Department: Head
Editor: Name, xxxx@email

The UK's Cyber Security Degree Certification Programme: A CyBOK Case Study

Lata Nautiyal
University of Bristol, United Kingdom

Awais Rashid
University of Bristol, United Kingdom

Joseph Hallett
University of Bristol, United Kingdom

Ben Shreeve
University of Bristol, United Kingdom

Michael K, Chris E2 and Catherine H2
The National Cyber Security Centre, United Kingdom

***Abstract*—**
The Cyber Security Body of Knowledge (CyBOK) aims to codify common and broadly accepted foundations for cybersecurity as a discipline. CyBOK Version 1.0 was released on the 31st of October 2019 incorporating contributions from 110 expert authors, reviewers and advisors and nearly 1600 comments from wider public reviews from the community. We discuss how CyBOK has since been utilized to develop an updated programme for certifying undergraduate and postgraduate degrees in the UK. We also present a mapping framework showcasing how programme modules can be mapped to this certification to demonstrate that module content aligns with the certification requirements.

IN THE LAST FEW YEARS, cybersecurity has become an essential component in curricula at school, college and university level. With an array of materials available on the topic, educators often find it challenging to identify the foundational materials and authoritative sources to form the basis of academic degree programmes or training courses. Learners, on the other hand, need to

 Published by the IEEE Computer Society

understand the focus of different programmes to identify which may best suit their needs. Cybersecurity contains a wealth of different jobs, roles and specializations. Not all courses would be suited to the needs of a particular cybersecurity job role. For instance, a cybersecurity course offered at one university may predominantly focus on security operations, incident handing and forensics, while another may educate students on secure software development practices. The two cater to very different roles and specializations. Employers, similarly, have a challenge in identifying which courses (and their graduates) may serve the knowledge needs of particular job roles best.

The CyBOK project (https://www.cybok.org) was conceived to address this fragmentation and codify foundational knowledge about the topic. The aim of the project has been to enable a range of use cases—building on a foundational body of knowledge captured through broad community engagement across academia and industry. The aim is to not only provide programme designers with foundational sources and materials—similar to the SWEBOK (https://www.computer.org/education/bodies-of-knowledge/software-engineering)—but also offer a common foundational framework to contrast the focus and depth of coverage of different programmes [2].

CyBOK's scope (Fig. 1) was established through extensive community consultations [1]. This was followed by development of the detailed knowledge area texts for Version 1.0, which forms the basis of the certification case study discussed in this article. CyBOK has since evolved. CyBOK version 1.1, released on 31 July 2021 (https://www.cybok.org/knowledgebase1_1/), includes two new Knowledge Areas: Formal Methods for Security and Applied Cryptography, along with a new version of the Network Security Knowledge Area and some minor revisions to other Knowledge Areas.

Role of CyBOK in curricula

There are other curricular frameworks, qualification-based bodies of knowledge, and training programs that seek to specify what a cybersecurity education program should comprise: for example, the ACM/IEEE/IFIP

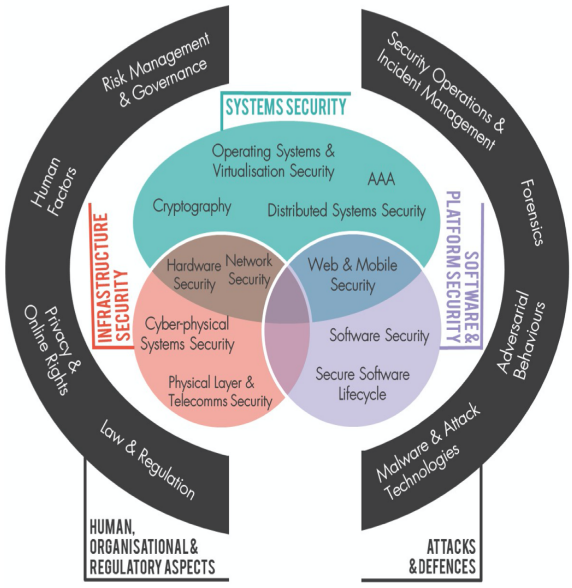


Figure 1: The 19 Knowledge Areas and their categorization within CyBOK Version 1.0

Joint Task Force guidelines for Cybersecurity Curriculum (https://cybered.hosting.acm.org/wp/, professional certifications such as the $(ISC)^2$ Certified Information Systems Security Professional (CISSP) (https://www.isc2.org/Certifications/CISSP) or the Chartered Institute of Informational Security (CIISec) skills framework (https://www.ciisec.org/Skills_Framework).

