Mirror, Mirror, On the Wall: What are we Teaching Them All? Characterising the Focus of Cybersecurity Curricular Frameworks

Joseph Hallett
University of Bristol

Robert Larson
University of Bristol

Awais Rashid
University of Bristol

Abstract

Many cybersecurity curricular frameworks exist, but are they all equal? If a student takes a course based on one framework, what should they expect to get out of it? Different frameworks have different emphasis and will shape the courses implementing them leading to varying skill sets. This is not bad, but such biases should be clear. The Cybersecurity Body of Knowledge (CyBOK) is a broad guide to foundational cybersecurity knowledge developed through consultation with industry and academia. Using the knowledge areas from CyBOK as a basis for comparison, we characterise 4 curricular frameworks and find that different frameworks have different emphasis, and that not all frameworks cover all cybersecurity topics.

1 Introduction

Cybersecurity is increasingly taught as its own speciality. In order to aid teaching, various organisations and professional bodies have designed their own cybersecurity curricular frameworks to guide Universities and professional organisations when implementing their courses.

While many curricula frameworks agree on a rough set of topics within cybersecurity, the frameworks differ on the emphasis of the topics (i.e. the attention given to each topic over the entire curriculum). The differences in emphasis are not stated explicitly, making comparisons between the frameworks tricky as the analysis requires a full understanding of the text. One cannot trivially see what content one curricular framework includes and what another framework ignores.

Knowing the emphasis of a curricula framework lets companies assess a prospective employee's certifications against the company's needs. It helps students make informed choices about the courses they take. It allows course designers to understand which certification to tailor their courses to and which to recommend to students for post-graduate study [10].

To analyse the different curricular frameworks we need a foundational underpinning to act as the basis for any comparisons we make. The CyBOK project aims to codify foundational cybersecurity knowledge into 19 top-level knowledge areas and 5 broad categories [21]. CyBOK captures the foundational knowledge that underpins cybersecurity—identified through a series of consultations with researchers and practitioners. Given its broad foundational focus CyBOK provides a common basis to compare the different curricular frameworks.

By mapping the topics and knowledge units of four cybersecurity curricular frameworks onto the CyBOK knowledge areas, we can capture the emphasis each framework places on each of the CyBOK knowledge areas and categories. We can use this weighting to compare the different frameworks and assess how balanced each is, as well as explore what skills cybersecurity certifications are teaching students more generally.

This paper makes the following contributions:

- We map onto CyBOK knowledge areas several curricular frameworks topics.

  Specifically we look at the curricular frameworks from: the Institute of Information Security Professionals (IISP), the Joint Task Force on Cybersecurity Education (JTF), the National Initiative for Cybersecurity Education (NICE) and the National Cyber Security Centre (NCSC).

- A preliminary analysis of the curricular frameworks based on the number of CyBOK knowledge areas they cover, identifying areas of focus and overlooked topics in each curricular framework.

- We look at where cybersecurity curricular frameworks as a whole place their emphasis, and note that the most emphasised areas are not necessarily the most important.

Category	Knowledge Area
Attacks & Defences	Adversarial Behaviours Forensics Malware & Attack Technologies Security Operations & Incident Management
Human, Organisational & Regulatory Aspects	Human Factors Law & Regulation Privacy & Online Rights Risk Management & Governance
Infrastructure Security	Network Security Hardware Security Cyber-Physical Systems Security Physical Layer Security
Software & Platform Security	Software Security Web & Mobile Security Secure Software Design & Development
Systems Security	Cryptography Operating Systems & Virtualisation Security Distributed Systems Security Authentication, Authorisation & Accountability

Table 1: Overview of the 19 CyBOK knowledge areas and their categories.

2 The Problem

As cybersecurity has become more prevalent, there is an increasing need to produce certifications to assess people's cybersecurity competency. To help guide these certifications, several professional, academic, and governmental organisations have produced curriculum guidelines. We refer to these collectively as *curricular frameworks*. These frameworks exist to aid curriculum designers in understanding the requirements for cybersecurity disciplines and to define the topics and themes within cybersecurity that the framework authors consider fundamental.

While many of the curricular frameworks would seem to agree on the fundamental cybersecurity topics, the emphasis given to each topic varies from framework to framework. Cybersecurity topics cover a range of social, technical and legal themes. Even within the technical theme, cybersecurity topics cover aspects of software, hardware, network and distributed system engineering—each of which have been, historically, different disciplines. Understanding the different focus each curricular frameworks places on the cybersecurity topics helps educators assess on which framework to base their curricula. Equally, for employers, understanding what topics a certification emphasises can help them assess a prospective employee's suitability for a job [1].

