Open Access License Notice

Building Capacity for Systems Thinking in Higher Education Cybersecurity Programs

Esther A. Enright
Boise State University
Boise, ID, USA
estherenright@boisestate.edu

Connie Justice
Purdue School of Engineering and Technology, IUPUI
Indianapolis, IN, USA
cjustice@iupui.edu

Sin Ming Loo
Boise State University
Boise, ID, USA
smloo@boisestate.edu

Eleanor Taylor
Idaho National Laboratory
Idaho Falls, ID, USA
Eleanor.Taylor@inl.gov

Char Sample
Idaho National Laboratory
Idaho Falls, ID, USA
Charmaine.Sample@inl.gov

D. Cragin Shelton
Capitol Technology University
Laurel, MD, USA
dcshelton@captechu.edu

***Abstract*—The decentralized nature of cybersecurity programs in higher education leads to a lack of unifying knowledge, skills, and dispositions in the cybersecurity workforce. The emphasis on teaching the latest technologies and techniques without a sufficient foundation in systems thinking could result in graduating students without the capacity to function as constructive agents operating in complex systems. Having a unifying, cohesive cybersecurity systems framework can bridge some of these gaps. In this article, we argue that cybersecurity programs and courses must contextualize their instruction on a specific topic by teaching students to situate their learning on the system level. Additionally, we suggest that active learning strategies, in particular case study analysis and concept mapping, are particularly well suited to support this type of student learning. This article presents a cohesive framework for teaching systems thinking in cybersecurity programs and courses. The framework is designed to support meaningful reform in the currently decentralized, (mostly) unregulated academic ecosystem that manages the preparation of our cybersecurity workforce.**

Keywords—cybersecurity, systems thinking, active learning, higher education

I. Introduction

The cybersecurity field has undergone significant changes since the early days of firewalls [1]. Today, the field serves the design and maintenance of intrusion detection systems (IDSs) [2], security information event management systems (SIEMs), and [3] more recently, artificial intelligence (AI) and machine learning (ML) [4] solutions. Even the name of the field has changed over the past 40 years as the practice has matured, addressing increasingly wider aspects of protection. What began as computer security, addressing a computer system and the data it processed, transitioned to network security as the implications of multiple, interconnected computers became apparent. More recently, practitioners shifted to calling the field information security since past names focused on the hardware and software, instead of considering the stored and manipulated data and the meaning of the data in context (information). Further analysis of the responsibility for assuring confidentiality, integrity, and availability of information led to calling the field information assurance. While this might be a more complete, accurate name, the word assurance did not communicate well with the general public, who confused it with insurance. Now, the word cyber has captured the public's attention, so cybersecurity is currently the preferred term.

As technology developed the demands on the cybersecurity workforce have changed as well. The introduction of each new technology pushes university faculty in cybersecurity programs to adjust their curricula to reflect the ever- changing demands of employers. We argue that the dynamic nature of the field of cybersecurity is often in tension with the static nature and organization of departments, programs, and courses (and their curricula) found in most university cybersecurity programs. University structures change slowly, requiring a significant amount of time, paperwork, and administrative oversight [5]. For a rapidly changing field such as cybersecurity the slow-to-change structure of most universities can create barriers to preparing a workforce with the capacity to keep pace with changing technologies and employer needs.

An additional dimension of this tension can be seen in that cybersecurity problems are systemic in nature, while our cybersecurity courses tend to teach point solutions [6], for example pentesting, forensics, policy, reverse engineering or cryptology. Often, instructors teach specific topics without contextualizing those subjects using a systems perspective [7], [8]. Yet, a cyberthreat operates through a complex system. Thus, agents working within the system need a broader understanding of that system to combat threats. In this article, we present a generalized systems-thinking approach for use at two levels in cybersecurity education. First, our framework serves as a means of designing program curriculum flexible enough to respond to rapid changes in the cybersecurity environment within and outside of the academy. Second, our framework can be used across cybersecurity-related courses to help contextualize and ground point solutions in complex cybersecurity systems to

develop students with a systems approach to the field. Our cybersecurity systems framework is intended to support faculty in adapting their instruction to meet the dynamic demands of the cybersecurity field within the constraints of institutions of higher education. We recommend approaches to teaching systems thinking in higher education programs, drawing on active learning strategies and research on conceptual learning activities in higher education.

