Mapping Foundational Knowledge in Cybersecurity

Kalinka Kaloyanova[1, 2]

[1] Faculty of Mathematics and Informatics
University of Sofia St. Kliment Ohridski
5 James Bourchier Blvd., 1164, Sofia, Bulgaria
[2] Institute of Mathematics and Informatics, Bulgarian Academy of Sciences, Acad. G. Bonchev Str., Block 8, 1113 Sofia, Bulgaria
kkaloyanova@fmi.uni-sofia.bg

Abstract. Various cybersecurity curricular guidelines were announced during the last several years. These are the results from common efforts of many organizations, universities, professional bodies, practitioners, etc. This paper considers fundamental cybersecurity knowledge and its presentation in order to help educators to prepare new educational programs.

Keywords: information security, cybersecurity, curricula, CSEC2017, Cyber Security Body of Knowledge (CyBOK)

1 Introduction

In recent years, many universities have been included cybersecurity as an important element at different levels of their education programs. Various courses and completed programs were developed. They are based on the basic recommendations provided by a number of cybersecurity frameworks and educational guidelines, produced from different professional organizations, academic and practitioners. As different frameworks emphasize different topics, a complex view on the fundaments in cybersecurity is needed. Cyber Security Body of Knowledge (CyBOK), version 1.0, announced at the end of 2019, presents such a comprehensive understanding of foundational cybersecurity knowledge and provide it into several main categories and a number of knowledge areas [1].

In this paper, we discuss the main categories and knowledge areas recognized by CyBOK, and their correspondence to the educational requirements at university level. The last ones are best represented through the CSEC2017 curriculum [3].

2 Cyber Security Frameworks and Guidelines

The most widely accepted standard for information security - ISO/IEC 27000 provides organizations with the basic requirements of how to develop and implement their information security management systems [10]. A lot of major concepts, measures and implementation issues in cybersecurity are discussed in the ISO/IEC 27000 series and could be successfully used in delivering

education in the field [13]. In a number of countries, the development of national cybersecurity programs has begun [14], [16].

Many project and common efforts of different groups of educators, practitioners, national and professional organizations led to the publication of a number of frameworks and guidelines in cybersecurity. Widespread among them are the NICE Cybersecurity Workforce Framework, published by the U.S. National Initiative on Cybersecurity Education (NICE) [12], the National Centers of Academic Excellence in Cyber Defense (CAE-CD) Designation Program Guidance [11], IISP Knowledge Framework [9].

Several cybersecurity curricula were also announced. The Cybersecurity Curricular Guideline CSEC2017 presents the result of the work of several organizations - ACM, IEEE Computer Society, AIS SIGSEC, and IFIP WG 11 [4]. The curriculum recommendations provided here could be used to supplement the established computer science and computer engineering disciplines [3].

The Cybersecurity: A Generic Reference Curriculum is "the result of the work of multinational team of volunteer academics and researchers drawn from 17 nations associated with Partnership for Peace Consortium (PfPC) Emerging Security Challenges Working Group" [5]. The generic guidelines provided by all these documents can be used when particular programs and courses are created for scholars, students and workers.

Among the various cybersecurity frameworks and guidelines, CSEC2017 [3] could be most easily adopted for a university cybersecurity program [11]. First, it is more acceptable for universities due to the close connections with other computing curricula that are periodically defined by ACM (Association for Computing Machinery), IEEE (Institute of Electrical and Electronics Engineers), and AIS (Association for Information Systems) [5]. Second, it provides recommendations using traditional categories like *knowledge areas, knowledge units, topics*, etc.

Due to the rapid development of cybersecurity, the basic knowledge in this field is not well structured, yet. Plenty of books, scientific and white papers, blogs, etc. presents different aspects of the field [8]. It is not easy for teachers, students and even professionals to choose the most appropriate resources that should be used for each specific case, even when they follow curricula recommendations [15], [17].

Cyber Security Body of Knowledge (CyBOK) is trying to fill this gap exploring and systemizing the knowledge obtained from the existing resources (papers, technical documents, standards, reports, etc.) that can assist cybersecurity education. As CyBOK v.1.0 identifies definitions, explanation, examples in cybersecurity area, it complements other curricula recommendations and assists educators in creating new cybersecurity educational units.