The CyBOK project aims to collect, and serve as a reference to, the foundational knowledge of cybersecurity [20]. Inspired by the SWEBOK project [2], CyBOK in intended to act as a guide to the body of cybersecurity knowledge and show where existing literature (such as books, research, standards and technical reports) explain cybersecurity topics. It was developed both through community consultation [21] and by analysing existing textbooks, conferences and certification programs. Through consultation with industrial and academic specialists as well as analysis of various texts [21], CyBOK identified 19 top-level knowledge areas grouped into 5 broad categories (Table 1).

As a guide to cybersecurity topics, CyBOK can be used as the basis for comparisons between different cybersecurity curricular frameworks. For each curricular frameworks we map its topics and learning outcomes onto CyBOK knowledge areas. If, in one curricular frameworks, more topics are mapped to a single CyBOK knowledge area than in an alternative framework then we can say that *the first framework emphasises that knowledge area*.

Using the CyBOK knowledge areas lets us summarise the content of the curriculum in terms of discrete categories. As well as giving a snapshot of the curriculum content, the summaries let us make comparisons between different curricular frameworks without having to rely on textual descriptions. If one curriculum only has topics in a few knowledge areas and another curriculum has topics in many knowledge areas then we can identify that the first curriculum is more specialised and the second is broader. If one curriculum contains topics associated with more technical knowledge areas (such as those in the *systems, infrastructure and software and platform security* categories), whereas another looks more at the *human and regulatory aspects* then we can see which curricula are more suitable for an engineer, and which are more suitable for a lawyer.

Finally, by mapping the topics in several curricular frameworks onto CyBOK knowledge areas we can gain insight into the relative importance of each knowledge area (in the context of cybersecurity education). All knowledge areas are important in the right context, but if cybersecurity curricula *as a whole* are consistently referring to more topics from a few knowledge areas then this suggests more generally what skill a cybersecurity certification teaches.

3 Related Work

Tracking cybersecurity curricular frameworks's content is important as it lets us know what they include within them, and what they do not. Rowe et al. identified that, in an academic context, there were several aspects of cybersecurity that were not being taught by standard computer science curricula [23]. Sobiesk et al. has called for greater breadth in cybersecurity education [25] and Yue has discussed integrating cybersecurity topics with non-security units to help increase the general understanding of cybersecurity altogether [27].

As well as assessing the contents of the frameworks we need to assess how effectively we teach the existing topics. Sherman et al. described a framework for measuring how cybersecurity education has improved [24]. Mirkovic et al. proposed a 5-step process for evaluating how effective capture-the-flag competitions were at teaching cybersecurity lessons to students, by developing evaluation questions to ask to students and a systematic approach to collecting their responses [13]. Knowles et al. looked at how we examine existing curricular frameworks [11]; they found that despite multiple choice exams being a part of 81% of the curricular frameworks they looked at, they were the least effective way to assess cybersecurity competency (with the most effective being oral, or in-lab examination and qualification review).

CyBOK is a new attempt to define a body of knowledge for cybersecurity [20] but there have been earlier bodies of knowledge defined for cybersecurity. Crowley proposed Common Body of Information Systems Security Knowledge [7], Cooper et al. described an information assurance body of knowledge with many similar knowledge areas to CyBOK [5], the US Department of Homeland Security proposed a software assurance body of knowledge [22], and the National Security Telecommunications and Information Systems Security proposed a body of knowledge for information security professionals [14].

Some other studies have also looked at the differences between various curricular frameworks. Cooper et al. provided an overview of various information assurance curricular frameworks and gave a high-level comparison of them, but didn't examine their contents [6]. Knapp et al. took several university curricula and mapped the learning topics to 4 different curricular frameworks's exams to see how universities could prepare their students for professional exams later in their careers [10].

4 Analysed Curricular Frameworks

This paper looks at the following 4 curricular frameworks:

- The IISP Knowledge Framework [8]
- The JTF Cybersecurity Curriculum [3]
- The NICE Cybersecurity Workforce Framework (NIST SP 800–181) [17]
- The NCSC Certified Master's in Cyber Security [15]

The IISP Framework aims to define what knowledge professionals need to work in cybersecurity. It is developed by the Institute of Information Security Professionals, a British non-profit professional organisation, and as well as being used for their own certification, the IISP Framework (together with the IISP Skills Framework [9]) is used as the basis for the NCSC Certified Professional (CCP)—a professional certification for people working in information assurance.

On top of the CCP the NCSC is also developing their own Certified Master's program. Unlike the CCP which is for people already working in cybersecurity, the NCSC Certified Master's is an accreditation for academic degree programs. It defines several pathways for cybersecurity and digital forensics degrees that each describe what content must be covered and to what depth throughout the degree program. However, in this paper we have chosen to look exclusively at the cybersecurity pathways as the digital forensics pathways are focused on just one knowledge area. As of 2018, only 14 degree programs have been fully certified [16].

