INSTITUTE FOR DEFENSE ANALYSES

The Need for Higher Education in Cyber Supply Chain Security and Hardware Assurance

Daniel J. Radack, *Project Leader*

Brian S. Cohen
Michelle G. Albert,
Elizabeth A. McDaniel

September 2018

IDA Non-Standard
NS D-9246

INSTITUTE FOR DEFENSE ANALYSES
4850 Mark Center Drive
Alexandria, Virginia 22311-1882

The Institute for Defense Analyses is a non-profit corporation that operates three federally funded research and development centers to provide objective analyses of national security issues, particularly those requiring scientific and technical expertise, and conduct related research on other national challenges.

About This Publication

This work was conducted by the Institute for Defense Analyses (IDA) under contract HQ0034-14-D-0001, Task AU-5-4302, "Trusted and Assured Microelectronics," for ODASD (SE). The views, opinions, and findings should not be construed as representing the official position of either the Department of Defense or the sponsoring organization.

Acknowledgments

Stephen Olechnowicz, Tom Barth

For more information:

Daniel J. Radack, Project Leader
dradack@ida.org, 703-845-6842

Margaret E. Myers, Director, Information Technology and Systems Division
mmyers@ida.org, 703-578-2782

The Need for Higher Education in Cyber Supply Chain Security and Hardware Assurance

Michelle G. Albert, Brian S. Cohen, Elizabeth A. McDaniel
Institute for Defense Analyses, USA

ABSTRACT

Higher education curricula, specialized degrees, and certificate programs related to cybersecurity are proliferating in response to student demand; faculty interest and expertise; employer demand; government and industry standards and funding; and the expectations of specialized, state, or regional accrediting agencies. These expanding academic programs, however, do not adequately address supply chain threats that affect national security. The authors assert that cyber supply chain risk management (C-SCRM), with a focus on hardware assurance, should be considered a critical aspect of cybersecurity and be included in higher education curricula to prepare the future cyber workforce to face challenges related to supply chain security and hardware assurance.

Keywords: Cyber Supply Chain Risk Management (C-SCRM), Cyber Workforce, Cyber-Physical Systems, Cyber Resiliency, Curriculum, Department of Defense (DoD), National Institute for Standards and Technology (NIST), National Initiative for Cybersecurity Education (NICE), Joint Task Force on Cybersecurity Education, National Security Agency (NSA), Department of Homeland Security (DHS)

INTRODUCTION

The U.S. government, the nation's critical infrastructure sectors, and industry are increasingly dependent on commercially designed and manufactured components for *cyber-physical systems*, which are "engineered systems that are built from, and depend on, the seamless integration of computation and physical components" (National Science Foundation [NSF], n.d.). Risks to the supply chains of these components pose a national security threat and can render these systems vulnerable to manipulation or exploitation. These supply chains comprise interconnected webs of people, processes, technology, information, and resources spread around the world. Their complexity provides opportunities for malicious actors to tamper with components or steal information and poses security risks to the performance, integrity, and safety of the hardware components inserted in our systems and networks. To address these risks, the cybersecurity workforce must be well-educated in the latest practices, processes, and technologies related to the cybersecurity aspects of supply chain risk management (SCRM), specifically hardware assurance. Hardware assurance refers to the level of confidence that microelectronics (also known as microcircuits, semiconductors, and integrated circuits, including embedded software and/or intellectual property) function

as intended and are free of known vulnerabilities, whether intentionally or unintentionally designed or inserted as part of the system's hardware and/or embedded software and/or intellectual property throughout its life cycle (Defense Acquisition University, 2017).

In 2018 the National Institute for Standards and Technology (NIST) coined the term *cyber supply chain risk management* (C-SCRM), defined as "the process of identifying, assessing, and mitigating the risks associated with the distributed and interconnected nature of [information and operational technology] IT/OT product and service supply chains (NIST, n.d.). The authors use and endorse the C-SCRM term; however, SCRM is used in some places in the paper when citing earlier work.

BACKGROUND: RELATED POLICIES AND GUIDANCE

Efforts to manage the risks associated with the cyber supply chain began in earnest with the Comprehensive National Security Initiative (CNCI), which was launched in 2008 when President George W. Bush signed National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23), *Cybersecurity Policy* (The White House, 2008b). President Barack Obama determined that CNCI and its associated activities should evolve to become key elements of a broader, united national security strategy (The White House, 2008a).

CNCI Initiative #11 ("Develop a multi-pronged approach for global supply chain risk management") states that risks from both the domestic and global supply chains must be managed over the life cycle of a cyber-enabled component. The purpose of this initiative was to enhance the U.S. government's skills, policies, and processes to provide departments and agencies with a robust toolset to manage and mitigate supply chain risk levels commensurate with the criticality of, and risks to, the government's systems and networks (CNCI, 2008). Although CNCI's sunset provisions caused it to expire in 2013, its key elements continue.

The Committee on National Security Systems (CNSS) is responsible for the protection of national security systems belonging to the Department of Defense (DoD), the Intelligence Community, and other government agencies. CNSS's goals support CNCI and NSPD-54/HSPD-23. CNSS Directive 505, *Supply Chain Risk Management*, was published in 2012 in accordance with CNCI Initiative #11. It states that the U.S. Government must address the reality that the global marketplace provides increased opportunities for adversaries to penetrate supply chains by establishing an organizational capability to identify and manage supply chain risk to national security systems. Risks must be assessed early and throughout the acquisition life cycle, and all-source threat information must inform the use of risk mitigations (CNSS, 2017).

