (accessed 1 April 2020).
17. Hallett, J., Larson, R. and Rashid, A. (2018). "Mirror, Mirror, On the Wall: What are we Teaching Them All? Characterising the Focus of Cybersecurity Curricular Frameworks", in *2018 USENIX Workshop on Advances in Security Education*.
18. Furnell, S., K, M., Piper, F., E2, C., H2, C. and Ensor, C. (2018). "A National Certification Programme for Academic Degrees in Cyber Security", in T*owards a Cybersecure Society: Education and Training*. L.Drevin and M.Theocharidou (eds.), IFIP Advances in Information and Communication Technology, Springer, pp133-145.
19. The CAE in Cybersecurity Community. (2020). *CAE Institution Map*. https://www.caecommunity.org/content/cae-institution-map (accessed 1 April 2020).
20. Indiana University Center for Postsecondary Research. (2018). *The Carnegie Classification of Institutions of Higher Education*. https://carnegieclassifications.iu.edu/index.php (accessed 1 April 2020).