II. Literature Review

A. Situating cybersecurity programs in higher education

Historically cybersecurity grew out of computer science (CS), mathematics (Math), and information technology management (ITM) departments. CS has yet to effectively address secure coding [9]. Math is teaching cryptography and cryptanalysis, but crypto represents a subset of security topics and implementations of cryptographic key management remain troublesome [10]. ITM has traditionally been teaching information technology management. Some programs may concentrate too much on industry certifications (e.g., Microsoft, Cisco, etc.). Cybersecurity education and training is generally found in six environments: four in the traditional degree-focused academic environment, technical training (certificate) programs at commercial training enterprises, and certification and continuing education activities of professional associations. In the academic world, the four environments are at the associate, bachelor's, master's, and doctoral degree levels. These degree levels tend to have different mixes of technical training and discipline education. While associate's curricula naturally tend heavily toward training courses, bachelor and master's programs vary widely in the balance between training and education courses. The variation across types of programs makes reforming cybersecurity education even more challenging.

Cybersecurity programs exist on most university campuses in the United States. A quick query of various cybersecurity programs reflects a threat-based paradigm provided as the basis for the course offerings. The threat-based paradigm is supported by the NICE framework [11]. While the framework is rather comprehensive in defining threats, vulnerabilities, and risk, we believe there is a lack of foundational guidance for cybersecurity educators. A lack of proper foundational courses could bias the students' understanding of the topic, and in many cases, may disrupt students' capacity to transfer knowledge across domains. Attempts have been made to create cybersecurity standards, frameworks, foundational knowledge, and workforce standards through various government and professional organizations. Several initiatives exist to provide cyber security curricular guidance: National Centers of Academic Excellence (CAE) program jointly sponsored by the Department of Homeland Security (DHS) and the National Security Agency (NSA); the Joint Task Force ACM/IEEE/AIS SIGSEC/IFIP on Cybersecurity Education (CSEC 2017) [12]; and the NIST National Initiative for Cybersecurity Education (NICE) [11]. These programs focus on curricula as a discipline crossing path of study [6]. Again, these are risk assessment and threat-based frameworks. The field of cybersecurity has yet to arrive at a common body of knowledge (CBK) that allows a cohesive foundational knowledge level for the cybersecurity discipline. A CBK represents an agreed upon nomenclature that is accepted by the profession. As an extension of the CSEC 2017, UK's National Cyber Security Centre created the Cybersecurity Body of Knowledge (CyBOK) [13]. (ISC)2 maintains the CISSP Common Body of Knowledge (CBK) [14], and the European Union Agency for Cybersecurity (ENISA) created guides and tools for member states [15]. Additionally, NIST maintains an online cybersecurity glossary [16]. With the disparate curriculum, workforce, and CBKs, it is no surprise many graduates would like simply to be pentesters!

Due to the transdisciplinary nature of the field, cybersecurity programs do not have a natural home in the traditional discipline and subdiscipline organization of the department-structure of higher education. Since cybersecurity education work may involve both transdisciplinary and interdisciplinary efforts, the descriptions below will help the reader distinguish between them:

> *Transdisciplinary Research* is defined as research efforts conducted by investigators from different disciplines working jointly to create new conceptual, theoretical, methodological, and translational innovations that integrate and move beyond discipline-specific approaches to address a common problem. *Interdisciplinary Research* is any study or group of studies undertaken by scholars from two or more distinct scientific disciplines. The research is based upon a conceptual model that links or integrates theoretical frameworks from those disciplines, uses study design and methodology that is not limited to any one field, and requires the use of perspectives and skills of the involved disciplines throughout multiple phases of the research process. [17].

Cybersecurity interacts with so many disciplines that designating a particular specific standalone STEM department exacerbates the existing academic silo problem. This may explain the gap between cybersecurity education supply (i.e., graduates) and the demand (i.e., jobs). The current university organization structure is antiquated, failing to meet the challenges the field is facing [18]. To help mitigate these structural barriers, we propose a cybersecurity transdisciplinary working group to discuss various curriculum solutions to the antiquated department structure that would fit for each institution. The solution has to be localized based on personnel expertise and available resources. Two potential solutions are described below: students take a set of common content courses before a discipline-specific curriculum (Figure 1), or students take common content courses midway or at the end of a discipline-specific curriculum [6].

A common core set of content can consist of foundational courses and primary cybersecurity courses that all students

will take in the *common cybersecurity curriculum*. As an example, common courses might consist of the following:

Common cybersecurity courses	
Network O/S Administration	Offensive Cybersecurity
Advanced Network Security	Digital Forensics
Advanced Network Administration	Applied Security Protocols
Wireless Security	IT Risk Assessment

Foundation courses	
Prog Constructs Laboratory	Info Security Fundamentals
Information Tech Architecture	Web Site Design
Data Communications	Intro to Data Management
Networking Fundamentals	Programming for NetSec

Then the curriculum can split into several specific cybersecurity *disciplines* such as (i) offensive security; (ii) industrial controls cybersecurity; (ii) cybersecurity risk assessment; (iv) defensive security, and (v) digital forensics. The core curriculum can come before the discipline specific content as seen in Figure 1. Alternatively, the core curriculum can be split before and in the middle of the *discipline specific* content as shown in Figure 2.