The NICE Framework aims to categorise and describe the tasks and skills needed to do cybersecurity jobs [19]. It defines long lists of tasks, knowledge, skills and abilities (KSAs), and using these lists defines jobs roles and specialism in terms of which of the KSAs they include. Training and career progression is described as the new tasks and KSAs someone needs to take on and learn, making the NICE Framework rather prescriptive, compared to the other curricular frameworks.

The JTF Curriculum is a collaboration between the ACM, IEEE Computer Society, AIS SIGSEC and IFIP to develop curricula guidance for academic institutions that matches industrial need. It was developed from multiple sources (including the NICE Framework). It defines a body of knowledge over 8 knowledge areas (each with their own topics) and 6 *cross-cutting concepts* (which define connections between the knowledge areas). Unlike the NICE Framework, which defines precisely as a verbose list what each knowledge area contains, the JTF Curriculum breaks the knowledge areas down into units and topics before describing roughly what each topic contains.

5 Mapping onto CyBOK Knowledge Areas

To produce a mapping from a curricular framework to the CyBOK knowledge areas, we examined each framework to find its smallest *unit*. Each unit was mapped, if appropriate, to a single CyBOK knowledge area. The sum total of each of the CyBOK knowledge areas is used as a measure of the relative emphasis a framework gives to any particular topic.

For example, in the NCSC Certified Master's curricular framework the framework is split into nine *security disciplines* each with one or more *skills groups* and each skills group with multiple *indicative topics*. For the NCSC Certified Master's each indicative topic was mapped to a CyBOK knowledge area. Alternately in the case of the JTF Curriculum, the curriculum is split into eight *knowledge areas*, each with multiple *knowledge*

Curricular Framework	Mapped/Total	Mapped Percentage
IISP	215/252	85%
JTF	286/287	100%
NICE	206/630	33%
NCSC	114/118	97%

Table 2: Summary of the extent of mapping curricular frameworks to CyBOK knowledge areas.

units and each unit containing multiple *topics*. In this case we mapped each of the topics to a CyBOK knowledge area.

Figure 1 summarises the structure of each of the different curricular frameworks. Each curriculum is structured with top-level areas each containing smaller, more focused, areas. These smaller areas contain even smaller area, and so on until they break down to single learning outcomes or topics that specify a single cybersecurity idea. For each of these topics we map them to (typically) a single CyBOK knowledge area.

The sum total of the mapped knowledge areas is used to characterise the curriculum. For example if 20% of one curriculum's topics are mapped to the *Forensics* knowledge area, and only 5% of another course's topics are mapped to the Forensics knowledge area, then we would say that the first curriculum places a greater emphasis on Forensics than the second. This approach is not without its limitations—we do not take into account the time any curriculum may allot to a topic, or the depth in which the topic is covered. What it gives us is a metric as to the number of basic topics in each curriculum that fall into a particular CyBOK area.

Assuming all topics are of roughly equal importance, we would expect to see each CyBOK category and knowledge area equally represented. If one or more CyBOK knowledge area or category is over-represented then this may indicate an area which the curriculum emphasises more than other security areas.

To produce the mapping to CyBOK knowledge areas we examined the course's topic and compared it to each CyBOK knowledge area in the CyBOK scope document [20]. For most topics the mapping is fairly trivial. For example the IISP Knowledge Framework lists as a learning outcome for Skill Area A6.1 [8]:

> *"They shall be able to list the major applicable legislation and regulations affecting an example organization and describe their overall purpose."*

The CyBOK scope document states under the *Law and Regulation knowledge area* that this area looks at:

> *"International and national statutory and regulatory requirements, compliance obligations including data protection..."*

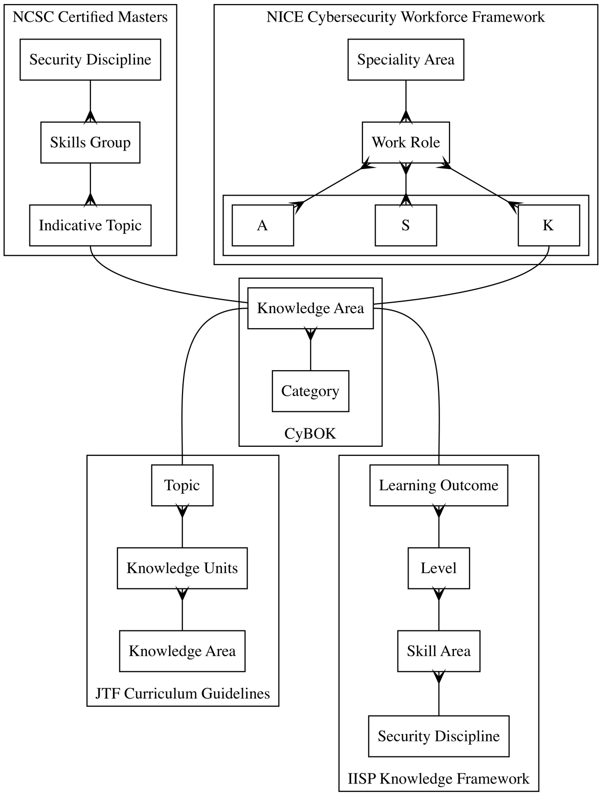

Figure 1: Mappings of the curricular framework subdivisions onto CyBOK. Straight arrow heads indicate a *to one* mapping. Forked arrowheads indicate a *to many* mapping.

