Journal of US-China Public Administration, April 2018, Vol. 15, No. 4, 155-162
doi: 10.17265/1548-6591/2018.04.001

Curriculum Development for a Doctoral Program in Cybersecurity

Donna M. Schaeffer
Marymount University, Virginia, USA
Patrick Olson
National University-San Jose, California, USA

Almost daily and current media has stories about data breaches, hacking, privacy, and security. In today's digital society, security of our personal information is a major concern for individuals, security of corporate data is a bottom line issue for organizations, and security of the physical and economic infrastructure is a national concern. The interconnectedness of our systems results in bigger and more complex risks. For individuals, their financial well-being and personal safety may be at risk. For companies, security risks drive costs up and impact revenues. Companies may lose their ability gain and maintain customers. For the nation, the economy, public safety and health are at risk. In recent years, countries and non-governmental organizations have created frameworks for enhancing the security and resilience of critical infrastructures and providing safe and secure systems for the public. Some examples include *Executive Order 13636*, "Improving Critical Infrastructure Cybersecurity" by then-President of the United States Barack Obama, the United Nations (UN) International Telecommunications Union (ITU) Global Cybersecurity Agenda (GCA), and China's Information and Communications Technology Governance Regime. Such frameworks can provide a basis for designing a curriculum and developing courses for academic programs in cybersecurity. This paper describes three frameworks and proposes a doctoral-level curriculum that synthesizes the frameworks to provide graduates with the necessary competencies to be cybersecurity experts in the global arena.

Keywords: cybersecurity, curriculum development, globalization

As an academic discipline, cybersecurity has its roots in information assurance and information security. Kessler and Ramsay (2014) noted that academic programs for information security have existed since the 1990s; Ramsay, Cutrer, and Raffel (2010) described program sponsored by the Department of Homeland Security (DHS) beginning in the mid-2000s.

A number of institutions across the United States have been designated as Centers of Academic Excellence (CAE) by the National Security Agency (NSA) and DHS. Degree programs at 255 universities, colleges, or systems have been granted CAE status for cyber defense, and 20 institutions hold CAE for cyber operations.

Gao (2017) reported that the Cyberspace Administration of China and its Education Ministry plan to

Corresponding author: Donna M. Schaeffer, Ph.D., Marymount University, Virginia, USA; research fields: cybersecurity, information technology, higher education, public policy, ethics.
Patrick Olson, Ph.D., National University-San Jose, California, USA; research fields: cybersecurity, information technology, higher education, public policy, ethics.

provide funding and other resources to four to six cybersecurity programs at its top universities by 2027. The effort is envisioned to include engineering, law, management, and other subjects, provide laboratories to foster research. Yang (2017) described the pilot universities (Xidian University, Southeast University, Beihang University, Wuhan University, Sichuan University, the University of Science and Technology of China, and the Strategic Support Force Information Engineering University) as representing the geographical vastness of the country as well a mixture of civilian and military-affiliated universities. Programs are expected to combine academic work with professional work experience.

Frameworks

United States National Institute of Standards and Technology

In February 2013, then-President Obama issued *Executive Order 13636*, "Improving Critical Infrastructure Cybersecurity". This executive order established that:

> [I]t is the Policy of the United States to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties.

To enact the policy, a voluntary risk-based Cybersecurity Framework (CSF) was developed. This is a set of industry standards and best practices to help organizations manage cybersecurity risks. CSF is a collaborative effort between government and the private sector. CSF avoids placing additional regulatory requirements on businesses.

The collaborators recognize that organizations will continue to have unique risks—different threats, different vulnerabilities, different risk tolerances, and implementation of the best practices set forth in the CSF will vary. It is a living document that is updated and improved as there is feedback on its implementation.

The National Institute of Standards and Technology (NIST) oversees the CSF. NIST is a non-regulatory agency of the United States Department of Commerce. Its origins are a physical science laboratory, but today, its domain encompasses all forms of information and communications technology as well as nanosciences and manufacturing. Its mission (National Institute of Standards and Technology, 2017) is "to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life". The CSF is described in Table 1.

The NIST CSF is comprised of five core functions: identify, protect, detect, respond, and recover. In the identify category, organizations would develop an understanding of how to manage cybersecurity risk to their systems, assets, data, and capabilities. This is the foundation of the CSF. It provides a perspective on cybersecurity in the business context, identifies the resources that support critical functions, and uncovers elated cybersecurity risks. The organization can then focus and prioritize its efforts, consistent with its risk management strategy and business needs.

