Co-evolution of Security's Body of Knowledge and Curricula

Paul C. van Oorschot Version: 27 June 2021[1]

Abstract: We review efforts to capture the body of knowledge in computer and Internet security, and discuss related curricular frameworks. The aim is to increase awareness of resources to guide the selection of topics in security education and training programs.

Suppose your task is to design and teach a new security course. From a blank sheet. Free of constraints. What would you cover, and what topics should you teach (and why)?

There is no correct answer. But in this article, we hope to inform your decision, pointing you to several menus to choose from and cross-check. We will discuss *security knowledge*, beginning with what is meant by that, and then review selected efforts, primarily from the past 10 years, to identify and categorize the main concepts in computer and Internet security (CIS).[2] Our aim is to provide awareness of resources available to guide the selection of topics for those who educate, or provide training for security-related careers.

We also consider curricular frameworks for courses and programs in security, with a primary focus on university and college education, and secondary focus on training for specific careers. Later articles in this column will explore technical details of particular items of security knowledge—but first the bigger picture.

For context, we begin with a few informal definitions. A *body of knowledge* (BoK) refers to the entirety of facts, current beliefs or understandings, concepts, and practices of an academic domain or profession. A BoK is commonly divided into *knowledge areas* (KAs) and finer-grained subareas or topics (called *knowledge units* in some curricula). The BoK of a domain may be formally organized into an *ontology* reflecting this structure, using categories to hierarchically group items with similar properties, defining the core terminology, and clarifying how the domain's important concepts and entities are related.

In the sense of what is in the literature or is known by experts, a BoK exists whether or not any authoritative organizations associated with the domain have made efforts to capture or describe it systematically, or have endorsed such a description.

BoKs and Curricula

The domain of CIS has matured to a point where several major efforts have now been made to capture its BoK; several major efforts have also aimed to specify detailed curricula for CIS programs (as will be discussed). An explicitly described BoK is valuable in designing curricula, but has numerous other uses (beyond our present scope). Aside from its quality, the value of an attempt to describe a BoK depends on the level of consensus that the description represents the domain and its stakeholders (who may of course have different viewpoints of the domain).

Our underlying agenda in exploring BoKs, KAs and cybersecurity curricula, is to understand the current "shape" of the CIS field. (Authoritative books may also reveal the landscape, and may heavily influence formal BoKs.) One specific goal is to inform decisions on what topics to cover in a broad security-based educational program. The intentionally under-specified question in our opening paragraph has been considered by many instructors, with different answers depending on target audiences, personal goals, and views on what concepts are important. What we teach

[1] (c)IEEE *Security & Privacy* 19(5): 83–89, 2021, at `https://ieeexplore.ieee.org/document/9529234`

[2] Others may prefer the term *cybersecurity*, which we personally view as broader or vaguer; definitions vary.

or prioritize, and even individually consider the BoK to consist of, also depends on our own experience and knowledge.

We now begin our tour of the security knowledge landscape.

Early-stage curricular development

Although far from the first to consider defining security knowledge areas or curricula, Crowley [5] explored these in 2003, with a selective literature survey, discussing differences between education and training, noting differing priorities of academia, industry and government, and building on work by these three sectors, offering a modest four-course proposal for a graduate specialization program.

Historically, government groups (such as the US National Institute of Standards and Technology, NIST) have advanced training programs to meet government needs, industry has encouraged certification programs for designations such as Certified Information Systems Security Professional (CISSP), and academics have led efforts defining bodies of knowledge and educational curricula for CIS education and training. In 2003, the absence of an agreed BoK and curricula was already long recognized, as was the fact that CIS, then called *information assurance* (IA) or *information systems security*, involved far more than securing data or information alone. To allow a view of the evolution of curricula, we note that Crowley's four-course proposal included:

1. Principles of information system security
2. Secure enterprise computing—incident response and computer forensics
3. Information systems security—cryptography and intrusion detection
4. Information systems security—risk analysis and management

While progress towards curricular guidelines continued on numerous fronts, our selective tour picks up next with a 2010 paper by Cooper et al. [4], again under the IA moniker. They noted that security's maturation from 1980 to 2010 resulted in it being recognized as an independent domain, and proposed a body of knowledge for IA education, specifically composed of 83 subjects (topics) grouped under the 11 areas noted in Table 1. This followed a recommendation to "rely less on training standards, more on modern pedagogical and educational practices."