This learning outcome is therefore mapped to the Law and Regulation knowledge area.

We used our best judgement for topics that didn't map neatly onto CyBOK. In some cases it was not possible to map subjects onto CyBOK knowledge areas, as the topics were too general or outside of the CyBOK scope. For example, in the NICE Framework, to meet K0015 the student should have:

> *"Knowledge of computer algorithms."*

The CyBOK knowledge areas look at cybersecurity principles and not more general software engineering ones (such as those covered by the SWEBOK project [2]). No mapping to CyBOK was made for K0015.

Table 2 summarises the number of mapped topics and the extent to which the topics, within the curricular frameworks, could be mapped onto the CyBOK knowledge areas. For the IISP Framework, JTF Curriculum and NCSC Certified Master's curricular frameworks most topics within them could be mapped on to CyBOK knowledge areas, however only a third of the NICE Framework

Curricular Framework	Total	Cohen's κ
IISP	25	0.90
JTF	28	0.81
NICE	63	0.85
NCSC	11	0.70
Overall	127	0.86

Table 3: Inter-rater reliability in producing the mapping for each curricular framework.

K's can be mapped to CyBOK knowledge areas. This is because the NICE Framework contains many topics outside of the scope of CyBOK. The NICE Framework includes many topics which relate to basic computer science topics, such as knowledge of algorithms or databases, which are not part of CyBOK. It also includes topics such as physical security (such as locking cabinets), and intelligence gathering (outside of a cybersecurity theme) that are also not in scope of CyBOK. The NICE Framework is also larger (in terms of topics) than the other curricular frameworks. Though the percentage of mapped topics is low, the total number of mapped topics is still over 200 and comparable to the other curricular frameworks.

Though we have tried to be consistent and rigorous when producing our mappings from curricular frameworks onto CyBOK knowledge areas, there is always some subjectivity when deciding to which knowledge area a topic belongs. The mapping we have produced represents a *first attempt* at tying these curricular frameworks to CyBOK.

To verify how consistent the mapping was we extracted 10% of the topics from each syllabus (selected at regular intervals) and had a separate author redo the mapping. The mappings were compared and Cohen's κ calculated. The results (in Table 3) indicate that our mapping is reasonable and that there was strong to fair consensus on the mappings.

6 Results

Figure 2 shows radar plots of the relative emphasis that each curricular frameworks places on the CyBOK categories. If each category was equally weighted in the curricular frameworks, then we would expect to see a pentagon with all points on the grey inner circle. Instead, we see that all curricular frameworks place a greater emphasis on the Human Organisational & Regulatory aspects. The JTF Curriculum seems the most balanced, giving a similar weighting to all CyBOK security categories, whereas the IISP Framework appears to effectively ignore any infrastructure or systems security aspects instead focusing predominantly on attack and defence as well as human aspects and to a lesser extent software security.