3 CyBOK - Cyber Security Body of Knowledge

While most of the above presented documents and frameworks, especially curricula guidelines, aim to develop cybersecurity educational programs, the main goal of the Cyber Security Body of Knowledge (CyBOK) [1] project is to systemize the existing knowledge in the field and to serve as common information resource for these educational programs. To achieve its main goal, the current version – CyBOK v1.0 determines a number of knowledge areas (KA) grouped under the following five categories [7]:

- Human, Organizational and Regulatory aspects;
- Attacks and Defenses;
- Software and Platform Security;
- System Security;
- Infrastructure Security.

All categories consist of four knowledge areas, except Software and Platform Security category, which consists of three.

Security management systems and organizational security controls are the focus of the first category - **Human, Organizational and Regulatory aspects**. Formulating four substantial knowledge areas - Risk Management and Governance, Law and Regulation, Human Factors and Privacy and Online Rights, this category addresses the security issues at the organizational level. Also is addressed the application of instruments like procedures, standards, organizational policies to mitigate risks.

The second category **Attack and Defense** refers to more technical issues and analyses. The technical aspects of computer attacks and malicious software and hardware are discussed in Malware and Attack Technologies knowledge area. The next knowledge area Adversarial Behaviors presents specific aspects of cybercrime such as behavior of the attackers, their motives and methods used and cybercrime relation with economics and society. The technical aspects of operational security (system management, security monitoring) and how to respond to the incident management are covered by Security Operations & Incident Management. The last knowledge area in this category – Forensics, concerns the work with digital evidence of security events and crimes.

Software engineering and security aspects are in the focus of **Software and Platform Security** category. The role of the security in the system development life cycle is marked in Secure Software Lifecycle knowledge area. Specific programming practices leading to security faults and techniques improving software security are the subject of knowledge area Software Security. In addition, particular issues concerning security of web application are Web and Mobile Security.

The **Systems security** category introduce fundamental concepts of cryptography, algorithms, and proof techniques through the Cryptography knowledge area. The other KA - Operating Systems and Virtualization Security presents the protection mechanism to ensure the security at operation systems level. The case security issues of different large-scale distributed systems were discussed in more details the Distributed Systems Security area. The Authentication, Authorization & Accountability knowledge area focuses on the identification management discussing technics and technologies for user identification and user authorization.

Network Security, Hardware Security, Cyber-Physical Systems Security and Physical Layer Security knowledge areas belong to the **Infrastructure security** category. Each of these four knowledge areas cover security issues at different sides of the physical infrastructure – hardware security, different computational devices, networking and telecommunications protocols, etc.

The chosen topics demonstrate not only the breath of scope CyBOK, but also the significant efforts to finding a balance between the more rigorous academic forms and the practical orientation, demanded by the industry.

Despite the presenting variety of topics, this is not the last version of the CyBOK and the process for change requests have already started [2].

4 A Comparison of the frameworks

As the nineteen CyBOK knowledge areas are organized into five categories these categories could be easily used for the correspondence with the eight knowledge areas of CSEC2017 curricula. This comparison is presented in Table 1.

Table 1. CSEC 2017 & CyBOK comparison

CSEC2017 Knowledge areas	**CyBOK 2019 Categories**	**CyBOK 2019 Knowledge areas**
Data security	Attacks and Defences	Malware & Attack Technologies Adversarial Behaviours Security Operations & Incident Management Forensics
System security	Systems security	Cryptography Operating Systems & Virtualisation Security Distributed Systems Security Authentication, Authorisation & Accountability

Software Security	Software and Platform Security	Software Security Web & Mobile Security Secure Software Design & Development
Component security		Security Operations & Incident Management
Connection security	Infrastructure Security	Network Security Hardware Security Cyber-Physical Systems Security Physical Layer Security
Human security	Human, Organizational and Regulatory Aspects	Human Factors Law & Regulation Privacy & Online Rights Risk Management & Governance
Organizational security		
Societal security		

Even at such high-level, the parallel, presented in Table 1, demonstrates that CyBOK categories and knowledge areas could be successfully used as a basis for comparison with CSEC 2017 knowledge areas [3].

As the CSEC2017 knowledge areas are further broken down into knowledge units, these units could be used for the next step of the compliance. The topics in CSEC2017, present more detailed pieces of knowledge (Attacks, Malware, Forensics, Cryptography, etc.) and they could be used for finding correspondence within the content of CyBOK knowledge areas. In some cases, the CSES2017 essentials, listed at the beginning of each KA could be used to find parallels, as they present the essential concepts presented in units and modules.