For one exemplar subject, *secure coding*, under the *Secure software design and engineering* area, they gave a detailed description, specifying seven "core" learning outcomes and 18 further elective learning outcomes or questions to be answered. They noted that IA programs may live in academic departments ranging from CS, Computer Engineering, Information Technology, and Security, to Business, Public Policy and Forensic Science. The first four reappear among the six domains comprising the ACM's Curricula Recommendations (later); the other three illustrate

1	Fundamental concepts
2	Cryptography
3	Security ethics
4	Security policy
5	Digital forensics
6	Access control
7	Security architecture and systems
8	Network security
9	Risk management
10	Attack/defense
11	Secure software design and engineering
x	(deprecated) Operational issues

Table 1: Security Areas Identified in Cooper's Curricular Guidelines of 2010 [4].

security's multidisciplinary breadth, stretching beyond traditional computing departments.

Four-year baccalaureate programs in either CS or Computer Engineering departments, when focused on security, often emphasize security technology; these may then serve as a reference point for other programs, e.g., 2-year college-level programs focused on training for specific roles or career paths, professional certifications, and shorter programs focused on practical or operational aspects. However, such short programs do not map back onto typical 4-year programs well.

ACM Computing Classification System (2012)

The 2012 *ACM Computing Classification System* [2] is a classification of computing areas, designed in the form of an ontology for use, e.g., in organizing journal articles by subject areas and subareas. *Security and Privacy* is one of 13 subject *categories*, and has 10 areas within it, each with many further topics (not shown). We list the 10 main areas (Table 2) to allow comparison with the knowledge areas chosen by the related efforts discussed herein. This 2012 classification replaced that of 1998, and remains the most recent version at the time of writing.

1	Cryptography
2	Formal methods and theory of security
3	Security services
4	Intrusion/anomaly detection and malware mitigation
5	Security in hardware
6	Systems security
7	Network security
8	Database and storage security
9	Software and application security
10	Human and society aspects of security and privacy

Table 2: 2012 ACM Computing Classification System: *Security and Privacy* category [2].

Security under the Computer Science Curricula 2013

The *Computer Science Curricula 2013* [1] is a joint effort of the ACM and the IEEE Computer Society. This resource is intended to serve as a curriculum guideline for undergraduate degree programs in Computer Science (CS). It includes a detailed specification of what it refers to as the *Body of Knowledge* for 18 different *Knowledge Areas* (KAs) in CS, and substantial appendices, one including an extensive set of course exemplars. For example, pages 492–502 give the curricular details of the Computer Science Major program at Stanford University, with nine available tracks for CS majors, noting which Stanford CS courses provide which *knowledge units* from among the 18 KAs of the CS Curricula 2013.

This curricula added two new KAs in 2013, one being *Information Assurance and Security (IAS)*; the previous version, CS Curricula 2008, had 16 KAs. Eleven IAS subareas are listed as suitable to teach as stand-alone units (see Table 3), with finer-grained *topics* identified under each subarea. Additional IAS subareas are identified as being suitable to teach under the other KAs "where they are applied"; the document cross-references these to the respective KAs. This pervasiveness of IAS across the other 17 KAs distinguishes IAS. For example, under the KA of HCI, *HCI/Human Factors and Security* is listed, and this then includes a variety of topics (e.g., usability design and security, security economics, impersonation/fraud/phishing, biometric authentication, identity management). Another cross-referenced example is *OS/Security and*

Protection, including topics such as: overview of system security, policy/mechanism separation, and protection/access control/authentication among others.

1	Foundational Concepts in Security
2	Principles of Secure Design
3	Defensive Programming
4	Threats and Attacks
5	Network Security
6	Cryptography
7	Web Security
8	Platform Security
9	Security Policy and Governance
10	Digital Forensics
11	Secure Software Engineering

Table 3: CS Curricula 2013: KA for Information Assurance and Security, isolatable subareas [1].

NICE Framework, 2012-2020 (US)

NICE is the acronym for the US National Initiative for Cybersecurity Education. Our interest is the NICE Workforce Framework for Cybersecurity (NICE Framework), whose origins predate the 2010 establishment of NICE itself [10].

The framework aims to help build a cybersecurity workforce, and is positioned to meet the needs of both public and private sectors, from a US government perspective; it identifies and summarizes employment roles and duties in cybersecurity-related careers, including statements defining *tasks* and *skills* relevant to security careers. This supports the development and training of suitable personnel. The framework's profiling of the cybersecurity job landscape and skills required gives another view of knowledge areas in the field of security. The framework's specified audience includes employers, potential workers in security-related careers (called *learners*), and those in a position to train and educate the learners (including *credential providers*). For further context here, *knowledge* is explicitly defined as a "retrievable set of concepts within memory", *skill* as "the capacity to perform an observable action", and *task* as "an activity directed toward achieving organizational objectives".