In response to CNCI #11 and CNSS Directive 505, NIST published organizational SCRM approaches for the acquisition, development, and operation of information systems and systems of systems. NIST Special Publication (SP) 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*, provides guidance to federal departments and agencies on identifying, assessing, and mitigating supply chain risk at all levels of their organizations using a multi-tiered SCRM-specific approach. It integrates SCRM into federal agency risk management activities at all organizational levels and includes guidance on supply chain risk assessment and mitigation activities (Boyens et al., 2014). The NIST Interagency Report (NISTIR) 7622, *Notional Supply Chain Risk Management Practices for*

Federal Information Systems (Boyens et al., 2012), offers a set of practices that can be used for information systems categorized as high impact by Federal Information Processing Standard (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems* (NIST, 2004). These practices are intended to promote the acquisition, development, and operations of information systems or systems of systems to meet cost, schedule, and performance requirements in today's environment, which is characterized by global suppliers and active adversaries. NISTIR 7622 suggests risk mitigation strategies for various phases of the system development life cycle (Boyens et al., 2012).

Responding to the real possibilities of supply chain risk to critical systems, DoD issued two instructions to guide action. DoD Instruction 5200.39, *Critical Program Information (CPI) Protection Within the Department of Defense* (USD[I] & USD[AT&L], 2015), and DoD Instruction 5200.44, *Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)*, focus on threats to technology and threats to components, respectively (DoD CIO & USD[AT&L], 2012). For protecting CPI, the policy provides guidance to mitigate CPI exploitation; extend operational effectiveness of military systems through the application of appropriate risk management strategies; employ the most effective protection measures, including system assurance and anti-tamper (AT); and document these measures in a Program Protection Plan (PPP) (USD[I] & USD[AT&L], 2015).

The DoD TSN strategy identifies program protection and information assurance implementation as essential to the development of uncompromised weapons and information systems. The strategy strives to integrate robust systems engineering, SCRM, security, counterintelligence, intelligence, information assurance, hardware and software assurance, and information systems security engineering disciplines to manage risks to system integrity and trust. Systems security engineering, a specialty discipline within systems engineering, supports the development of programs and design-to-specifications that provide life cycle protection for critical defense resources. The primary vehicle for integrating systems security engineering into systems engineering processes during the acquisition life cycle is program protection planning. Programs perform criticality analysis to identify their systems' mission-critical functions and components; assess threats, vulnerabilities, risks, and impacts; and select and apply countermeasures and mitigations (DoD CIO & USD[AT&L], 2012).

To respond to global supply chain risks and cybersecurity risks, DoD requires application of the Risk Management Framework (RMF) described in DoD Instruction 8510.01, *Risk Management Framework for DoD Information Technology (IT)* (DoD CIO, 2014). NIST, in partnership with DoD, the Office of the Director of National Intelligence (ODNI), and CNSS, developed a common information security framework for the federal government and its contractors. Captured in NIST SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, the framework seeks to improve information security, strengthen risk management processes, and encourage reciprocity among federal agencies (NIST, 2010). DoDI 8510.01 mandates the implementation of this common information security framework in DoD. The Services and Agencies have primary responsibility for resourcing RMF implementation.

The RMF is intended to be an integrated, enterprise-wide decision structure for cybersecurity risk management across all DoD mission areas. It informs acquisition processes for IT and applies to all DoD

IT that receives, processes, stores, displays, or transmits DoD information, including information systems; weapons systems; sensor systems; command, control, communications, computers, and intelligence (C4I) systems; and platform IT systems (DoD CIO, 2014). The IT acquisition process includes requirements development, procurement, and both developmental test and evaluation (DT&E) and operational T&E (OT&E), but the RMF does not replace these processes. The RMF's objective is to integrate cybersecurity activities into existing processes, and it provides instructions for addressing attack vectors and resulting cybersecurity risks affecting global supply chains throughout the life cycle of a component or system.

These instructions are designed to protect U.S. interests, DoD operational capabilities, and DoD assets. They stipulate that C-SCRM should be addressed as early as possible in a component or system's life cycle. The authors' previous work, which was driven by these policies and instructions, affirms that C-SCRM has not received sufficient attention (Naval Postgraduate School Acquisition Research Program, 2017).

PREPARING THE CYBER WORKFORCE

This paper focuses on the C-SCRM aspects of the cybersecurity workforce with an emphasis on hardware assurance and the roles that universities play in designing and delivering curriculum. Faculty members at two-year, four-year, and graduate institutions contribute to the advancement of cybersecurity research and practice in many ways, and they develop curriculum to build student knowledge of cybersecurity. Higher education is one of many communities that advances cybersecurity research and practice; other communities include the U.S. government, the private sector (including cyber-related industries), employers, research organizations, professional organizations, standards bodies, and accreditation organizations (see Figure 1, below).