In the protect function, organizations would develop and implement appropriate safeguards for the security of their critical infrastructure services. This may include building security into systems development, establishing data security, providing access control, and creating awareness among users of its systems.

Identifying that a cybersecurity event has occurred happens in the detect function. This is followed by the respond function, in which organizations take action. The final function is recover, during which organizations minimize the impacts of cybersecurity events to themselves and their constituents.

Table 1

NIST Framework Functions and Categories

Function	Category
Identify	Asset management
	Business environment
	Governance
	Risk assessment
	Risk management strategy
Protect	Access control
	Awareness and training
	Data security
	Information protection processes and procedures
	Maintenance
	Protective technology
Detect	Anomalies and events
	Security continuous monitoring
	Detection processes
Respond	Response planning
	Communications
	Analysis
	Mitigation
	Improvements
Recover	Recovery planning
	Improvements
	Communications

United Nations International Telecommunications Union Global Cybersecurity Agenda

The United Nations (UN) International Telecommunications Union (ITU) Global Cybersecurity Agenda (GCA)[1] originated in 2007 with a goal of enhanced confidence and security in today's information society. It deploys cybersecurity solutions to countries around the world.

The GCA comprises five strategic pillars or work areas: legal measures, technical and procedural measures, organizational structures, capacity building, and international cooperation. The framework is portrayed in Figure 1.

The legal pillar addresses laws and regulations. In order for cybersecurity strategy to be effective at national levels, there needs to be harmonious regional and international strategies. To this end, ITU has developed mandates.

The technical pillar involves standards. Internationally accepted standards are critical in the global arena. Standards are currently being developed with international bodies, like the International Standards Organization (ISO), the European Telecommunications Standards Institute (ETSI), and the International Engineering Task Force (IETF). Standards cover topics, such as secure architecture for end-to-end communications, public keys, and information exchange.

The organizational pillar involves strategy and metrics. Through its Global Response Centre, the ITU

[1] Retrieved from https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx.

works with national Cyber-Incident Response Teams (CIRTs). The Global Response Centre provides real-time threat monitoring and assessment, performs cyber-threat trend statistical analysis, and identifies malware threats. It maintains a database of key resources from around the world and provides a secure and trusted platform where experts from around the globe can collaborate remotely.

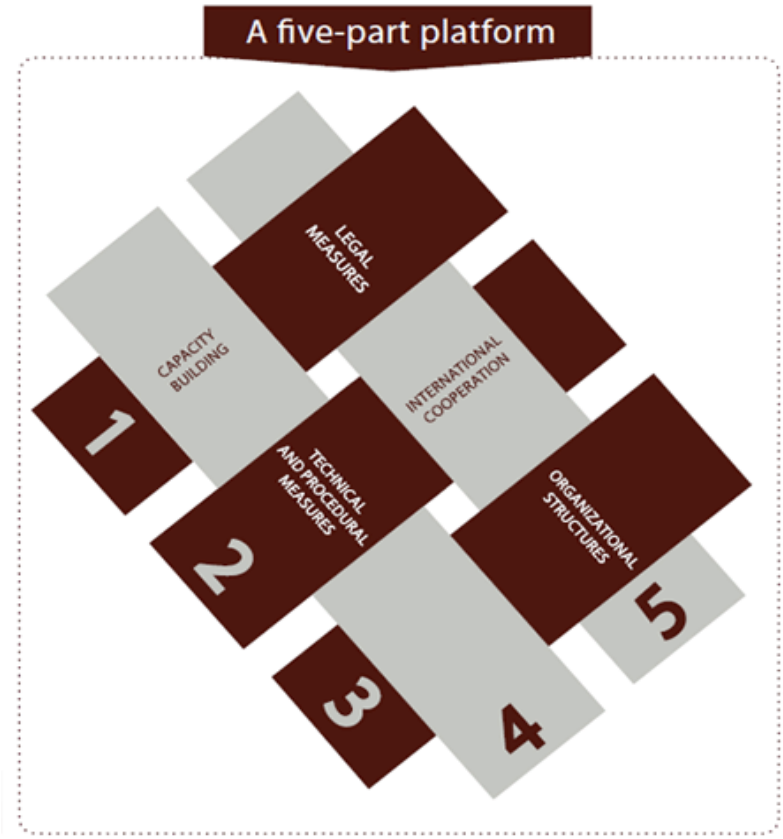

Figure 1. The ITU GCA (Source: https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx).