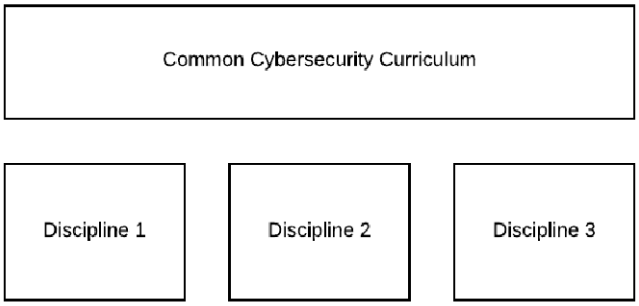

Fig. 1. Common cybersecurity curriculum preceding Disciplines

As we argued previously, cybersecurity is transdisciplinary in nature [19]. While cybersecurity touches everything, cybersecurity programs tend to exist in academic silos in higher education. There are several barriers to achieving the desired disciplinary merging. One major barrier is organizational, as attempts to introduce new courses must go through an approval process. Existing academia structure is not always set up for collaboration across departments and disciplines; the organization may even invite competition between departments, which is not conducive to transdisciplinary collaborations. For example, at a university with a strict activity-based budget model, competition over revenue could complicate collaboration efforts across departments. Another challenge within the current academic structure is communication across disciplinary divides. Even once a transdisciplinary team is formed, the team will need a common vocabulary for collaboration [16]. We believe that operating with a collaborative approach may dramatically reduce these challenges.

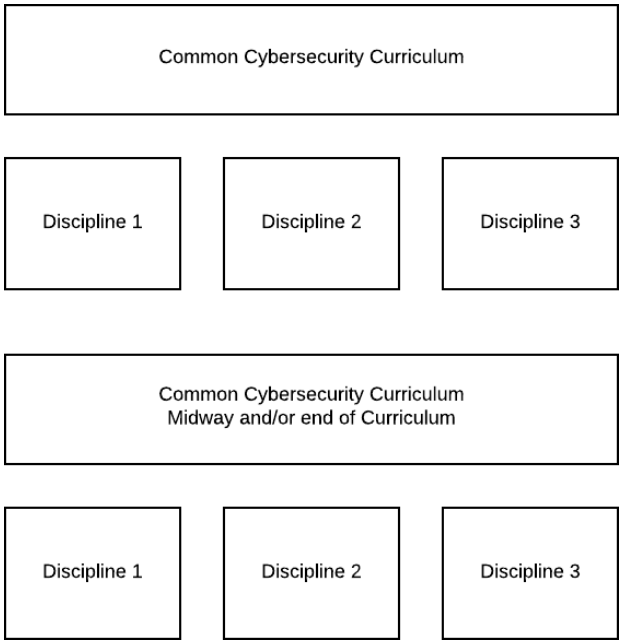

Fig. 2. Common cybersecurity curriculum interspersed with Disciplines

B. Teaching systems-thinking across cybersecurity coursework

In cybersecurity, we are not confronted with problems independent of each other. We manage complexity, juggle budget requirements, and plan for challenges that impact coverage, such as intended/unintended consequences, over-promising, and personnel limitations. Cybersecurity deals with people, processes, tools, technology, and metrics. Cybersecurity functions as a system of systems within an ecosystem. To understand cybersecurity well, a comprehension of system thinking is critical.

The early days of cybersecurity where signatures prevailed reflected the reductionist view since the problems were easily defined. Changes in cybersecurity have resulted in an open, dynamic environment that extends beyond hardware and software into wetware. This change requires a broader and inductive approach to student education that teaches the theoretical while reinforcing the broad concepts with applied exercises. Von Bertalanffy [7], "the father of systems theory" [8] advocated for holism. Coincidentally, cybersecurity experts have also been advocating for holism [20], and expansions into holistic thinking in cybersecurity appear with the relatively newer emphasis on situational

awareness [21]. A potential benefit to cybersecurity may exist in adopting a systems approach. The systems approach to security architecture has been successfully adopted by the SABSA Institute; where security practitioners undergo additional training for various levels of SABSA certifications. This opportunity to introduce cybersecurity professionals to holistic thinking should extend to the earliest exposures so that holistic thinking becomes an automatic process.