The detail-rich 2017 version of the NICE framework specifies seven work *categories* and 31 *specialty areas*, derived from an analysis of security-related work roles; Table 4 gives examples. Note: while the categories in most of our other tables refer to knowledge areas, here they correspond to job roles. The 2020 update [11] refactors the framework's information into a smaller main document and supporting resources, allowing independent maintenance and update; and deprecates use of categories and specialty areas, although these remain available in the 2017

	Work category	Specialty areas (examples)
1	Securely Provision	software development; technology R&D
2	Operate and Maintain	systems administration; systems analysis
3	Oversee and Govern	cybersecurity management; strategic planning and policy
4	Protect and Defend	incident response; vulnerability assessment and management
5	Analyze	threat analysis; exploitation analysis
6	Collect and Operate	cyber operational planning; cyber operations
7	Investigate	cyber investigation; digital forensics

Table 4: NICE Workforce Framework (selected summary from NIST SP 800-181, 2017).

version for those who find them useful. Resources available from the framework landing page[3] include pointers to industry training partners, and content of some related training programs.

CSEC 2017

Another curriculum document expressing views of curricular areas for security is the report from the Joint Task Force on Cybersecurity Education (`https://cybered.acm.org/`) consisting of the ACM, IEEE Computer Society, AIS SIGSEC and IFIP WG 11.8. This report is titled *CSEC 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity* [3], and cites among its own sources: the CS Curricula 2013, a corresponding IT Curricula 2017, and the NICE Framework. Relevant to our interest, we note its definition of *cybersecurity*:

> *A computing-based discipline involving technology, people, information, and processes to enable assured operations in the context of adversaries. It involves the creation, operation, analysis, and testing of secure computer systems. It is an interdisciplinary course of study, including aspects of law, policy, human factors, ethics, and risk management in the context of adversaries.*

For each of its eight *knowledge areas*, the report lists a set of essential topics, as well as a more detailed specification of *knowledge units*, each of those composed of a set of *topics* and corresponding descriptions or curricular guidance. The high-level summary in Table 5 is included to allow top-level comparison to the other factorings of knowledge discussed herein. Motivated by CSEC 2017, an ACM-led effort also produced guidelines for 2-year (associate-degree) security programs [15].

	Security KA	Knowledge Units included (partial list of KUs)
1	Data Security	cryptography, authentication, access control, secure communications, forensics
2	Software Security	design principles, software analysis and testing, configuration, ethics
3	Component Security	component lifecycle & vulnerabilities, supply chains, security testing
4	Connection Security	architectures, physical/software interfaces, attacks (connection, transmission)
5	System Security	policy, access control, monitoring, recovery, testing
6	Human Security	identity management, social engineering, privacy and security
7	Organizational	risk management, governance, law, ethics, planning
8	Societal Security	cybercrime, law, ethics, policy, privacy

Table 5: CSEC 2017 (essential Knowledge Areas, summarized from [3]).

CyBOK 2019–2021 (UK)

CyBOK, the *Cybersecurity Body of Knowledge* [12], is an ambitious project sponsored by the UK government, positioned as "a comprehensive Body of Knowledge to inform and underpin education and professional training for the cyber security sector." As of March 2021, it has 21 *knowledge areas* (KAs) organized in five groups (Table 6). The CyBOK document has a major chapter for each KA, albeit with some inconsistency on whether each chapter aims to itself deliver a knowledge summary, or to identify the knowledge and then point to authoritative literature for details.

CS and Engineering security courses, which tend to focus on security technology, have often under-represented topics in Table 6's first group, whose focus is the human element, organizations, governments, and international aspects. Swire [14] models these as being "above" layer 7

[3] `https://nist.gov/nice/framework`

Grouping		Knowledge Area (KA)
Human, Organizational and Regulatory Aspects	1	Risk Management and Governance
	2	Law & Regulation
	3	Human Factors
	4	Privacy & Online Rights
Attacks & Defenses	5	Malware & Attack Technologies
	6	Adversarial Behaviors
	7	Security Operations & Incident Management
	8	Forensics
Systems Security	9	Cryptography
	10	Operating Systems and Virtualization
	11	Distributed Systems Security
	12	Authentication, Authorisation & Accountability
	13	*Formal Methods for Security
Software Platform Security	14	Software Security
	15	Web & Mobile Security
	16	Secure Software Lifecycle
Infrastructure Security	17	Network Security
	18	Hardware Security
	19	Cyber-Physical Systems Security
	20	Physical Layer Security & Telecommunications
	21	*Applied Cryptography