The capacity building pillar addresses training, public awareness, and research and development. The ITU provides strategy guides and toolkits. It has entered pilot projects to develop talent for nation's CIRTs. The ITU conducts regional cybersecurity seminars, and can perform readiness assessments for member countries.

The cooperation pillar sustains multilateral agreements and public/private partnerships, such as the Child Online Protection Initiative, which provides guidelines for policy-makers, industry, parents and educators, and children for safe Internet use and the ITU-IMPACT partnership. This stands for the International Multilaterial Partnership Against Cyber Threats. Figure 2 describes learning objectives that emerged from the ITU Global Cybersecurity Agenda.

China's Information and Communications Technology (ICT) Governance Regime

China's Information and Communications Technology (ICT) Governance Regime is a developing effort that has that nation's cybersecurity law at its center. It includes national and local strategies, national laws and regulations, and standards. It focuses on data protection and encryption, securing critical infrastructure, and internet content. There are hopes that the ICT Governance Regime will strengthen China's technology industry. Figure 3 depicts the ICT Governance Regime.

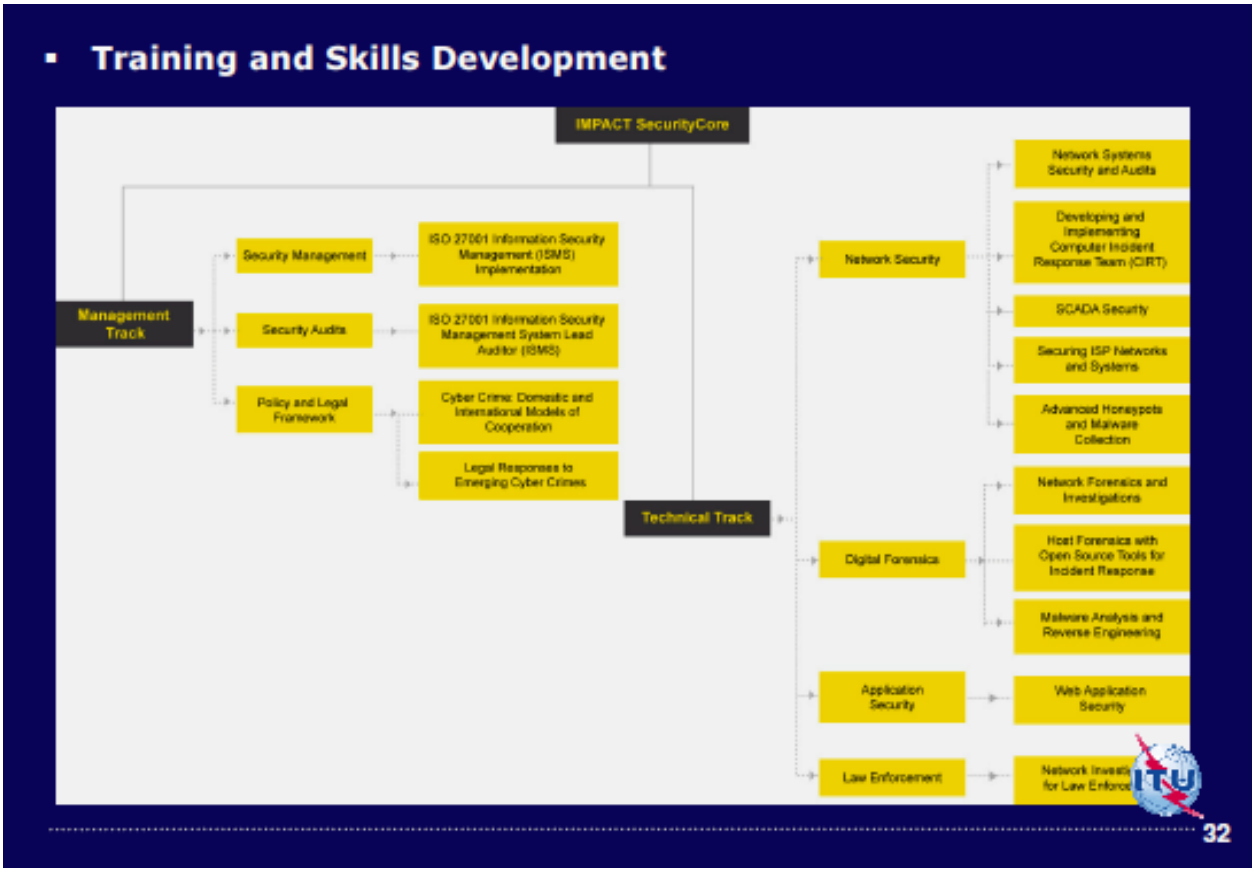

Figure 2. Training and skills development.