Increasingly, aspects of complex systems such as swarming and emergent phenomenon [22] have been examined in cybersecurity research. This reflects the acknowledgment of complexity found in cybersecurity events and systems. Research efforts [23], [24], [25], [26], [27], [28], reflect the merging of complexity and cybersecurity as a means to explain cybersecurity incidents and events within a larger comprehensive framework. We argue that students benefit from understanding a systems theory framework reinforced through active learning activities. The importance of active learning in cybersecurity education is discussed in Section 3 C.

The ability to transfer cybersecurity knowledge and skills across disciplines is becoming increasingly important as illustrated by the introduction of data science into cybersecurity [29]. The increasing awareness of the interdisciplinary nature of cybersecurity requires that students and practitioners work with an overarching educational framework that can be applied to cybersecurity courses as well as other related fields. The framework would need to be foundational, so the lessons learned would be reinforced throughout the learning process. At the beginning and end of every course, students should be able to identify the part of the systems framework on which they are working. The decentralized nature of cybersecurity programs in higher education creates significant challenges to developing unifying knowledge, skills, and dispositions in the cybersecurity workforce. We argue that our cybersecurity systems framework can help bridge some of these gaps.

III. Conceptual Framework

A. Defining system thinking

Defining systems thinking requires a contextual definition of *system*. Context is important, because related disciplines use the term *system* differently. For instance, in computer science and electrical engineering *system* refer to a *computer system*, hardware and software, neglecting the people using the computer and the procedures they follow. INCOSE provided a useful definition for systems engineering which works well in the broader systems thinking context:

> An integrated set of elements, sub-systems, or assemblies that accomplish a defined objective. These elements include products (hardware, software, firmware), processes, people, information, techniques, facilities, services, and other support elements. [30, p. 265].

Systems thinking is an approach to planning projects or solving problems that incorporates a variety of tools with the goal of using a holistic or "big picture" [30, pp. 20-21] approach. A complete explanation of systems thinking is beyond the scope of this paper; three significant sources, INCOSE [30], MITRE [31,], and SEBoK [32] each devote a major section of a chapter to the concept. That said, MITRE introduced the section on systems thinking with the following simple definition, quoting two authors:

> The ability and practice of examining the whole rather than focusing on isolated problems (P. Senge) [1]. The act of taking into account the interactions and relationships of a system with its containing environment (Y. Bar Yam, New England Complex Systems Institute) [31, p. 31].

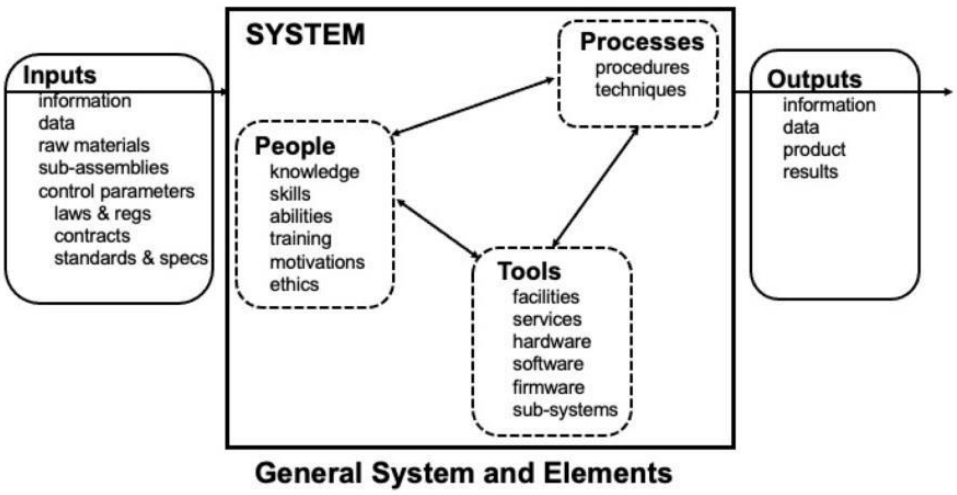

Fig. 3. General system framework

Practitioners of systems management and systems engineering often simplify the collection of system elements, grouping the elements into *people*, *processes*, and *tools*. Figure 3 illustrates this framework, useful for describing any system based on the desired output, the known inputs, and the necessary system elements. Figure 3 is a visual model of the general system framework concept, grouping system elements under the three types inside the system with a defined boundary, as well as elements of the two external groups of inputs to the system and outputs from the system. (Note that Figure 3 is not a workflow diagram, which is why no feedback loop is included.) This general framework is a useful tool for identifying the key aspects of any system, to include the known inputs, expected outputs, setting a system boundary, and identifying key elements essential to producing the output. Clear identification of the elements allows decisions on which elements to use to accomplish the goal outputs.