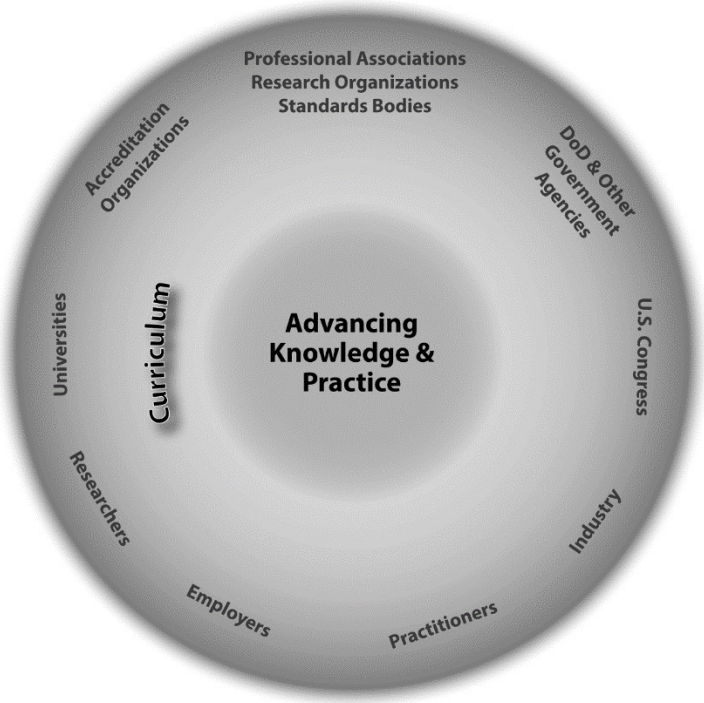

Figure 1. Ecosystem of Cybersecurity Research and Practice

The interactions among members of these communities are complex and multi-directional. For example, the higher education community contributes to the advancement of cybersecurity research and practice through faculty research and participation in professional associations, research organizations, and standards bodies. Faculty also engage with government and private-sector employers, including cybersecurity companies, defense and government contractors, and companies in the microelectronics industry. Figure 1, above, illustrates the ecosystem of communities that advance cybersecurity research and practice.

The body of cybersecurity research and practice increasingly identifies supply chain security as a topic of cybersecurity curriculum. A recent MITRE report *Deliver Uncompromised: A Strategy for Supply Chain Security and Resilience in Response to the Changing Character of War* (Nissen et al., 2018) focused on the need for C-SCRM in critical Department of Defense systems and articulated the need for an educated workforce. The recommended third course of action, "Execute a Campaign for Education, Awareness, and Ownership of Supply Chain and Digital Risk (ST)," calls for "new comprehensive curriculums on supply chain risk and asymmetric adversary intent" to be made available to members of the DoD and the Services and Agencies' acquisition, sustainment, and operations communities (Nissen et al., 2018). Although the report mentions hardware as a supply chain primary attack vector, it primarily focuses on the software aspects of supply chain. This report and others call for enhanced supply chain security focused on software assurance, but hardware assurance does not receive the same attention.

The authors of this paper, researchers in hardware assurance and C-SCRM for the DoD, posit that current cybersecurity standards, workforce frameworks, and curricula do not adequately address the hardware security aspects of C-SCRM. A well-educated cybersecurity workforce needs to understand hardware risks, assess them, and make effective decisions for mitigating them.

SUPPLY CHAIN RISK AND HARDWARE ASSURANCE

The proliferation of cyber-driven technology has brought speed, power, and convenience to all aspects of modern life. But vulnerabilities in the hardware supply chain expose cyber-physical systems to risks associated with protecting system and mission confidentiality, integrity, and availability, as well as the indirect effects of those risks on safety and quality. Hardware of concern includes the microelectronics embedded in cyber-physical systems. These microchips, systems-on-chip (SOC), and field programmable gate arrays (FPGA) are primarily fabricated and assembled outside the U.S. According to one estimate, on average, a microelectronics component makes 15 trips between countries and companies before it is installed into a system (Bernstein, 2014).

According to the *Fiscal Year 2017 Annual Industrial Capabilities Report to Congress* prepared by the DoD, "Assuring the integrity of the Department microelectronics supply chain is becoming increasingly difficult. Globalization, increasing device complexity, low volumes, and small market share have increased the risk of supply chain attacks, placing DoD intellectual property at increased risk of theft by adversaries and increasingly challenging the Department's ability to access leading-edge technologies. DoD recognizes that trusted and assured microelectronics are a critical building block of secure military systems" (OUSD[A&S] & DASD[MIBP], 2018). The Congressional Research Service (CRS), citing a Government

Accountability Office (GAO) report on Department of State telecommunications, affirmed that the "technology is manufactured worldwide and vulnerabilities may be inserted by other actors. Some of those actors may include foreign intelligence services, malicious insiders, or criminals. These actors may be motivated to steal intellectual property, tamper with products, insert counterfeit goods, gain unauthorized access, sell extraneous access, or manipulate the operation of the technology. They may accomplish their goals through inserting malicious code in software, manipulating hardware, or a combination of the two" (CRS, 2018). Actors that conduct industrial espionage are also of significant concern.

C-SCRM focuses on understanding and managing the security risks of using hardware and software sourced from commercial global supply chains in our government, private, and personal devices and systems. C-SCRM covers the entire cycle of a system (including design, development, distribution, deployment, acquisition, maintenance, and destruction) as supply chain threats and vulnerabilities may intentionally or unintentionally compromise an IT/OT product or service at any stage (NIST, n.d.). Hardware supply chain risks include inserting counterfeit components, producing components without authorization, tampering with components, theft, losing information and intellectual property, and employing poor manufacturing practices (Boyens et al., 2014). Hardware components that have been tampered with can result in unwanted functionality of a device, system, or platform (such as monitoring activity or sharing information with an adversary) or fail prematurely, which can affect how the device, system, or platform works. These risks can adversely affect national security—something that Congress[1] and other federal government organizations increasingly recognize. Malicious actors who successfully exploit vulnerabilities in the supply chain affect component performance and integrity and introduce product vulnerabilities that may expose systems and missions to exploitation. The goal of supply chain security is to reduce a component's or system's susceptibility to supply chain threats and reduce or mitigate the potential impact of any such exploitation.