Table 6: CyBOK 2019 Groupings and Areas [12]. *KA added in March 2021.

in the Open System Interconnection (OSI) network stack model, describing new layers 8–10 respectively labelled: Organization, Government, and International. The remaining four groups in Table 6 are given a variety of names by different experts, with the term *Systems Security* sometimes capturing a majority of them, but confusingly, the scope of both this term and *Network Security* vary significantly across experts. We thus give less emphasis to Table 6's group names, and more to the knowledge areas themselves, and especially to the identified elements within each KA. For a detailed overview of CyBOK's goals and methodology, see Rashid et al. [13].

ACM Curricula Recommendations (summary context)

While it is clear from our review that the full story on curricula guidelines for security education is not simple, a helpful resource is the ACM's summary page: *Curricula Recommendations*.[4] This delivers overall context through an overview report, *Computing Curricula 2020* (CC2020), and identifies Cybersecurity as one of six ACM domains: Computer Engineering, Computer Science, Cybersecurity, Information Systems, Information Technology, Software Engineering. (Data Science is pending as a seventh domain.) The earlier-mentioned CS Curricula 2013 is then listed under the Computer Science heading on the summary page. This context helps to explain why the "shape" of security within, say, Computer Engineering differs from that within Computer Science, and again from that within the separate domain of Cybersecurity itself.

Note that under the separate Cybersecurity heading on this ACM summary page, the main curriculum document for Cybersecurity itself is the CSEC 2017 document (discussed above). The alternative factoring of cybersecurity Knowledge Areas by CSEC 2017 (Table 5), and the

[4] https://www.acm.org/education/curricula-recommendations

IAS knowledge areas under the CS Curricular 2013 (Table 3), are distinct from but interesting to compare to the 2012 *ACM Computing Classification System* of Table 2 [2]. We include these tables to allow comparison; there is no single "correct" view, but rather, each informs us.

Studies on curricular content and breadth

We now briefly review some related studies, for further context.

Parekh et al. [9] executed two studies beginning in 2014, to identify "core cybersecurity topics", aiming to clarify what university and college programs might consider core cybersecurity knowledge. Thirty-six experts with security-related PhDs participated in different stages, the majority being faculty at research-focused universities or teaching-focused colleges, with a smaller number from community colleges, industry and government. They ranked security topics according to various criteria, for a first course in security in one study, and in a second study, for topics that should be known by an entry-level workforce security professional. The topics ranking 1 and 2 were respectively *privacy* and *ethics* (an apparent mismatch with curricular priorities). These particular experts ranked *use of modern tools* near the bottom, and in general gave higher rankings to abstract-conceptual topics (over technology-specific topics).

Hallett and al. [7] measured the breadth of four security curricular frameworks (noted next), based on how equally the topics they emphasized reflected CyBOK's five main groups (from CyBOK's 19 knowledge areas). The Joint Task Force's CSEC 2017 [3] had the best balance; a Certified Master's in Cybersecurity curriculum from the UK NCSC (National Cyber Security Center) had good balance; the 2017 NICE framework (SP 800-181) had less overall balance; and a framework from the UK Institute of Information Security Professionals (IISP) was least balanced, in the sense of giving topics in two of CyBOK's five groups little attention.

Dragoni et al. [6] analyzed over 100 European MSc (university) programs in cybersecurity across 28 countries. As candidates on which to base their analysis, they considered using the content of four frameworks, each reflecting somewhat different biases: CSEC 2017, the 2017 NICE Workforce framework (SP 800-181), a 2019 European taxonomy proposal, and CyBOK 2019. In the end they chose to use CSEC 2017's eight KAs of Table 5 (a cited reason being that their target audience was educational professionals familiar with ACM terminology), augmented by a ninth KA, *Operate and Maintain*, from the NICE Framework (Table 4). They also explicitly labelled 56 KUs (*knowledge units*) under these KAs, as used in their analysis. The MSc programs analyzed were found to cover the 9 KAs unevenly, the best-covered being (in order) data security, connection security, system security, and societal security. They found considerable variation in coverage from country to country, and some KUs specifically positioned as important by the researchers were poorly covered, e.g., *security design* and *component procurement*.