B. *Applying systems-thinking to cybersecurity programs*

Figure 4 provides an example of using the general system framework to describe an enterprise cybersecurity environment. The items listed are not exhaustive but represent what might be selected in a specific enterprise environment. Once developed to a satisfactory level of detail, the items in such a framework could be used to select topics for inclusion in courses of a structured curriculum intended to develop graduates to take part in an enterprise security practice. This example also demonstrates how a program graduate attuned to using systems thinking could approach various responsibilities while working in a security organization.

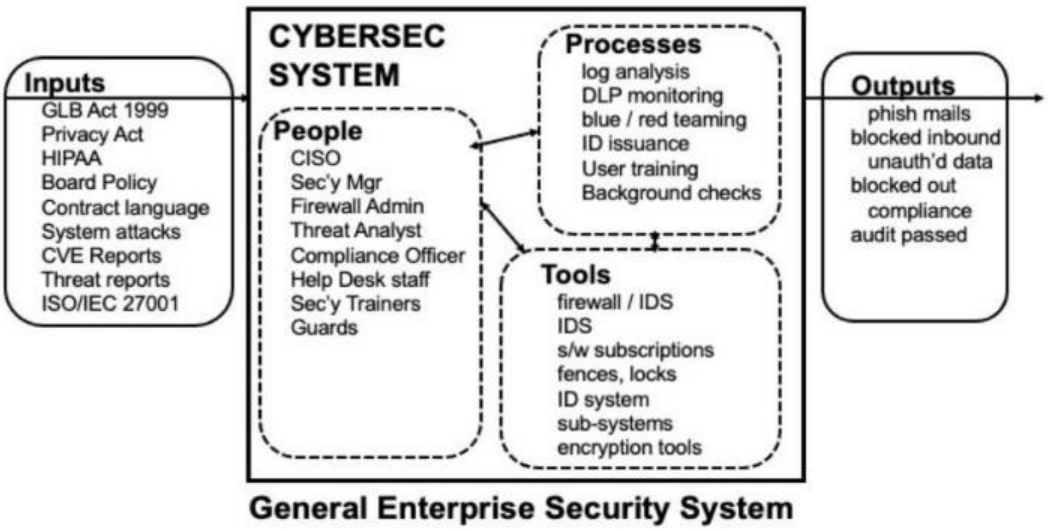

Fig. 4. A system framework for cybersecurity

C. *Leveraging active learning strategies in cybersecurity instruction to foster systems-thinking*

Not only are the content of and approach to teaching systems thinking in cybersecurity programs critical, the strategies used to teach systems thinking also merit attention. After reviewing the research on cybersecurity programs, we argue for the integration of active-learning strategies to improve access to meaningful learning for all postsecondary cybersecurity students. A meta- analysis of 225 studies found that students had better course outcomes in university STEM courses that utilize active learning strategies than those that utilize traditional lecturing [33]. A study on active learning in a large biology course showed that students who engaged with an active learning strategy had higher exam scores than those who did not [34]. In particular, we urge the use of conceptually oriented tasks, shown to increase students' retention, comprehension, and application [35].

One particularly promising instructional tool is case study analysis, which can be designed to be an active-learning activity as well as a conceptually oriented task. We also believe that case study analysis is particularly well suited to the integration of systems-thinking into cybersecurity coursework. Moreover, engaging students in analytical tasks as a part of case study analysis, such as concept mapping, has the potential to support students' clarification, integration, and organization of complex concepts [36]. In other terms, a key benefit of leveraging these active learning strategies -- case study analysis and concept mapping -- in cybersecurity coursework would be to help students learn to contextualize point-solutions in a complex cybersecurity system using the systems-thinking framework previously presented.