To prevent intentional or intentional defects and ensure that hardware components operate as expected when needed, the workforce needs to be aware of the risks associated with the cyber supply chain (specifically in relation to hardware components) and be able to assess and mitigate them.

CYBERSECURITY AS A MULTIDISCIPLINARY ACADEMIC ENDEAVOR

Cybersecurity has evolved into a multidisciplinary academic field with perspectives from computer science, engineering, information technology, law, the social sciences, ethics, and business/management. The need for cybersecurity has stimulated the development of new industries, multidisciplinary research, standards, workforce roles and careers, as well as a wide range of educational programs and training approaches, and specialized certificates.

Career fields and roles, specializations, disciplinary and multidisciplinary research, and education in cybersecurity continue to expand and evolve. In the case of cyber-physical systems, risks include system security, resiliency in the face of attack or compromise, and unintended effects of machine failure (NSF, n.d.). The hardware components in these systems cannot easily be updated with replacements, and patching software or hardware components may create compatibility issues with other components in the same complex "system of systems." For these systems, efficiency is a priority; the need for resiliency, such as

the ability to patch, is not considered a requirement (NSF, n.d.). Systems engineers who design and operate cyber-physical systems and systems of systems need to understand the importance of designing resiliency into cyber-physical systems and of life cycle vulnerabilities and threats posed by the hardware supply chain. As such, the refinement of new cybersecurity work roles, such as cyber engineering, and new curricula for systems security engineering that include cybersecurity and resilience of cyber physical systems are in discussion.[2]

A recent report by the National Academies of Science advocates a new discipline called "Security Science" to strengthen the scientific underpinnings of cybersecurity by drawing from science, law, testable explanations, predictions about systems, and confirmation or validation of outcomes. According to *Foundational Cybersecurity Research: Improving Science, Engineering, and Institutions,* "Cybersecurity can be viewed as a cutting edge of computing that demands a broad, multidisciplinary effort. Addressing the global cybersecurity challenge needs not just computer science, engineering science, and mathematics, but partnerships with other disciplines to draw on what we know and understand about human nature and how humans interact with and manage systems—and each other" (National Academies of Science, Engineering, and Medicine, 2017).

NIST recommends a multi-disciplinary approach to C-SCRM, incorporating information security, system and software engineering, software assurance, acquisition, logistics, contracting, and law (Boyens et. al., 2012). The development and continued advancement of the cybersecurity workforce requires a curriculum that covers all aspects of C-SCRM and hardware assurance. The U.S. government, private industry, standards bodies, and academic communities are collaborating to define and elaborate C-SCRM and hardware assurance standards and best practices.[3] They also collaborate with members of other communities to inform curricula in computer science, cybersecurity, information technology, electrical engineering, systems, cyber and systems security engineering, business, law, and the social sciences.

CYBERSECURITY WORKFORCE FRAMEWORKS

The current cyber workforce in the DoD, the U.S. government as a whole, and the private sector needs greater awareness of C-SCRM and, specifically, hardware risks and security. The future workforce, including current and future students, needs the knowledge, skills, and abilities (KSA) to implement current C-SCRM practices and to develop new practices as the technologies, risks, and responses change. In recent years, cybersecurity workforce frameworks have articulated dozens of roles and careers that are critical to cybersecurity in government and private sector organizations, as well as KSAs associated with each. KSAs are the attributes needed to perform specific work roles (Newhouse et al., 2017). Subject matter experts from various communities contributed to the development of the National Initiative for Cybersecurity Education (NICE) and the latest version of the *Cybersecurity Workforce Framework* (Newhouse et al., 2017). The latter work, developed in coordination with the DoD Cyber Workforce Framework (DoD CIO, n.d.), identifies seven categories of activity: Securely Provision (SP), Operate and Maintain (OM), Oversee and Govern (OV), Protect and Defend (PR), Analyze (AN), Collect and Operate (CO), and Investigate (IN). These categories are further elaborated into 32 total specialty areas, each representing an area of concentrated work or function within cybersecurity and related fields (Newhouse et al., 2017). The specialty areas are organized by work roles that comprise groupings of related work in cybersecurity and other fields,

as well as the KSAs needed to perform each role. Within this framework, SCRM requires a cross-cutting set of competencies.

The framework primarily addresses SCRM in its SP category, but it is found in most of the categories, affirming its cross-cutting nature. The hardware assurance aspect of SCRM, however, is not called out specifically.

Table 1, below, lists work roles related to SCRM and hardware assurance.

Table 1. NICE Work Roles Related to SCRM and Hardware Assurance

Category	Specialty Area	Work Role
Securely Provision (SP)	Systems Development (SYS)	Information Systems Security Developer
		Systems Developer
Operate and Maintain (OM)	Systems Analysis (ANA)	Systems Security Analyst
Oversee and Govern (OV)	Cybersecurity Management (MGT)	Information Systems Security Manager

CURRICULUM GUIDELINES FOR C-SCRM AND HARDWARE ASSURANCE

Higher education curricula in various disciplines are expanding, and specialized degrees and certificates related to cybersecurity are proliferating in response to student interest and/or employer demand; faculty interest and expertise; and the expectations of specialized, state, and regional accrediting agencies. For clarity and consistency in curriculum across academic programs, experts collaborated to publish curriculum guidelines aligned with cybersecurity topics and outcomes.