This last study, among others, not only highlights the evolution and maturation of the cybersecurity body of knowledge (BoK), but illustrates how a BoK may be leveraged to evaluate which parts are embedded into curricula of different institutions. Catalogues of prescribed knowledge units are similarly used to accredit cybsecurity educational programs—for example, the US National Security Agency's *Centers of Academic Excellence in Cybersecurity* program (NCAE-C) [8] accredits 2-year, 4-year and graduate-level cybersecurity programs. Other countries have their own programs, for example, the UK National Cyber Security Centre (NCSC) defines subject areas to be covered in CS Master's degree programs, in order for the programs to be NCSC-accredited in security.

Collectively, studies such as those we have mentioned suggest that the dominant curricular framework is CSEC 2017, while CyBOK 2019 plays a large role in discussions of the security body of knowledge, and the NICE Workforce framework is a central information resource on cybersecurity training and career opportunities, complementing industry certification programs.

In summary, the efforts discussed herein help us track the evolving shape of the field of computer and Internet security, and inform our view of the broader cybersecurity landscape. A spectrum of security curricula, and a collection of past efforts to capture a common security BoK, are available for instructors to consult and cross-check as they select topics to build into their security courses, seeking knowledge areas and skills suitable to their personal teaching objectives, their target audiences, and demands for security knowledge workers in industry, government and academia. As you set out in your roles as instructors and organization leaders, we encourage you to make use of the many resources cited herein, developing programs and evolving them to educate and train tomorrow's security experts.

References

[1] ACM and IEEE. Computer Science Curricula 2013: Curriculum Guidelines for Undergraduate Degree Programs in Computer Science. Joint Task Force on Computing Curricula (ACM, IEEE Computer Society), 20 Dec 2013, `https://www.acm.org/binaries/content/assets/education/cs2013_web_final.pdf`

[2] Association for Computing Machinery. ACM Computing Classification System (2012), "Security and Privacy" category, `https://dl.acm.org/ccs`

[3] D L Burley, M Bishop, S Buck, J J Ekstrom, L Futcher, D Gibson, E K Hawthorne, S Kaza, Y Levy, H Mattord, A Parrish. Cybersecurity Curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity. Joint Task Force on Cybersecurity Education, Version 1 Report, 31 Dec 2017, `https://www.acm.org/binaries/content/assets/education/curricula-recommendations/csec2017.pdf`

[4] S Cooper, C Nickell, L Pérez, B Oldfield, J Brynielsson, A G Gökce, E Hawthorne, K J Klee, A Lawrence, S Wetzel. Towards Information Assurance (IA) Curricular Guidelines. Conference on Innovation and Technology in C.S. Education 2010, pp.49-64.

[5] E Crowley. Information systems security curricula development. ACM Conference on Information Technology Curriculum (CITC), pp.249-255, 2003.

[6] N Dragoni, A L Lafuente, F Massacci, A Schlichtkrull. Are we preparing students to build security in? A survey of European cybersecurity in higher education programs. *IEEE Security & Privacy* 19(1):81-88, Jan-Feb 2021.

[7] J Hallett, R Larson, A Rashid. Mirror, mirror, on the wall: What are we teaching them all? Characterising the focus of cybersecurity curricular frameworks. Pages 1–9, USENIX Workshop on Advances in Security Education (ASE18), 2018.

[8] National Security Agency. National Centers of Academic Excellence in Cybersecurity (NCAE-C). `https://www.nsa.gov/resources/students-educators/centers-academic-excellence/`

[9] G Parekh, D DeLatte, G Herman, L Oliva, D Phatak, T Scheponik, A Sherman. Identifying core concepts of cybersecurity: Results of two Delphi processes. *IEEE Trans. Educ.* 61(1):11-20, 2018.

[10] C Paulsen, E McDuffie, W Newhouse, P Toth. NICE: Creating a cybersecurity workforce and aware public. *IEEE Security & Privacy* 10(3):76-79, May-Jun 2012.

[11] R Petersen, D Santos, K A Wetzel, M C Smith, G Witte. NIST SP.800-181rev1: Workforce Framework for Cybersecurity (NICE Framework). US Dept. of Commerce, Nov 2020. `https://doi.org/10.6028/NIST.SP.800-181r1`

[12] A Rashid, H Chivers, G Danezis, E Lupu, A Martin. CyBOK: The Cyber Security Body of Knowledge. Version 1.0, 31 Oct 2019, `https://www.cybok.org`

[13] 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):96-102, May-Jun 2018.

[14] P P Swire. A pedagogic cybersecurity framework. *Commun. ACM* 61(10):23–26, Oct 2018.

[15] C Tang. Cyber2yr2020: ACM Guidelines for Associate-Degree Cybersecurity Programs. *ACM Inroads* 19(2):8-11, June 2019.