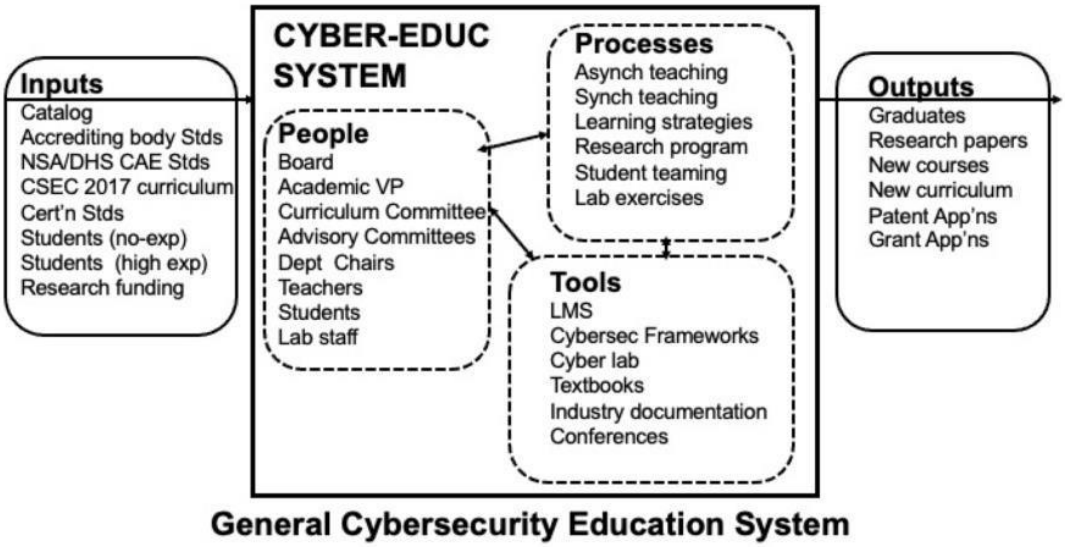

Fig. 5. A system framework for cybersecurity education

Figure 5 illustrates the use of the general system framework model to describe a cybersecurity education program as a system with identified inputs and desired outputs. As with other applications of the framework model, using this tool to explicitly identify system elements may help focus attention on selecting the optimum system elements to generate the goal outputs. For a given output (e.g. a funding grant application), this model can help determine which people can use which tools in what processes to generate the desired output. Visualizing the options in this way can assist in optimizing use of resources, and even balancing the load on high-use resources, whether people or tools.

IV. Conclusion and Future Work

The challenge of achieving holistic cybersecurity depends on people – arguably even more so than on technology (tools) or policy (processes). The workforce shortage within cybersecurity is well documented - opportunities abound but hiring and staffing within the current model is not sustainable. Future careers in almost every industry and discipline will require an understanding of both technology and the underlying logic necessary to evaluate risk, mitigate threats, and adjust strategies. The need to train more cybersecurity professionals will remain but building a resilient workforce, one capable of adapting to the everchanging cyber-landscape is a promising approach to ensuring that those in the field remain engaged and are effective. This high-quality preparation requires a more active learning approach to cybersecurity education that emphasizes critical thinking, problem solving and systems thinking.

The Cyberspace Solarium Commission report [37], included several supporting recommendations to address the recruitment, development and retention of cyber talent by promoting digital literacy, civics education, and public awareness. The report also referenced the need to build societal resilience and improve cyber-oriented education. To address these needs, cybersecurity education will need to take a more holistic approach. Cybersecurity as a field is still maturing. In many ways, cybersecurity has many parallels to medicine as a field, from its organization into specialties and subspecialties to the overarching need to understand system interdependencies while working in concert to heal and do no harm. The needed skills and logic are continually developing as are the approaches to instruction and collaboration. This ecosystem is broader and more pervasive than the current domains in which it is taught, providing the opportunity to create new programs, curricula, and training, designed to reach a broader range of students. In turn, leveraging existing models to incorporate greater resilience and critical thinking, in the students and the field as a whole, may bridge gaps across our current needs, existing resources, and future demands.

Adopting systems thinking into cybersecurity education institutions may be able to improve the resiliency and robustness of the discipline while creating more resilient and adaptive students. These empowered students can utilize their problem-solving skills in the very domains that cybersecurity must interact. Furthermore, these students will possess the necessary tools to prevent obsolescence when new AI/ML based technologies replace many of the jobs for which higher education currently prepares students. Recognizing that introducing new courses is a time-consuming process, the ability to provide foundational courses in systems thinking provides a reasonable entry point.

Historically, cybersecurity has been reactive to events; this reactive focus must change to a proactive focus. For example, the patch and run model has been present since the Morris Worm. Proactive cybersecurity is the ultimate goal.

Hackers continue to test assumptions made by developers, which feeds the traditional reactive model resulting in a significant amount of certification training. Professionals attempt to remain relevant in the field through these certificates, yet those programs are limiting. As technology continues to grow, and the AI footprint in cybersecurity grows as well, professionals will need cybersecurity programs that extend beyond point solutions to help them learn to be resilient and adaptive. Integrating systems thinking into these programs could provide the needed adaptive processes.