The Joint Task Force on Cybersecurity Education was established in September 2015 as part of the Cyber Education Project, an initiative to develop curriculum guidelines for undergraduates and promote accreditation for curricula in the "cyber sciences" (Cyber Education Project, n.d.). In February 2018, the Joint Task Force published *Cybersecurity Curricula 2017* (CSEC2017), which offers curriculum guidance for cybersecurity education. CSEC2017 establishes a "component security" knowledge area that focuses on "the design, procurement, testing, analysis and maintenance of components integrated into larger systems" (Joint Task Force on Cybersecurity Education, 2017). The curriculum guidelines identify supply chain risks, supply chain security, supplier vetting, and component design security, and specifically mention security threats and risks to hardware. *Table 2*, below, lists the knowledge units of "Component Security."

Table 2. Component Security Knowledge Units and Topics

Knowledge Unit	Topics
Component Design	Component design security, principles of secure component design, component identification, anti-reverse engineering techniques, side-channel attack mitigation, anti-tamper technologies
Component Procurement	Supply chain risks, supply chain security, supplier vetting
Component Testing	Principles of unit testing, security testing
Component Reverse Engineering	Design reverse engineering, hardware reverse engineering, software reverse engineering

The National Security Agency (NSA) and the Department of Homeland Security (DHS) sponsor the Centers for Academic Excellence in Cyber Defense (CAE-CD) program. The CAE-CD program promotes higher education curriculum and research in cyber defense by designating institutions that conduct related research and offer either two- or four-year educational programs in cyber defense as CAE institutions (NSA & DHS, 2018). To be eligible for the designation of CAE-CD, academic programs must map their existing curricula to the CAE-CD Knowledge Units that specify technical and non-technical areas in which students are expected to acquire certain knowledge and skills. The "foundational" and "core" Knowledge Units comprise the base curricular requirements for eligibility. Optional Knowledge Units allow institutions to highlight additional areas of focus (NSA & DHS, n.d.). SCRM and hardware assurance are not mentioned in the required Knowledge Units, but elements of each can be found in the descriptions related to optional Knowledge Units. *Table 3*, below, lists a few SCRM and hardware assurance-related optional Knowledge Units and topics.

Table 3. Relevant Knowledge Units

Knowledge Unit	Topics
Hardware Reverse Engineering	Principles of reverse engineering; stimulus, data collection, data analysis; specification development; capability enhancement/modification techniques, detecting modification; stimulation methods/instrumentation (probing and measurement); JTAG IEEE 11.49.1; defining and enumerating interfaces; functional decomposition
Hardware/Firmware Security	Physical vulnerabilities, hardware side-channel attacks, sourcing attacks, equipment destruction attacks, hardware security components, physical security attributes, bootloader vulnerabilities, microcode vulnerabilities, firmware vulnerabilities, security role of intermediate layers
Supply Chain Security	Global development, offshore production, transport and logistics of IT components, evaluation of third-party development practices, understanding of the capabilities and limits of software and hardware reverse engineering

CURRICULUM IN HARDWARE ASSURANCE

Hardware assurance does not receive the same level of attention in higher education curricula as software assurance; however, faculty at some research universities that conduct hardware assurance research are beginning to offer hardware-security-related topics and courses primarily at the graduate level. The curricula of three institutions are cited here as examples.

The University of Florida's Department of Electrical and Computer Engineering offers introductory and advanced courses in hardware security and trust on integrated circuits, including cryptographic hardware, side-channel attacks, counterfeit detection, and hardware Trojan detection and prevention. "Introduction to Hardware Security and Trust" covers cryptographic processing and analysis, physical and invasive attacks, side-channel attacks, physically unclonable functions (PUF), hardware-based random number generators, intellectual property (IP) watermarks, FPGA security, piracy prevention, access control, and hardware Trojan detection and isolation in IP cores and integrated circuits (Tehranipoor, n.d.). "Computer and Information Security" reviews programmed threats and controls in hardware. The hardware security lab offers students opportunities to learn to hack a system and analyze countermeasures for different hardware attacks (Florida Institute for Cybersecurity Research, n.d.).

The University of Maryland Department of Electrical and Computer Engineering offers an advanced laboratory on hardware security and software reverse engineering that focuses on security vulnerabilities in hardware design, hardware security threats and countermeasures, and enhancing hardware system security and trust. It also covers techniques for designing secure systems, reverse engineering, and secure programming (University of Maryland, n.d.).

The University of Connecticut's Center for Hardware Assurance, Security, and Engineering (CHASE) promotes "interdisciplinary hardware-oriented research and applications" and creates opportunities for interdisciplinary research and education (University of Connecticut, n.d.). Areas of current research are device-to-system security and trust, security assessment, counterfeit detection and prevention and supply chain management, device-to-system reliability, device-to-system quality, and standards. Some courseware in hardware security and trust topics is available to students. "Hardware Security" covers several topics, including secure processor architectures, cryptographic concepts, side-channel attacks, PUFs, digital signatures, and public key encryption, and it also offers several coding labs (van Dijk, 2017). "Trustable Computing Systems" offers an introduction to trust and hardware security and covers side-channel attacks, differential power analysis, acoustic analysis, DRAM data remanence, and embedded systems security (Chandy, 2016).

CURRICULUM CHANGE AS A PROCESS IN THE ECOSYSTEM

Curricular change in the form of new topics and learning outcomes, courses, and programs of study is the result of ongoing engagement by several communities inside and outside academic institutions. Faculty and administrators participate as experts with accreditation organizations such as the Accreditation Board for Engineering and Technology (ABET) and the Association to Advance Collegiate Schools of Business (AACSB), professional associations such as the Association for Computing Machinery (ACM) and the IEEE Computer Society, and standards bodies such as the International Organization for

Standardization (ISO) and NIST. They articulate emerging and important curricular topics and standards, workforce roles, and workforce needs. Industries that manufacture microelectronics and build systems that use them and employers with a dynamic and advanced cybersecurity workforce communicate with members of the higher education community because of its role in preparing qualified students to enter the workforce.