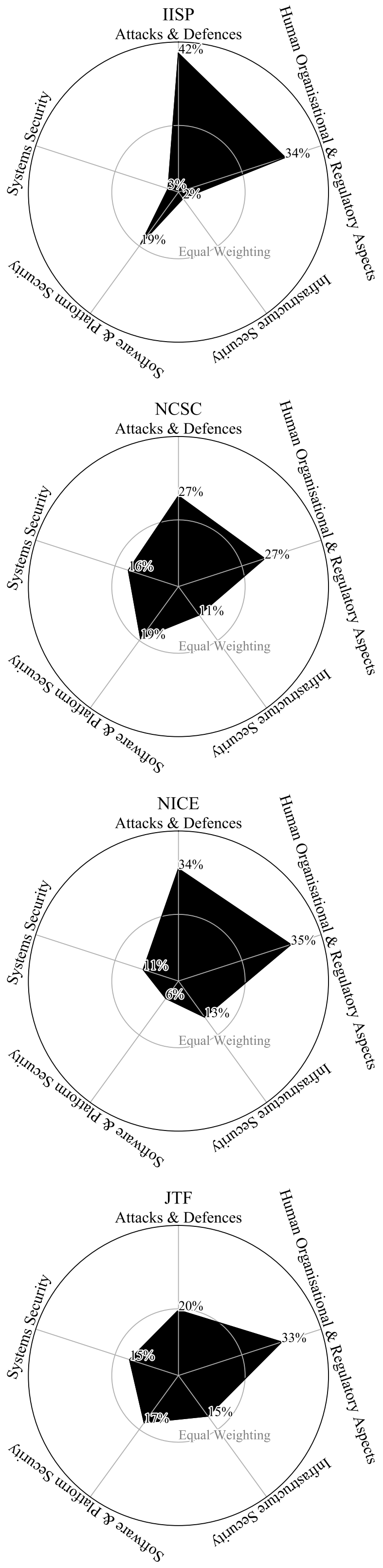

Figure 2: Relative emphasis of each CyBOK category for each of the curricular frameworks.

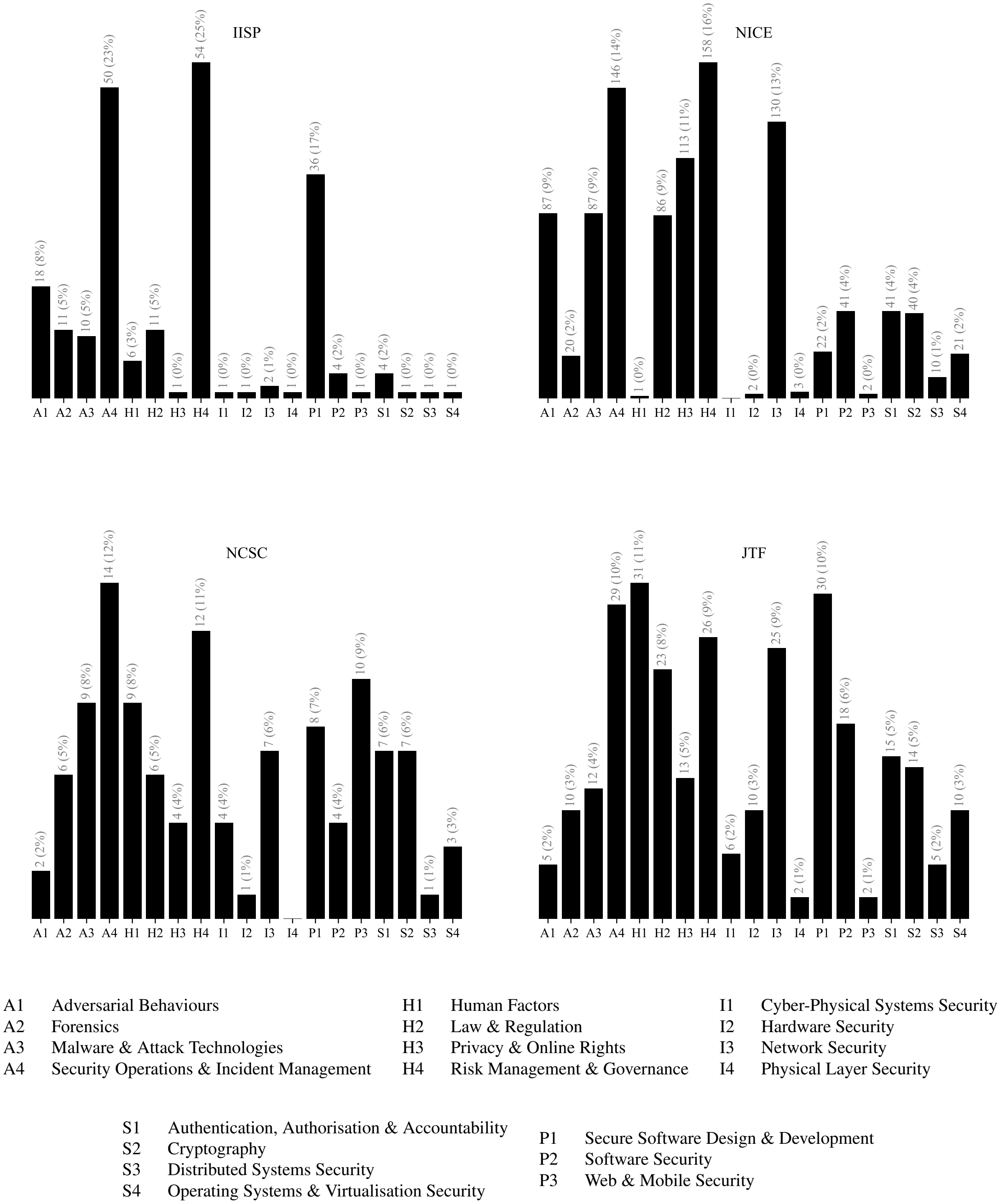

Figure 3: Count of the number of mappings to CyBOK knowledge areas in each curricular framework. Absolute values (and percentages) for the mapped topics are shown atop the bars.