Cybersecurity educators are facing increasing challenges to better support students through their teaching. The rise of AI along with the transdisciplinary nature of the field requires students to become conversant in other complementary subjects as well as cybersecurity. If we do not educate students in other areas we will create gaps that run the risk of inconsistent solutions. Cybersecurity as a field must both mature and broaden. These goals often exist in tension since in order to mature a field focuses inward gathering metadata for abstraction, which can make expansion a challenge. Cybersecurity must become more resilient to the changing landscape. Additionally, cybersecurity educators need to ensure broader access and participation in the field, which among other initiatives, means utilizing active learning strategies. As cybersecurity as a field becomes more mature, broader, and more resilient, cybersecurity education also needs to develop in pace with advances in higher education teaching and learning to provide cybersecurity students with rich learning opportunities that develop their systems-thinking.

REFERENCES

[1] W. R. Cheswick, S. M. Bellovin, and A. D. Rubin, *Firewalls and Internet security: repelling the wily hacker*. Addison-Wesley Longman Publishing Co., Inc. 2003.

[2] H. J. Liao, C. Lin, C. H. R., Lin, Y. C., and K. Y. Tung. "Intrusion detection system: A comprehensive review". *J. of Netw. and Comput. Appl*., vol. 36, no. 1, pp. 16-24, 2013.

[3] H. Debar and J. Viinikka, "Intrusion detection: Introduction to intrusion detection and security information management," in *Foundations of security analysis and design III*, Springer, Berlin, Heidelberg, pp. 207-236, 2005.

[4] A. L. Buczak and E. Guven. "A survey of data mining and machine learning methods for cyber security intrusion detection," *IEEE Commun. Surveys & Tutorials*, vol. 18, no. 2, pp.1153-1176, 2015.

[5] B. Sporn, "Governance and administration: Organizational and structural trends," in *International Handbook of Higher Education*. Springer, Dordrecht, 2007.

[6] Justice, C. Sample, and E. Darraj, "Future Needs of the Cybersecurity Workforce", 2020. *19th European Conference on Cyber Warfare and Security, ECCWS 2020*, University of Chester, UK, 25 - 26 June 2020. unpublished. [Online] https://www.academic-conferences.org/conferences/eccws/

[7] L. Von Bertalanffy. "The history and status of general systems theory," *Acad. of Manage. J*., vol. 15, no. 4, pp. 407-426, Dec. 1972 [Online] doi: 10.2307/255139. Available: https://www.jstor.org/stable/255139

[8] J.P. Van Gigch, *System Design Modeling and Metamodeling*, New York, NT, USA: Plenum Press, 1991.

[9] J. Viega and G. McGraw, *Building Secure Software: How to Avoid Security Problems the Right Way*, Addison-Wesley, Reading, MA, USA: 2011.

[10] I. Curry, *An Introduction to Cryptography and Digital Signatures*, Entrust. 2001. [Online] Available: https://www.entrust.com/wp-content/uploads/2013/05/cryptointro.pdf

[11] W. Newhouse, S. Keith, B. Scribner, and G. Witte, *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (SP 800- 181)*. Gaithersberg, MD, USA: NIST, 2017. [Online] Available: https://doi.org/10.6028/NIST.SP.800-181

[12] Joint Task Force on Cybersecurity Education (JTF), Cybersecurity Curricula 2017, [Online] Available: https://cybered.hosting.acm.org/wp/ Download: https://cybered.hosting.acm.org/wp-content/uploads/2018/02/newcover_csec2017.pdf

[13] *The Cybersecurity Body of Knowledge*. Crown Copyright, The National Cyber Security Centre 2019. [Online] Available: https://www.cybok.org

[14] J. Warsinske, M. Graff, K. Henry, C. Hoover, B. Malisow, S. Murphy, C. P. Oakes, G.e Pajari, J. T. Parker, D. Seidl, and M. Vasquez, *The Official (ISC)2 Guide to the CISSP CBK Reference, 5th Ed*., Hoboken, NJ, USA: Wiley, 2019.

[15] European Union Agency for Cybersecurity (EISA) [Online] https://www.enisa.europa.eu/topics/national-cyber-security-strategies

[16] *Glossary*, NIST Computer Security Resource Center [Online] Available: https://csrc.nist.gov/glossary

[17] S. W. Aboelela, E. Larson, S. Bakken, O. Carrasquillo, A. Formicola, S. A. Glied, J. Haas, K. M. and Gebbie, "Defining Interdisciplinary Research: Conclusions from a Critical Review of the Literature," *Health Services Res*., vol. 42, 2007, pp. 329–346, 2007, doi: 10.1111/j.1475-6773.2006.00621.x as cited in *Definitions, Harvard Transdisciplinary Research in Energetics and Cancer Center* [Online] Available: https://www.hsph.harvard.edu/trec/about-us/definitions/

[18] S. A. McChrystal, T. Collins, D. Silverman, and C. Fussell. *Team of teams: new rules of engagement for a complex world*. New York, USA, Penguin Random House, 2015.