Workforce education and skill requirements identified by public- and private-sector organizations stimulate the refinement of existing courses of study related to cybersecurity. New cybersecurity topics, courses, and specializations are emerging in disciplines such as computer science, engineering, systems and cyber engineering, business and management, law, and the social sciences. For example, as manufacturers and operators recognize the cyber risks associated with cyber-physical systems, they are articulating their workforce needs. Demand for cybersecurity personnel with interdisciplinary specializations will influence new guidelines articulated by accreditation organizations and standards organizations and new research and practice.

Figure 2 illustrates interactions in the ecosystem with a focus on higher education. Faculty conduct research and participate in research, accreditation, standards, and professional organizations. They design and deliver curriculum in a dynamic environment that provides continuous feedback loops related to research, innovation, and analysis contributed by faculty and other researchers and organizations. Students demand educational programs that will lead to employment; employers demand an educated workforce to meet their needs. Funders from government organizations and industry stimulate change in research and practice, and accreditation and professional organizations develop priorities and engage faculty, researchers, and private sector experts in their development.

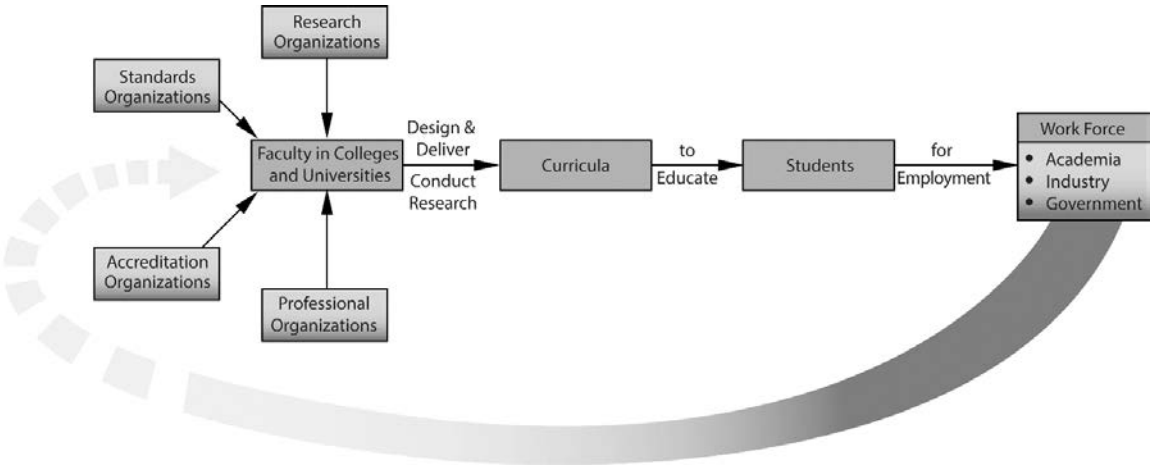

Figure 2. The Higher Education Community

FACTORS THAT INFLUENCE CURRICULUM CHANGE IN HIGHER EDUCATION

Institutions of higher education have a tradition of self-governance. Changes in curriculum are motivated by new knowledge and practice, accreditation guidelines, and/or faculty and administrator

considerations. At most institutions, governance processes related to curriculum involve faculty in, and sometimes across, departments, as well as institutional boards in well-articulated layers of review and approval. Enrollment demands and institutional investments in emerging areas of student interest are among the drivers of curriculum change. Curriculum change typically involves the equities of faculty and departments, resource constraints, student demand, and administrative priorities. Interdisciplinary fields like cybersecurity engage faculty and departments, sometimes in complicated processes and priorities. Curriculum is "an expression of intellectual accountability to external factors—society's expectations and changes in knowledge—and to internal factors, such as students' needs. … At its best, it is the product of an independent reading by an academic community of what is needed at a particular time and an educational expression of that need" (Putchinski, 1998).

Depending on the size and significance of a proposed change, curricular change typically involves faculty governance bodies, university academic administrators and board members, state review boards (in some cases), and regional and specialized accrediting agencies. Requirements specified by accrediting agencies, recommendations from professional organizations, and workforce demands are often motivating factors of curriculum change.

THE WAY FORWARD

Given the rapid pace of technology innovation and the evolution of hardware- and supply-chain-related cyber threats to cyber-physical systems, the authors promote the inclusion of hardware assurance as part of C-SCRM in cybersecurity curricula. To develop a workforce capable of addressing supply chain security and hardware assurance challenges, the authors make the following recommendations for action to the communities in the cybersecurity research and practice ecosystem:

1. Develop hardware assurance roles and KSAs for inclusion in the DoD Cyber Workforce Framework and the NICE Cyber Workforce Framework.
2. Add hardware assurance as a Knowledge Unit in the NSA Centers of Academic Excellence criteria and to similar lists of critical topics in cybersecurity that form the basis of curricula in various disciplines.
3. Raise the level of awareness about hardware risk and promote hardware assurance as a foundational element across disciplines.
4. Develop curricula to address emerging technologies, risks, and responses related to hardware assurance and C-SCRM.
5. Advance the knowledge and practice of professionals serving in various workforce roles related to cyber-physical systems with training specific to C-SCRM and hardware assurance.