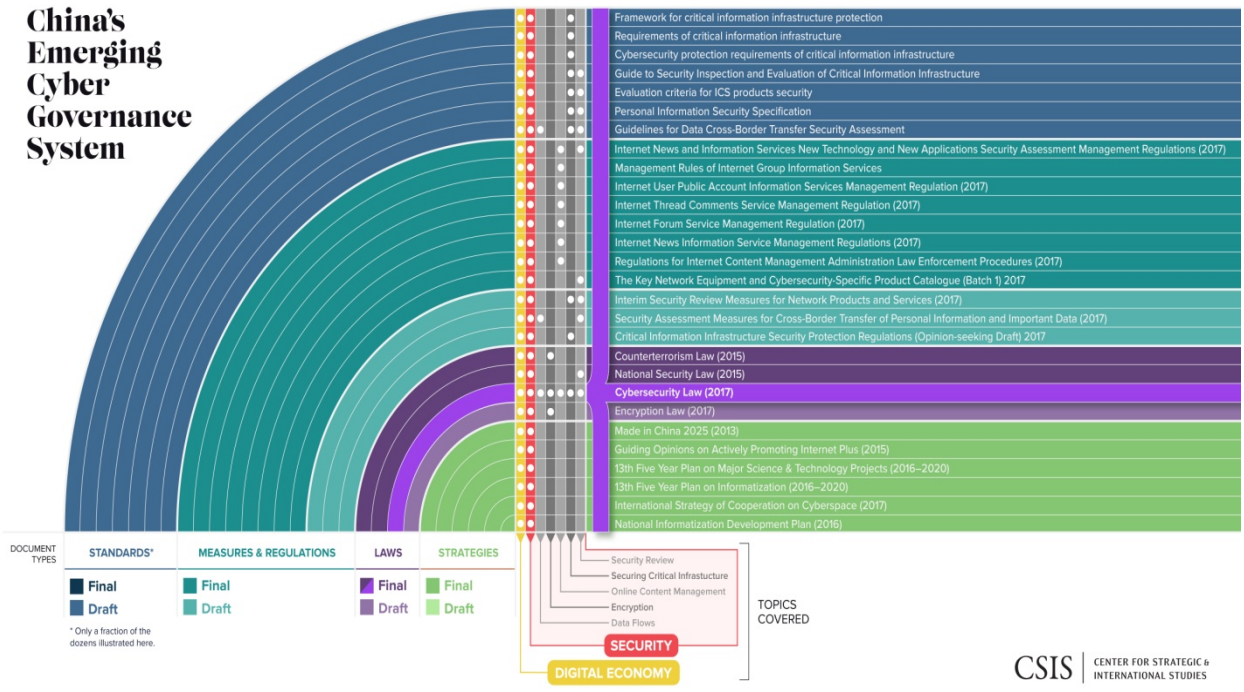

Figure 3. ICT Governance Regime (Source: Sacks, 2018).

Curriculum Development

Although these frameworks are diverse, there are some commonalities that can translate into global learning objectives and form the basis of curriculum. In this paper, we focus on doctoral level curriculum.

At the doctoral level, it is important that cybersecurity curriculum includes both technical and managerial coursework, as well preparation for research. It is essential that ethics be integrated throughout the curriculum.

Students need to have strong technical skills, so they can oversee technical staff and make good decisions about cybersecurity policy and strategy. We recommend coursework in secure systems development, database administration, and network security. Introductory level courses in Information and Software Assurance, Requirements Planning, and Secure Systems Architecture can set the foundation for more advanced coursework in Cybersecurity Testing and Evaluation, Systems Administration, Computer Network Defense Analysis and Infrastructure, Incident Response, Vulnerability Assessment, and Management. Course in forensics and investigation are essential. These technical courses can account for nine credits of introductory work, and 15 credits of more specialized technical courses. It is possible that students could transfer some of this coursework from accredited Master's programs.

After completing a doctoral-level degree in cybersecurity, individuals may move into managerial positions. Thus, it is important that course work includes operations planning, law, and strategic planning and policy development. Additionally, two courses in threat analysis are appropriate. Management-oriented courses can account for 15 credits in a doctoral program.