The NCSC Certified Master's and NICE Framework are also similar to the JTF Curriculum, albeit with less emphasis on software security and a greater emphasis on the attack and defense aspects.

Breaking the curricular frameworks down to the individual knowledge areas (Figure 3), we can see that not only is the IISP Framework focused on only the *attacks & defences*, *human aspects* and *software security* CyBOK categories, but that 1 knowledge area in each category dominates: *security operations*, *risk management* and *secure software design* respectively. The other cybersecurity knowledge areas, especially the more technically focused areas, are covered minimally if at all. The IISP Framework appears to define a specialist curriculum for those interested in those specific knowledge areas, rather than a more general curriculum.

The NICE Framework fares better with topics covering most CyBOK knowledge areas, however there are still gaps: physical hardware-based knowledge areas, such as *cyber-physical systems, hardware* and *physical layer* security do not seem to be covered, along with the *human factors* and *web and mobile* security knowledge areas.

The JTF Curriculum contains content associated with all the CyBOK knowledge areas. This suggests that it covers a broad range of topics. The NCSC Certified Master's, while appearing to be broader than the IISP Framework, appears to have inherited the IISP Framework's emphasis on *risk management* and *security operations*, with spikes of topics mapped to those knowledge areas.

With the mapping made, we can start to ask questions about the relative importance of individual CyBOK knowledge areas themselves. If curricular frameworks are referring to (on average) more topics in certain knowledge areas, then this may act as a guide to what knowledge is possessed, in general, by someone with a cybersecurity certification. It also acts as a simple check that cybersecurity curricular frameworks are teaching what we expect: if the overall emphasis is surprising to us then we may need to re-evaluate the curricular frameworks to make sure that what we're teaching is what we need.

Figure 4 shows the median emphasis (normalised number of mappings in each curricular frameworks) for each knowledge area over all 4 curricular frameworks. Though this is only looking at a relatively small number of curricular frameworks, it is interesting to note that *risk management* and *security operations* are emphasised significantly more by these 4 curricular frameworks. In contrast, it is the knowledge areas with a greater engineering emphasis, *cyber-physical systems, hardware security, web and mobile security, distributed systems* and *operating system security* that appear to be under-emphasised.

The lack of emphasis in the more technical knowledge areas is surprising as a study into the core concepts of cybersecurity identified secure programming, operating system security and the ability to root trust in hardware as being among the most important cybersecurity concepts [18] yet the knowledge areas which contain these topics are comparatively less emphasised compared to the legal and operational aspects which were all ranked as being of lesser importance.

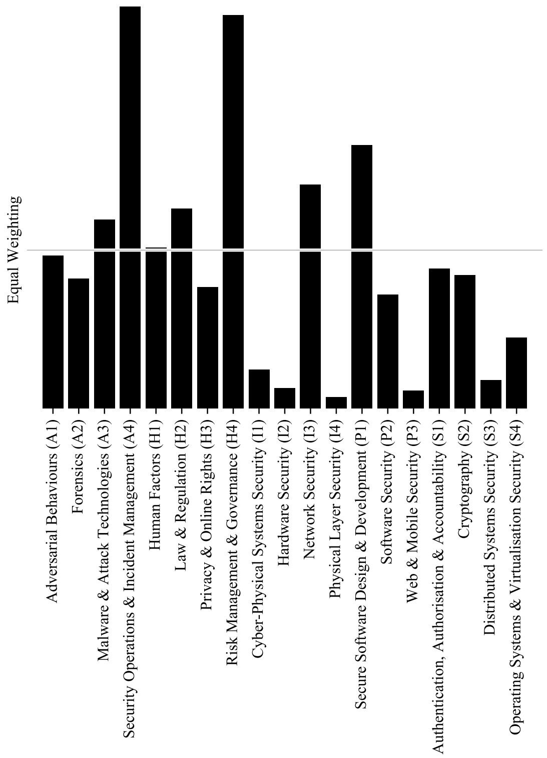

Figure 4: Median emphasis (as percentage of curriculum topics) placed on each CyBOK knowledge area over the 4 curricular frameworks.

Recruitment for cybersecurity skills is considered hard—in particular in a survey of companies recruiting for people with technical cybersecurity skills, finding people with skills in implementing secure systems was reported as being the most difficult [26]. One suggested explanation for the shortage of cybersecurity professionals is a lack of up-to-date, relevant or practical cybersecurity content in training materials and degree curricula [4]—our mappings would seem to support this view: the technical engineering knowledge required to learn these skills does not appear to be covered by current cybersecurity curricular frameworks.

7 Discussion

Using the CyBOK knowledge areas we are able to characterise where the curricular frameworks place their emphasis and identify knowledge areas which the frameworks focused on as well as the knowledge areas some of the frameworks ignored.