ACKNOWLEDGMENTS

This work was conducted by the Institute for Defense Analyses (IDA) under contract HQ0034-14-D-0001, Project AU-5-4302, "Trusted and Assured Microelectronics." The views, opinions, and findings should not be construed as representing the official position of either the Department of Defense or the

sponsoring organization, the Trusted and Assured Microelectronics Program for the Office of the Deputy Assistant Secretary of Defense for Systems Engineering (ODASD(SE)).

IDA researchers Thomas H. Barth and Stephen M. Olechnowicz contributed to early projects focused on higher education’s role in developing the cybersecurity workforce.

REFERENCES

Bernstein, K. (2014). *An example from the defense supply chain*. Arlington, VA: DARPA Microsystems Technology Office.

Boyens, J. M., Paulsen, C., Bartol, N., Moorthy, R., & Shankles, S. (2012, October 16). *Notional supply chain risk management practices for federal information systems* (NIST IR 7622). Retrieved from https://nvlpubs.nist.gov/nistpubs/ir/2012/nist.ir.7622.pdf.

Boyens, J., Paulsen, C., Moorthy, R., & Bartol, N. (2014, June). *Supply chain risk management practices for federal information systems and organizations* (NIST Second Draft SP 800-161). Retrieved from https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-161.pdf

Chandy, J. A. (2016). *ECE 4095: Trustable computing systems*. Storrs, CT: University of Connecticut. Retrieved from http://www.engr.uconn.edu/~chandy/courses/4095s16/Syllabus-S16.pdf.

Committee on National Security Systems (CNSS). (2017, July 26). *Supply chain risk management* (CNSS Directive 505). Retrieved from https://federalnewsradio.com/wp-content/uploads/2017/08/CNSSD_505_Final2-Published-08-01-2017.pdf.

Congressional Research Service. (2018, June 29). Cyber supply chain risk management: An introduction. *In Focus.* Retrieved from https://fas.org/sgp/crs/homesec/IF10920.pdf.

Cyber Education Project. (n.d.). Retrieved from https://www.cybereducationproject.org/. Accessed June 27, 2018.

Defense Acquisition University. (2017, November 6). Hardware assurance. *Defense Acquisition Guidebook*, Ch. 9, Sec. 3.2.4.

Department of Defense (DoD) Chief Information Officer (DoD CIO). (n.d.). *The DoD cyber workforce framework (DCWF).* Retrieved from https://dodcio.defense.gov/Cyber-Workforce/dcwf.aspx.

DoD CIO & the Under Secretary of Defense for Acquisition, Technology and Logistics (USD[AT&L]). (2012, November 5). *Protection of mission critical functions to achieve trusted systems and networks (TSN)* (DoD Instruction 5200.44, Incorporating Change 2, July 27, 2017). Retrieved from https://fas.org/irp/doddir/dod/i5200_44.pdf.

DoD CIO. (2014, March 12). *Risk management framework for DoD information technology (IT)* (DoD Instruction 8510.01 Incorporating Change 2, July 28, 2017). Retrieved from http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/851001_2014.pdf.

Florida Institute for Cybersecurity Research. (n.d.). *Cybersecurity courses*. Retrieved from https://fics.institute.ufl.edu/cybersecurity-courses/?doing_wp_cron=1532711191.5793690681457519531250#CIS2354. Accessed July 27, 2018.

Joint Task Force on Cybersecurity Education. (2017, December 31). *Cybersecurity curricula 2017*. Retrieved from https://cybered.hosting.acm.org/wp-content/uploads/2018/02/newcover_csec2017.pdf.

National Academies of Science, Engineering, and Medicine. (2017). *Foundational cybersecurity research: Improving science, engineering, and institutions*. Washington, DC: The National Academies Press. http://doi.org/10.17226/24676.

National Institute of Standards and Technology (NIST). (n.d.). *Cyber supply chain risk management*. Retrieved from https://csrc.nist.gov/Projects/Supply-Chain-Risk-Management. Accessed July 30, 2018.

National Institute for Standards and Technology (NIST). (2004, February). *Standards for security categorization of federal information and information systems* (Federal Information Processing Standard [FIPS] 199). Retrieved from https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf.

National Institute for Standards and Technology (NIST). (2010, February). *Guide for applying the risk management framework to federal information systems* (NIST SP 800-37 Revision 1). Retrieved from https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-37r1.pdf.

National Science Foundation (NSF). (n.d.). *Cyber-Physical Systems*. Retrieved from https://www.nsf.gov/funding/pgm_summ.jsp?pims_id=503286.

National Security Agency (NSA) Central Security Service (CSS). (2018, July 3). *National Centers of Academic Excellence*. Retrieved from https://www.nsa.gov/resources/students-educators/centers-academic-excellence/#defense.

National Security Agency (NSA) & the Department of Homeland Security (DHS). (n.d.). *Centers of Academic Excellence in Cyber Defense (CAE-ED) 2019 Knowledge Units*. Retrieved from https://www.iad.gov/NIETP/documents/Requirements/CAE-CD_2019_Knowledge_Units.pdf.

Naval Postgraduate School Acquisition Research Program. (2017). *14th Annual Acquisition Research Symposium*. Monterey: CA. Retrieved from https://www.researchsymposium.com/conf/app/researchsymposium/home#!/page/38.

Newhouse, W., Keith, S., Scribner, B., & Witte, G. (2017, August). *National initiative for cybersecurity education (NICE) cybersecurity workforce framework* (NIST SP 800-181). Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf.