CyBOK differs in that, rather than specifying a strict curriculum guide, it captures the foundational knowledge on top of which curricular frameworks or specific programmes can build. Consequently, by varying the breadth and depth of coverage, a programme can specialize on specific topics (or offer a broad coverage). At the same time, there is a common framework on the basis of which different curricular frameworks or specific programmes can be contrasted as to what aspects of cybersecurity knowledge they cover and to what depth.

In this article, we discuss this very use case—how a national scale certification programme for undergraduate and postgraduate degrees in the UK has been developed on the basis of CyBOK, and how it enables courses to demonstrate their breadth and depth of coverage.

From a skills-based to a knowledge-based certification framework

The degree certification programme is part of a range of certifications, which the National Cyber Security Centre (NCSC) and its government partners have initiated across UK academia, designed to address the knowledge, skills and capability requirements for cybersecurity education. The certification is a *quality indicator* which is used as a differentiator by prospective applicants and is valued by employers as an indicator that certified degrees produce well-trained graduates. The certification process itself involves an extensive application, submitted by the candidate degrees, and a rigorous review of resulting submissions. Materials reviewed include support of the institution, the team and their expertise, the content of the degree, and topics covered by the modules, as well as assessment materials and dissertations.

There was already an existing NCSC certification programme in place, based on the IISP[1] Skills Framework, with some additions by the NCSC to help make it broader. However, academic degree specifications typically focus on, and express content in terms of, the knowledge to be learnt during the degree. The IISP/CIISec skills framework was created with information security professionals in mind and its focus on a core set of related CyBOK Knowledge Areas bears this out [2]. Whilst the NCSC's augmented version was broader and more general, it was still difficult for universities offering degrees focused on specialized areas in depth – such as Systems Security, Secure Software development or Physical layer and Telecommunications Security – to achieve certification[2].

Furthermore, a degree providing a general foundation in cybersecurity required a minimum of nine of the skills groups to be covered. This approach potentially limited both the flexibility applicants had in their initial application (as they had to ensure that their course content could relate to the specific skills groups), as well as ongoing updates to degree content. A key motivation for moving the certification to CyBOK, therefore, was to improve the flexibility for applicants.

Specifically, we set out to investigate the possibility of developing a CyBOK-based certification scheme that would:

1) allow for courses to differentiate themselves by selecting different topics. We recognized that courses need not cover *identical* material as the range of cybersecurity roles (as well as specialist expertise at academic institutions) would lead to different areas of focus for a course. Courses should be able to demonstrate breadth and depth of coverage to a sufficient degree to achieve certification.
2) enable courses to demonstrate the *claimed* coverage of particular Knowledge Areas (and depth of that coverage).

This is non-trivial as CyBOK Knolwedge Areas are mainly textual documents (as is the case with most bodies of knowledge) with a set of bibliographic references to key source materials. Therefore, we converted each of the Knowledge Areas into a tree, using the structure of the text to mould the topic trees.

CyBOK Knowledge Trees

CyBOK Knowledge Trees provide hierarchical representations of the detailed content covered in the text of each of the Knowledge Areas. More foundational topics form the basis, with specific examples of knowledge and sub-topics being the leaves. For instance, Fig. 2 shows a partial snapshot of the Knowledge Tree for the Software Security KA. The Level 1 node represents the categories of vulnerabilities with level 2 nodes covering particular classes, e.g., memory management, race condition, etc. with their sub-nodes capturing more details relating to these classes of vulnerabilities.

As a quick search mechanism, the knowledge trees provide a means to explore the content of each Knowledge Area. At the same time, by controlling the breadth and depth of topics from a range of knowledge trees, one can develop specific courses or degree programmes covering relevant topics and details. In a similar fashion,

[1] IISP is now CIISec: Chartered Institute of Information Security

[2] We note that content coverage is one element of the certification programme and there are other criteria such as expertise of the team, quality of assessments, etc. which also must be met. A degree may fail to achieve certification even if it meets the content coverage requirement.

Figure 2: Part of the Software Security Knowledge Tree

the trees can serve as a basis to define certification programmes—to specify the coverage of topics and depth expected—as is the case for the NCSC certification use case.