We applied this approach in the case of CSEC2017 knowledge area Component Security - it does not match directly to any of the CyBOK categories. Instead, we could find the correspondence with the Security Operations & Incident Management, which is a part of Attacks and Defenses Category, as well with particular elements from other areas. For example, supply chain management (one of the essentials of Component security) is discussed in CyBOK within the Adversarial Behaviors area.

It can be seen that CSEC 2017 content is fully addressed by the CyBOK knowledge areas. The topics are covered in a balanced manner. In the case, where specific knowledge is needed, the CyBOK presents the latest research in the field. For example, in Cryptography contemporary theoretical results in quantum algorithms and calculations are examined.

Not only technical, but also human, organizational and law aspects are explored in both documents. The CyBOK provides an international perspective on regulatory requirements and online rights, but it lists noted technologies for

protecting data and user privacy. In this way, it draws attention to wider socio-technical view and covers the issues, discussed in the last tree CSEC2017 areas.

5 Conclusions

In this paper, we explore the CyBOK approach for knowledge areas in cybersecurity and show its applicability to educational process. As a comprehensive store of established knowledge sets, including papers, documents and many other references, it is the best starting point for universities and other academic institutions when creating their educational programs. The presented accordance with CSEC2017 will assists educators in preparing courses and other teaching materials. For all organizations, it could be a good foundation to enhance their own IT security management.

Acknowledgements

This paper is partially supported by the National Scientific Program "Information and Communication Technologies for a Single Digital Market in Science, Education and Security (ICTinSES)", financed by the Ministry of Education and Science.

References

1. About CyBOK, Aims of the CyBOK project, https://www.cybok.org/about/, last accessed 2020/05/11.
2. Change-requests-now-welcome, https://www.cybok.org/news/change-requests-now-welcome, last accessed 2020/03/25.
3. CSEC2017, Cybersecurity Curricula 2017 Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity, Version 1.0, https://www.acm.org/binaries/content/ assets/ education/curricula-recommendations/csec2017.pdf, last accessed 2020/04/21.
4. CSEC_Overview, http://www.ncsl.org/ documents/taskforces/ CSEC_Overview.pdf, last accessed 2020/04/22.
5. Curricula Recommendations, https://www.acm.org/education/curricula-recommendations
6. Cybersecurity. A Generic Reference Curriculum. https://pfp-consortium.org/ index.php/pfpc-products/education-curricula/item/262-cybersecurity-reference-curriculum, last accessed 2020/04/08.
7. CyBOK V.1.0, https://www.cybok.org/media/downloads/, last accessed 2020/02/20. CyBOK_ version_1.0_YMKBy7a.pdf, last accessed 2020/02/18.
8. Dimitrov, V., Semantics of Vulnerabilities and Intelligent Search, Computer and Communications Engineering, Vol. 13, No. 2, pp. 20-25, 2019.
9. 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, last accessed 2020/04/21.
10. ISO/IEC 27000:2018(E): Information technology - Security techniques - Information security management systems - Overview and vocabulary. Standard. ISO/IEC, Switzerland
11. NIETP programs, http://www.iad.gov/NIETP/CAERequirements.cfm, last accessed 2020/04/19

12. Newhouse, William et al., National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework, https://doi.org/10.6028/NIST.SP.800-181, 2017.
13. Orozova D., Kaloyanova K, Todorova M., Introducing Information Security Concepts and Standards in Higher Education, TEM Journal. Volume 8, Issue 3, pp. 1017-1024, August 2019.
14. Savoska S., Tozievska V., Computer crime forms and mechanism for security and protection, Proc. of ISGT2018, Sofia, Bulgaria, November 16-17, 2018, CEUR-WS.org, online CEUR-WS.org/Vol-2464/paper7.pdf, last accessed 2020/02/18.
15. Shalamanov V., Penchev G., Academic Support to Cyber Resilience: National and Regional Approach, Computer and Communications Engineering. 13, No. 2: pp. 73-80, 2019.
16. Sharkov G., Papazov, Todorova K., Koykov G., Georgiev M. and Zahariev G., Cyber Threat Map for National and Sectoral Analysis, Computer and Communications Engineering. 13, No. 2: pp. 29-32, 2019.
17. Trifonov R., Nakov O., Manolov S., Popov, G., Tsochev, G. and Pavlova, G., Framework for the Development of Cybersecurity Training Programs for Students of Engineering Specialties, Related to Computer Systems and Information Technologies, Computer and Communications Engineering. 13, No. 2: pp. 65-68, 2019.