[19] D. Craigen, N. Diakun-Thibault, and R. Purse, "Defining cybersecurity" *Technology Innovation Manage. Rev*., 4(10). 2014.

[20] K. T. Dean, *Cyber-Security Holism: A System of Solutions for a Distributed Problem*. USMC C&S Col, Quantico, VA, USA: Pennyhill Press, 2013.

[21] H. Tianfield, Cyber security situational awareness. In *2016 IEEE int. Conf. on Internet of Things (iThings)* and *IEEE green computing and communications (GreenCom)* and *IEEE cyber, physical and social computing (CPSCom) and IEEE smart data (SmartData)* (pp. 782-787). IEEE, Dec. 2016.

[22] G. A. Fink, J. N. Haack, A. D. McKinnon, and E. W. Fulp, "Defense on the move: anti-based cyber defense," *IEEE Secur. & Privacy*, vol. 12, no. 2, pp. 36- 43, 2014.

[23] S. M. Loo and L. Babinkostova, "Cyber-physical Systems Security Introductory Course For Stem Students," *2020 Annual ASEE Conf*., June 20-24, Montreal, Canada.

[24] C. Sample, S. M. Loo, C. Justice, E. Taylor, and C. Hampton, "Cyber-Informed: Bridging Cyber Security and Other Disciplines," *19th European Conference on Cyber Warfare and Security*, June 25-26, 2020, Chester, UK.

[25] Centre for Complexity Science, U. of Warwick, [Online] Website: https://warwick.ac.uk/fac/cross_fac/complexity

[26] L. Chittka, Queen Mary U. London, [Online] Website: https://www.qmul.ac.uk/sbcs/staff/larschittka.html

[27] B. J. West, B, "Colloquium: Fractional calculus view of complexity: A tutorial." *Reviews of Modern Physics*, vol. 86 no. 4, p. 1169, Dec. 2014. [Online] Available:

https://journals.aps.org/rmp/abstract/10.1103/RevModPhys.86.1169#fulltext

[28] B. P. Turnbull, Researcher, Univ New S. Wales, [Online] Website: https://research.unsw.edu.au/people/dr-benjamin-peter-turnbull

[29] D. McMorrow, ED. *Science of cyber-security* (Report No. JSR-10-102). McLean, VA, USA: JASON Program Office, MITRE Corp, 2010.

[30] D. D. Walden, G. J. Roedler, K. J. Forsberg, and T. M. Shortell, Eds. *Systems Engineering Handbook, 4th ed*. Hoboken, NJ, USA: John Wiley & Sons, 2015.

[31] G. Rebovich, Jr., Ed. *MITRE Systems Engineering Guide*, Burlington, MA, USA: MITRE Corp., 2014. [Online] Available: https://www.mitre.org/publications/technical-papers/the-mitre-systems- engineering-guide

[32] R.J. Cloutier, Ed. in C., SEBoK Editorial Board. *The Guide to the Syst. Eng. Body of Knowl. (SEBoK), v. 2.1*, . Hoboken, NJ. 2019. [Online] Available: https://www.sebokwiki.org/ Download: https://www.sebokwiki.org/w/images/sebokwiki-farm!w/8/8b/SEBoK_v2.1.pdf

[33] S. Freeman, S. L. Eddy, M. McDonough, M. K. Smith, N. Okoroafor, H. Jordt, and M. P. Wenderoth, "Active learning increases student performance in science, engineering, and mathematics," *Proc. of the Nat. Acad. of Sciences*, vol. 111, pp. 8410-8415, 2014.

[34] P.A. Ertmer, J. A. Quinn, and K. D. Glazewski, Eds., *The ID casebook: Case studies in instructional design, 5th ed*., Evanston, IL, USA: Routledge, 2019.

[35] M. A. Ruiz-Primo, D. Briggs, H. Iverson, R. Talbot, and L. Shepard, "Impact of undergraduate science course innovations on learning," *Science*, vol. 331, pp. 1269-1270, 2011.

[36] B. J. Daley and D.M. Torre, "Concept maps in medical education: an analytical literature review." *Medical Educ*., vol. 44 no. 5, pp. 440-8, 2010.

[37] A. King and M. Gallagher, Eds., *Cyberspace Solarium Commission [Report]*, Washington, DC, USA: Cyberspace Solarium Commission, March 2020. [Online] Available: https://www.solarium.gov/, https://drive.google.com/file/d/1ryMCIL_dZ30QyjFqFkkf10MxIXJGT4yv/view