This allows us to see when curricular frameworks are not as broad as they might be. In particular almost exclusive emphasis in the IISP Framework placed on *risk management*, *operations* and *secure development* suggests that it is not a general cybersecurity curriculum. Even the NICE Framework appears to lack coverage of some cybersecurity knowledge areas. In contrast the JTF Curriculum, and to a lesser extent NCSC Certified Master's curricular frameworks, are broader and cover a wider range of cybersecurity topics.

This is early work. We have mapped the topics in the curricular frameworks onto the CyBOK knowledge areas, but we do not know how much of each knowledge area is covered by the topics. Broadly, we know how many different topics we mapped in each curriculum mapped to each knowledge area but we don't know in what depth the curricula cover them. Depth, especially practical experience, is important for education programs as there is evidence that cybersecurity skills cannot be mastered without it [12]. When describing emphasis, we do not account for the time the frameworks allocate to individual topics, just the number of them. Future work should look to study implementations of these frameworks to see how emphasis within courses varies from the frameworks they are based on.

We have not yet analysed whether there are topics within an individual knowledge area that are not being covered or whether there are topics mapped to certain knowledge areas that are not *currently* part of that knowledge area's subjects. The inter-rater reliability metrics we calculated suggest at least that there is some consistency in what *should* be mapped to each knowledge area, and the CyBOK knowledge areas can be updated as technology and needs change.

CyBOK is a new body of knowledge under active development and the knowledge areas within it are themselves not well-defined. We have textual, natural language description of the topics within each knowledge area as part of the CyBOK scope document [20], but we lack a prescriptive list of topics that each area contains. One approach to generating the list of topics for each knowledge area could be to use the curricular frameworks we have already mapped and build the list of topics based on what has already been mapped, perhaps using natural language analysis to extract keywords and build hierarchical clusters within knowledge areas.

As part of this initial mapping work we have looked at 4 curricular frameworks but others also exist (such as the (isc)^2 CISSP or EC-Council CEH programs) that could be mapped and analysed. One approach to mapping these curricular frameworks would be to train a machine-learning model with our current mapping and then try to map the new curricular frameworks automatically based on the curriculum description and topics. This would not only speed the mapping process up but given an arbitrary cybersecurity-focused document we could map keywords to CyBOK knowledge areas and generate references to the cybersecurity documentation in CyBOK, which may help with reading comprehension. We could also assess which knowledge areas the document leans towards, which may provide a useful summary.

This paper attempts to characterise what we are teaching through the existing cybersecurity curricular frameworks. Using the CyBOK knowledge areas as a basis for comparison, we can say that it depends on which curricular frameworks one is following but that generally it involves teaching risk management, security operations with some software security and attack technologies. Looking at individual curricular frameworks we see that some frameworks (in particular the IISP Framework) are far narrower in their scope than the others—and that whilst most of the frameworks are touching on most of the topics we would expect them to cover, the more technical areas are less emphasised in these curricular frameworks than we might expect.

8 Conclusions

We started this paper asking if all curricular frameworks were equal: *no*—just by looking at the topics each framework includes we can see differences in emphasis between them, and in some cases entire knowledge areas that are not covered. We also ask what a student taking a course based on a curricular framework might expect to get out of it—our diagrams in Figures 2 and 3 may help describe the emphasis within the course, but won't say the precise topics.

So which curricular framework is best? Further work is needed to decide if one curricular framework is the fairest of them all.

9 Acknowledgements

The CyBOK project is sponsored by the National Cyber Security Programme in the UK.

10 Availability

The mappings between each of the curricular frameworks and the CyBOK knowledge areas are available online, as well as the scripts to generate all figures:

`https://www.cybok.org/static/cybok/media/mirrormirror.zip`

References

[1] Bishop, M., and Frincke, D. Academic Degrees and Professional Certification. *IEEE Security & Privacy* (2004).

[2] Bourque, P., and Fairley, R. E., Eds. *Guide to the Software Engineering Body of Knowledge*. No. 3.0 in SWEBOK. IEEE, 2014.

[3] Burley, D. L., Bishop, M., Buck, S., Exstrom, J. J., Futcher, L., Gibson, D., Hawthorne, E. K., Kaza, S., Levy, Y., Mattord, H., and Parrish, A. Cybersecurity Curricula 2017. Report, Computing Curricula Series Joint Task Force on Cybersecurity Education, 2017.

[4] Caldwell, T. Plugging the cyber-security skills gap. *Computer Fraud & Security* (2013).

[5] Cooper, S., Nickell, C., Pérez, L. C., Oldfield, B., Bryneilsson, J., Gökce, A. G., Hawthorne, E. K., Klee, K. J., Lawrence, A., and Wetzel, S. Towards information assurance (IA) curricular guidelines. In *Annual Conference on Innovation and Technology in Computer Science Education* (2010).