Nissen, C., Gornager, J., Metzger, R., & Rishikof, H. (2018, August). *Deliver uncompromised: A strategy for supply chain security and resilience in response to the changing character of war*. McLean, VA: The MITRE Corporation. Retrieved from https://www.mitre.org/sites/default/files/publications/pr-18-2417-deliver-uncompromised-MITRE-study-8AUG2018.pdf.

Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD[A&S]) & Office of the Deputy Assistant Secretary of Defense for Manufacturing and Industrial Base Policy (DASD MIBP). (2018, March). *Fiscal Year 2017 Annual industrial capabilities report to Congress*. Retrieved from https://www.businessdefense.gov/Portals/51/Documents/Resources/2017%20AIC%20RTC%2005-17-2018%20-%20Public%20Release.pdf?ver=2018-05-17-224631-340.

Putchinski, L. B. (1998). *Case study of curriculum change in a College of Business Administration*. (Doctoral Dissertation). Retrieved from ProQuest Dissertations Publishing. (9910803). Citing Toombs, W. & Tierney, W. (1992). *Meeting the mandate: Renewing the college and departmental curriculum*. (ERIC digest). Washington, D.C.: George Washington University. (ERIC Document Reproduction Service No. ED347957).

Tehranipoor, M. (n.d.). *EEL 4714/5716: Introduction to hardware security and trust*. Storrs, CT: University of Connecticut. Retrieved from http://tehranipoor.ece.ufl.edu/hst.html.

The White House. (2008a). *The comprehensive national cybersecurity initiative*. Retrieved from https://obamawhitehouse.archives.gov/node/233086.

The White House. (2008b, January 8). *Cybersecurity policy* (NSPD-54/HSPD-23). Retrieved from https://fas.org/irp/offdocs/nspd/nspd-54.pdf.

Under Secretary of Defense for Intelligence (USD[I]) & Under Secretary of Defense for Acquisition, Technology and Logistics (USD[AT&L]). (2015, May 28,). *Critical program information (CPI) protection within the Department of Defense* (DoD Instruction 5200.39 Incorporating Change 1,

November 17, 2017). http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/520039p.pdf.

University of Connecticut. (n.d.). *Center for Hardware Assurance, Security, and Engineering*. Retrieved from http://chase.uconn.edu/.

University of Maryland. (n.d.). *ENEE459B: Reverse engineering and hardware security laboratory*. Retrieved from http://www.ece.umd.edu/undergrad/courses/400-level/enee459b.

van Dijk, M. (2017). *ECE4451 and CSE5451: Hardware security*. Storr, CT: University of Connecticut. Retrieved from https://scl.engr.uconn.edu/courses/ece4451/hs.php.

---

[1] The National Defense Authorization Act (NDAA) for fiscal year (FY) 2019 states that the Secretary of Defense shall establish a Defense Acquisition Workforce Cyber Training Program "to certify small business professionals and other relevant acquisition staff within the Department of Defense to provide cyber planning assistance to small manufacturers and universities" (H.R. 5515—115th Congress, 2017–2018).

[2] From July 31–August 2, 2018, DoD held its sixth Engineering Cyber Resilient Weapons Systems (CRWS) workshop, which included a discussion of current academic programs that address cyber resilient systems and education gaps and challenges.

[3] NIST publications related to C-SCRM include Special Publication (SP) 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*, published in 2015, and NIST Interagency Report (NISTIR) 8179, *Criticality Analysis Process Model: Prioritizing Systems and Components*, published in April 2018. A complete list of NIST publications related to C-SCRM can be found at https://csrc.nist.gov/Projects/Supply-Chain-Risk-Management/publications.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE (DD-MM-YY)	2. REPORT TYPE	3. DATES COVERED (From – To)
09-15-2018	Non-Standard	

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
The Role of Higher Education in Preparing the Cybersecurity Workforce for Supply Chain Security and Hardware Assurance	HQ0034-14-D-0001
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBERS

6. AUTHOR(S)	5d. PROJECT NUMBER
Brian S. Cohen, Michelle G. Albert, Elizabeth A. McDaniel	AU-5-4302
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESSES	8. PERFORMING ORGANIZATION REPORT NUMBER
Institute for Defense Analyses 4850 Mark Center Drive Alexandria, VA 22311-1882	NS D-9246

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR'S / MONITOR'S ACRONYM
Dr. Jeremy Muldavin ODASD (SE) 4800 Mark Center Drive, Suite 16E08, Alexandria, VA 22350	AU/DASD, SE
	11. SPONSOR'S / MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

This draft has not been approved by the sponsor for distribution and release.

13. SUPPLEMENTARY NOTES

Project Leader: Brian S. Cohen

14. ABSTRACT

Higher education curricula, specialized degrees, and certificate programs related to cybersecurity are proliferating in response to student demand; faculty interest and expertise; employer demand; government and industry standards and funding; and the expectations of specialized, state, or regional accrediting agencies. These expanding academic programs, however, do not adequately address supply chain threats that affect national security. The authors assert that cyber supply chain risk management (C-SCRM), with a focus on hardware assurance, should be considered a critical aspect of cybersecurity and be included in higher education curricula to prepare the future cyber workforce to face challenges related to supply chain and hardware security.

15. SUBJECT TERMS

cyber supply chain risk management (C-SCRM), cyber workforce, cyber-physical systems, cyber resiliency, curriculum, higher education, cybersecurity workforce, supply chain security and hardware assurance

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Dr. Jeremy Muldavin
Unclassified	Unclassified	Unclassified	Unlimited	16	19b. TELEPHONE NUMBER (Include Area Code) 571-372-6690