For the research preparation component, we recommend 15 credit hours. All students should start with basic research methods course, and then choose two courses—one introductory and one advanced—on the methodology they intend to pursue in their research, e.g., qualitative research or quantitative research.

It may also be appropriate that courses are offered in design research and action research. Design research is a relatively young field, having originated in the 1960s in the United Kingdom. It can be applied to the design of systems, especially in the realm of cybersecurity. It looks at research that is embedded in the process of design and aims to understand and improve design processes and practices. Action research is another appropriate methodology for cybersecurity research. The goal of Action research is to solve an immediate problem or serve as part of progressive problem-solving (Stringer, 2013). Denscombe (2010) acknowledged the methodology's ability to produce guidelines for effective practices. Students would conclude the research component of the doctoral program by registering for dissertation or continuing study.

Table 2 presents the proposed course topics and maps them to the NIST CSF and to the ITU Global Cybersecurity Agenda.

Table 2

Curriculum Map

Proposed course topics	NIST cybersecurity framework	ITU Global Cybersecurity Agenda
Information and software assurance	X	X Network systems security and audits
Requirements planning	X	X Information security management and implementation
Secure systems architecture	X	X Web application security

Table 2 to be continued

Cybersecurity testing and evaluation	X	X Securing ISP networks and systems; SCADA security
Systems administration	X	
Computer network defense analysis and infrastructure	X	X Host forensics for open source tools for incident response
Incident response, vulnerability assessment and management	X	X Network investigation for law enforcement
Operations planning	X	X Developing and implementing CIRT
Law	X	X Legal responses to emerging cybercrimes
Strategic planning and policy development	X	X Cybercrime: Domestic and international models of cooperation
All source intelligence and threat analysis	X	X Network forensics and investigations
Exploitation analysis and targets	X	X Malware analysis and reverse engineering; advanced honeypots and malware collection
Research courses		

Conclusions

This discussion shows that the frameworks for prioritizing and/or planning the public efforts, particularly standards, are useful in developing curriculum for cybersecurity. In fact, most topic areas are consistent among the frameworks. Even though the visions for the establishment of these frameworks vary, the meta-concepts are consistent and sound. Thus, using frameworks for curriculum development will yield high quality programs. That result is essential to address these overwhelming issues, like data breaches, hacking, security of our personal information, security of corporate data, and security of physical and economic infrastructure.

References

Denscombe, M. (2010). *Good research guide: For small-scale social research projects* (4th ed.). Berkshire, GBR: Open University Press.

Gao, C. (2017). *China plans to build world-famous cybersecurity schools in 10 years.* Retrieved from https://thediplomat.com/2017/08/china-plans-to-build-world-famous-cyber-security-schools-in-ten-years/

Jing, M. (2017). *China plans network of influential cybersecurity schools.* Retrieved from http://www.scmp.com/tech/china-tech/article/2106919/china-plans-network-influential-cybersecurity-schools

Kessler, G. C., & Ramsay, J. D. (2014). A proposed curriculum in cybersecurity education targeting homeland security students. Proceedings from *the 47th Hawaii International Conference on System Sciences (HICSS)*. January 6-9, Waikoloa, HI, USA.

National Institute of Standards and Technology. (2014). *Framework for improving critical infrastructure cybersecurity.* Retrieved from https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf

National Institute of Standards and Technology. (2017). *Mission, vision, core competencies, and core values.* Retrieved from https://www.nist.gov/about-nist/our-organization/mission-vision-values

Ramsay, J., Cutrer, D., & Raffel, R. (2010). Development of an outcomes-based, undergraduate curriculum in homeland security. *Homeland Security Affairs Journal, 6*(2). Retrieved from http://www.hsaj.org/?article=6.2.4

Sacks, S. (2018). *China's emerging cyber governance system.* Retrieved from https://www.csis.org/chinas-emerging-cyber-governance-system

Stringer, E. T. (2013). *Action research*. London: Sage Publications.

Taylor, C., & Alves-Foss, J. (2005). The need for information assurance curriculum standards. Proceedings from *the 2005 Computer, Information, and Systems Sciences, and Engineering (CISSE 05)*. June, Atlanta, GA.

Yang, Z. (2017). *China is massively expanding its cyber capabilities*. Retrieved from https://nationalinterest.org/blog/the-buzz/china-massively-expanding-its-cyber-capabilities-22577