[6] Cooper, S., Nickell, C., Piotrowski, V., Oldfield, B., Abdallah, A., Bishop, M., Caelli, B., Dark, M., Hawthorne, E. K., Hoffman, L., Pérez, L. C., Pfleeger, C., Raines, R., Schou, C., and Brynielsson, J. An exploration of the current state of information assurance education. *ACM Special Interest Group on Computer Science Education Bulletin 41*, 4 (Jan. 2010).

[7] Crowley, E. Information System Security Curricula Development. In *Proceedings of the 4th Conference on Information Technology Curriculum* (2003).

[8] IISP. IISP Knowledge Framework. Report, IISP, 2017. https://www.iisp.org/imis15/iisp/About_Us/Our_Knowledge_Framework/iisp/About_Us/Our_Knowledge_Framework.aspx?hkey=6e8644f9-fc2f-4f53-9784-b0fb2dba5e8b.

[9] IISP. IISP Skills Framework. Report, IISP, 2017. https://www.iisp.org/imis15/iisp/About_Us/Our_Skills_Framework/iispv2/Accreditation/Our_Skills_Framework.aspx?hkey=e77a6f03-9498-423e-aa7b-585381290ec4.

[10] Knapp, K. J., Maurer, C., and Plachkinova, M. Maintaining a Cybersecurity Curriculum: Professional Certifications as Valuable Guidance. *Journal of Information Systems Education* (2017).

[11] Knowles, W., Such, J. M., Gouglidis, A., Misra, G., and Rashid, A. All That Glitters Is Not Gold: On the Effectiveness of Cyber Security Qualifications. *IEEE Computer* (2017).

[12] Manson, D., and Pike, R. The Case for Depth in Cybersecurity Education. *ACM Inroads* (2014).

[13] Mirkovic, J., Dark, M., Du, W., Vigna, G., and Denning, T. Evaluating Cybersecurity Education Interventions: Three Case Studies. *IEEE Computer and Reliability Societies* (2015).

[14] Nation Security Telecommunications and Information Systems Security. *Nation Training Standard for Information Systems Security (INFOSEC) Professionals*, 1994.

[15] National Cyber Security Center. *Certified Master's in Cyber Security*, 2017.

[16] NCSC. NCSC-certified degrees. Online, 2018. https://www.ncsc.gov.uk/information/ncsc-certified-degrees.

[17] Newhouse, W., Keith, S., Scribner, B., and Witte, G. National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. Report NIST.SP.800-181, NIST, 2017.

[18] Parekh, G., DeLatte, D., Herman, G. L., Oliva, L., Phatak, D., Scheponik, T., and Sherman, A. T. Identifying Core Concepts of Cybersecurity: Results of Two Delphi Processes. *IEEE Transactions on Education 61*, 1 (2018).

[19] Paulsen, C., McDuffie, E., Newhouse, W., and Toth, P. NICE: Creating a Cybersecurity Workforce and Aware Public. *IEEE Security & Privacy* (2012).

[20] Rashid, A., Danezis, G., Chivers, H., Lupu, E., and Martin, A. Scope for the Cyber Security Body of Knowledge (Version 2.0), November 2017.

[21] Rashid, A., Danezis, G., Chivers, H., Lupu, E., Martin, A., Lewis, M., and Peersman, C. Scoping the Cyber Security Body of Knowledge. *IEEE Security & Privacy* (2018).

[22] Redwine Jr., S. T., Baldwin, R. O., Polydys, M. L., Shoemaker, D. P., Ingalsbe, J. A., and Wagoner, L. D. *Software Assurance: A Guide to the Common Body of Knowledge to Produce, Acquire, and Sustain Secure Software (Version 1.0).* US Dept. of Homeland Security, 2006.

[23] Rowe, D. C., Lunt, B. M., and Ekstrom, J. J. The Role of Cyber-Security in Information Technology Education. In *ACM Special Interest Group on Information Technology Education* (2011).

[24] Sherman, A. T., Oliva, L., DeLatte, D., Golaszewski, E., Neary, M., Patsourakos, K., Phatak, D. S., Scheponik, T., Herman, G. L., and Thompson, J. Creating a cybersecurity concept inventory: A status report on the CATS project. In *Proceedings of the National Cyber Summit* (Huntsville, USA, 2017).

[25] Sobiesk, E., Blair, J., Conti, G., Lanham, M., and Taylor, H. Cyber Education: A Multi-Level, Multi-Discipline Approach. In *ACM Special Interest Group of Information Technology Education* (2015).

[26] Willetts, D. Cyber security skills—business perspectives and govenment's next steps. Tech. rep., HM Government, 2014.

[27] Yue, C. Teaching Computer Science with Cybersecurity Education Built-in. In *USENIX Workshop on Advances in Security Education* (2016).