Defining coverage

When defining requirements for coverage we investigated the potential for degree programmes to select a subset of topics from a subset of trees to cover. For example, we would expect a degree specialising in networks and telecoms to choose more topics from the *network security* and *physical layer & telecommunications security* Knowledge Areas compared to one specialising in forensics. Similarly, the former NCSC-certified broad and foundational MSc scheme was aimed at encouraging degrees to cover a wide range of cybersecurity topics. By ensuring degrees select topics from a broader range of Knowledge Areas, one can ensure that the resulting course actually is broad.

We modelled the coverage of different knowledge areas and CyBOK's five broad categories in programmes that were certified under the previous scheme, as well as some that provided good coverage, but could not demonstrate coverage of the certification requirements (the materials were shared by relevant institutions on condition of anonymity). The contrast can be observed in Figure 3. Both programmes are quite broad, however the certified one emphasises *infrastructure security* over *software security*, whereas the uncertified one does the opposite. This gives us a very quick guide to the differences between the two programmes. Of course, using our proposed scheme it is possible to certify many different programmes, as well as summarise the differences between them.

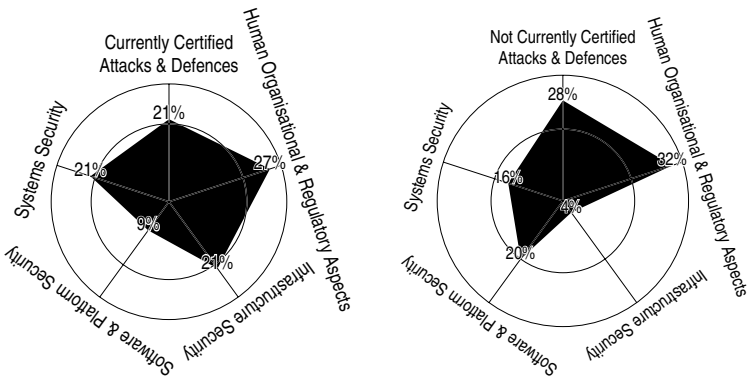
The certification process requires degrees to map their content onto *indicative material*. In the CyBOK-based certification scheme, this indicative material is based on level 2 in the CyBOK Knowledge Trees. So for each Knowledge Area, all the level 1 and level 2 nodes in the tree are used to identify this indicative material. Note that there is no expectation for a programme to cover all of the Knowledge Areas[3] and their indicative material. For instance, for a general broad master's degree programme in cybersecurity, at least 84 taught credits (out of a typical 120 credits) must be mapped to Knowledge Areas 0 to 20. However, this mapping need not provide coverage of all Knowledge Areas, and may also focus on specific topics within a set of Knowledge Areas. One of the biggest tasks in preparing such a certification application is, therefore, to explicitly showcase this mapping to the detailed module specifications, submitted as part of the application. The application requires completion of a pre-defined table to demonstrate this mapping. We, therefore, developed a systematic process to enable programme directors to undertake such a mapping and show how the claimed coverage of indicative material is provided through the modules covering that material.

CyBOK Mapping Framework

The mapping framework requires a list of concepts—typically in the form of keywords or phrases (KWoPs)—that are to be mapped on to the CyBOK-based certification scheme. These KWoPs are derived from module descriptors from a programme specification that represent the concepts covered in the programme material.

As shown in Figure 4, a user starts by looking up KWoPs using an *A-to-Z* of the indicative

[3]The certification also utilises the CyBOK Introduction which covers basic concepts and principles as well as the Knowledge Tree for the Formal Methods for Security Knowledge Area in development; so practically there are 21 Knowledge Areas used in the certification; Knowledge Area-0 (CyBOK Introduction) through to Knowledge Area-20 (Formal Methods for Security)



(a) Currently certified. (b) Not Currently certified.

Figure 3: Coverage of CyBOK broad categories by the two current programmes.

material to identify the relevant Knowledge Area where the content may reside. If there are KWoPs that cannot be mapped using the A-to-Z, the user can utilize the *CyBOK Mapping Reference 1.1*, a reference guide as to where 5087 common cybersecurity terms may find mappings within CyBOK. Any gaps left in the mapping using the Mapping Reference are completed by referring to the Knowledge Trees of the relevant KAs. If there are any further gaps remaining then a *Tabular Representation* summarizing the scope of each Knowledge Area is provided and the user utilizes this to identify the Knowledge Area and peruse the text to conduct the mapping.

Note, that the purpose here is not to do an exact string matching, but rather to identify the topic or sub-topics within a Knowledge Area to which a KWoP is mapped. Furthermore, a sufficient level of subject knowledge is required and expected to undertake the mapping correctly. It is also worth noting that, by design, the main focus of CyBOK is to capture foundational knowledge and it is, therefore, not encyclopaedic. For instance, a KWoP "Writing SNORT Rules" is unlikely to find an exact mapping within CyBOK as writing such rules is a skill. However, the foundational knowledge is covered within the CyBOK Knowledge Area on Security Operations and Incident Management (SOIM) under *analyse: analysis methods* $\rightarrow$ *misuse detection*[4]. There is also knowledge that may be relevant to cybersecurity but not within the direct scope of CyBOK. For instance, "Physical Security" of buildings and facilities is of high importance, but this topic has extensive bodies of knowledge of its own and is out of scope of CyBOK. Hence, other suitable bodies of knowledge and guides should be consulted and such concepts clearly denoted as *Out of Scope* when undertaking any mapping.

An example of the end product (we have omitted several intermediate tables and used a small set of KWoPs for simplifcation) of the mapping process is shown in Table 1.

Evaluating the Mapping Framework and Resources

The certification programme received 22 applications in total (MSc degrees). Two were successful at the original assessment panel, 14 were successful after addressing minor issues identified by the panel and re-submitting, and 6 were unsuccessful. The process from application to certification took two months for those successful at the original assessment panel and four months for those successful after re-submitting.

Prior to the application deadline, we provided various exemplar mappings of modules from UK and US universities (with permission) on our website[5], as well as a webinar and a range of resources (including tables and materials) to assist programme directors with mapping the taught content of their degrees onto CyBOK. One-to-one support from one of the researchers was also offered and eight directors took this up. The researcher maintained notes on the overarching challenges and positives that came up in these sessions.

[4]SNORT is discussed as a specific example in the KA text under misuse detection.

[5]https://www.cybok.org

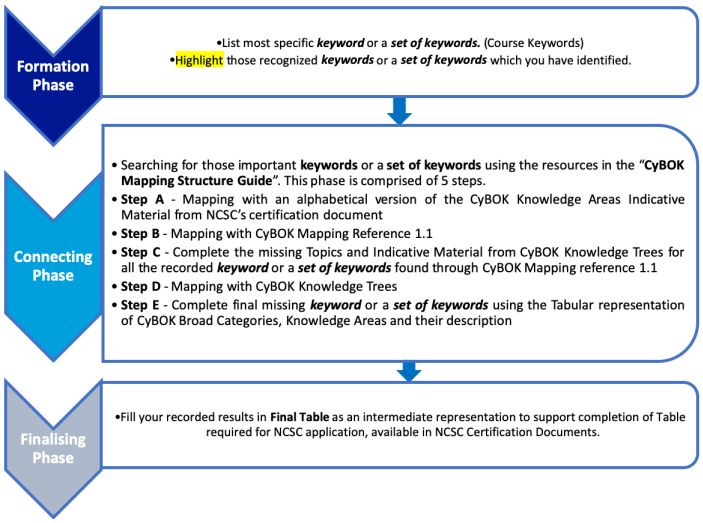


Figure 4: CyBOK Mapping Framework for Mapping University Degree Programmes to NCSC's Certification Requirements

	Broad Category	Knowledge Area	Topic	Indicative Material	Keyword/ Set of Keywords/Course keywords
1	Human, Organisational and Regulatory Aspects	RMG	Risk assessment and management principles	* * *	The business need for security
2	CyBOK Introduction	CI	Foundational Concepts	Objectives of cyber security	Confidentiality, availability, integrity
3	CyBOK Introduction	CI	Foundational Concepts	Definition of cyber security	Components of an information system: Software, hardware, data, people, procedures
4	Software and Platform Security	SSL	Motivations for secure software lifecycle	* * *	System and security development lifecycles
5	Human, Organisational and Regulatory Aspects	RMG	Risk Definition	Risk management	Risk Management terminology
6	Attacks and Defences	AB	Characterisation of Adversaries	* * *	Agents, threats, vulnerabilities
7	Human, Organisational and Regulatory Aspects	RMG	Risk assessment and management principles	Risk assessment and management methods 7	Risk Identification, assessment (quantitative and qualitative)
8	Human, Organisational and Regulatory Aspects	RMG	Risk assessment and management principles	Elements of risk	Risk appetite and residual risk

Table 1: Example Outcome from Mapping (*** indicates that an exact mapping to the indicative material is not found, but the content is covered in the text of the relevant Knowledge Area).

In addition, a separate set of eight interviews was conducted with programme directors who volunteered to participate in a feedback process[6]. The interviews (lasting, on average, 25–45 mins) explored the following key areas:

- Reflections on the new NCSC certification scheme;
- Reflections on the experience of mapping using the mapping resources provided by the CyBOK project;
- The resource which the participants found most useful and why?
- What would the participants change about the mapping resources and why?
- Reflections on what additional resources or support would be useful.

We undertook a thematic analysis of the interviews, identifying eleven themes as shown in Figure 5.

The programme directors described the map-

[6]The study received ethics approval from the University of Bristol, Faculty of Engineering Ethics Committee.

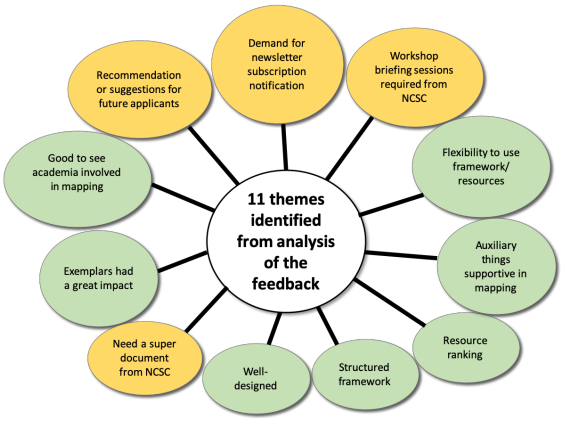


Figure 5: Feedback on the mapping framework and resources: green indicate positives and amber areas of improvement

ping process as very helpful, easy to understand and well designed. The resources and materials provided were also considered useful, easy to use and with a sufficient amount of information. The exemplar mappings were well-received. For instance, one participant noted: *"So, having access to the framework, and not only the framework, I have to say, the example that is given, that made things really, really useful overall."*.

We asked the programme directors to rank the resources provided for the mapping process. Views varied. Some highlighted the tabular representation as most useful. Others found the mapping reference or the visual representations (the knowledge trees) to be most helpful. Some developed their own auxiliary materials, e.g., spreadsheets and tables.

With regards to improvements, some of the programme directors noted that it would be useful to have a template application to be completed (we note that the latest call now includes a template-based application process). Some suggested that one should move in the direction from Knowledge Area to a specific module. Such an approach may be optimal, if the Knowledge Area topic and module content have a close alignment as the search space can be significantly narrowed when mapping KWoPs. However, as modules are rarely so homogeneous, there is a risk that any module content that does not closely align with the Knowledge Area would require a more expensive search across other Knowledge Areas. Participants also called for more workshops and briefing sessions organised by NCSC and one noted the need for a newsletter to stay up-to-date as CyBOK and the certification evolves.

Conclusion

We have presented a major national-level certification programme in the UK based on CyBOK. Our experience shows that a successful rollout of such a knowledge-based certification on a large, national-level, scale is feasible and that it not only improves transparency of the coverage of different programmes, but also makes it possible to demonstrate how their knowledge coverage (breadth and depth) meets the requirements of the certification framework.

Acknowledgements

This work was supported by the UK's National Cyber Security Programme.

REFERENCES

1. A. Rashid, G. Danezis, H. Chivers, E. Lupu, A. Martin, M. Lewis, C. Peersman, "Scoping the cyber security body of knowledge". IEEE security & privacy 16(3),2018, pp. 96-102.
2. J. Hallett, R. Larson, A. Rashid, "Mirror, mirror, on the wall: what are we teaching them all? Characterising the focus of cybersecurity curricular frameworks", Proc. Advances in Security Education Workshop (ASE), USENIX Security Symposium, 2018.

Lata Nautiyal is a Post Doc Researcher at University of Bristol, UK. Contact her at: lata.nautiyal@bristol.ac.uk

Awais Rashid is Professor of Cyber Security at University of Bristol, UK. Contact him at: awais.rashid@bristol.ac.uk

Joseph Hallett is Lecturer in Cyber Security at University of Bristol, UK. Contact him at: joseph.hallett@bristol.ac.uk

Ben Shreeve is a Post Doc Researcher at University of Bristol, UK. Contact him at: ben.shreeve@bristol.ac.uk

Michael K, Chris E2 and Catherine H2 members of the academia team within Cyber Growth at The National Cyber Security Centre, United Kingdom. Contact them at: academia@ncsc.gov.uk