Exploring Open Educational Resources in Cyber Training

Alan A. Stines and Houssain Kettani

***Abstract*—Advances in internet technologies continue enabling users across the globe access to information on-demand and at low cost. Taking advantage of this proliferation of information sharing is transforming how individuals learn and develop new skills for use in everyday life. Open learning materials provide a unique opportunity to many life-long learners wishing to pursue their interests. Many initiatives for creating and adopting Open Educational Resources (OER) in traditional learning environments are showing great promise for enriching the learning experience. Open materials can offer new opportunities for individuals seeking knowledge; but many limitations of OER can influence the effectiveness in learning. As a new and rapidly evolving field, cybersecurity presents unique challenges for individuals wishing to develop new and refine existing knowledge to maintain relevance. Educators face additional challenges of keeping up with industry trends, preparing students with both technical and critical thinking skills to excel in the field, and developing cyber curricula that provide pathways to the workforce. As the demand for cyber professionals in the workforce increases; developing new pathways for students to acquire relevant skills becomes imperative for securing our culture's digital infrastructure. This paper seeks to identify potential barriers and benefits for those wishing to supplement learning experiences in the field of cybersecurity by creating and adopting OER.**

***Index Terms*—Open Educational Resources (OER), cyber education.**

I. Introduction

The cyber landscape continues to evolve at a fast pace. An annual report from the European Union Agency for Network and Information Security (ENISA) demonstrates a shifting landscape of a wide variety of topics related to cybersecurity. In 2018 alone, many new emerging attack threats emerged that require constant development and refinement of skills by professionals to identify and respond to these cyber developments [1]. For all that these topics display the landscape in-breadth; it takes very deep skillsets from individuals to make an impact on cyber readiness overall. Cyber professionals become life-long learners of their trade; constantly following developments in the field to address new, changing, and more sophisticated attacks. The United States' Department of Defense (DoD) is taking strong initiatives to develop partnerships in industry, academia, and government bodies as a key initiative in its strategic plan. Through collaboration and resource sharing throughout the industry can new individuals begin to develop the skills needed to succeed in the workplace [2].

Manuscript received November 24, 2018; revised March 1, 2019.

The authors are with the Beacom College of Computer & Cyber Sciences, Dakota State University, Madison, South Dakota 57042 USA (e-mail: alan.stines@mga.edu, houssain.kettani@dsu.edu).

Using tools in cyber practices is a big part of performing job duties; but practitioners cannot be reliant on just using tools alone. Technical skills complement analytical skills to build a well-rounded cyber professional. The field requires skills that go deeper into researching how attacks happen and creating mitigations that prevent their success. This often requires problem-solving skills in addition to highly technical skills like programming to create new tools in this shifting environment. Educators should strive to not focus on teaching specific tools for techniques in identifying and preventing cyber threats; but instead try to bestow a more investigative and operations standpoint to learning cyber operations practices [3]. While efforts continue, there is a gap in to deliver qualified students to meet the needs of the evolving workforce [4]. Equipping students with knowledge, skills, and abilities to succeed in the workforce continues to evolve. In addition to preventing and mitigating attacks, professionals must create resilient systems and practices for recovering from cyber events [5].

Knowledge of programming structures and logic presents major core literacies in development of cyber professional skills. Forging new pathways in education to elevate computer literacy to that of reading, writing, and mathematical literacy is pivotal in preparing individuals in the digital age [6]. A recent survey from the Organisation for Economic Co-operation and Development (OECD) found that individuals with higher literacy and problem-solving skills in technology-rich environments are more employable and tend to have higher wages. The outlook on the labor force also shows in increase in demand for individuals to enter the workforce computer skills and problem-solving competencies [7]. Research into the digital divide, those with skills and access to technology and those without, covers how individuals interact with Internet and Communication Technologies (ICT). Although taking many forms, the digital divide creates a bottleneck for many individuals to learn new skills and problem-solving abilities in ICT environments [8].

Open educational materials provide a unique opportunity for individuals in reducing barriers to educational endeavors. No cost materials, cheap distributions methods like the Internet and diversity of topics available is transforming learning for individuals across the globe [9]. In particular, open materials availability on mobile devices is becoming increasingly popular for accessing information [10]. Individuals seeking to transform the landscape of cybersecurity education can create and find resources to shape technical, analytical and problem-solving skills needed for the cyber workforce. This paper surveys the literature to discover the benefits, drawbacks, and considerations developers and adopters of Open Educational Resources (OER) may have when dealing with cybersecurity topics.

doi: 10.18178/ijch.2019.5.3.139

II. Needs of Cyber Workforce

The National Cybersecurity Workforce Framework (NCWF) by the National Initiative for Cyber Education (NICE) is an effort to increase cyber awareness for workforce development needs. The framework identifies seven key areas to the cybersecurity field, which does not use jargon or technical languages, based on different roles cybersecurity professionals may work in the field [11]. These non-technical descriptions help eliminate language barriers to individuals with low computer skills to understand and interpret concepts into learning about the field. There are two major viewpoints in relationship to building a cybersecurity workforce as identified in the literature [12]. The first involves taking in introspective look to the needs-based demand on the cybersecurity field, while the second provides a call to partnerships through the Center of Academic Excellence (CAE) designated schools for cyber curriculum development. Institutions of higher learning that have CAE certifications from the National Security Agency (NSA) and Department of Homeland Security (DHS) must undergo a rigorous process for curriculum certification that covers cybersecurity focus areas [13].

In a recent survey of cybersecurity professionals, results suggest of the top ten skills and abilities identified as important to the job; all were learned mostly on-the-job by the individual to fill a required task. Learning the knowledge from a school setting showed second most important for only three of the most important skills. Individuals reported that most of the top skills required in the cybersecurity they acquired are either on-the-job or self-taught. Limitations to this study if that the concept of self-taught versus school setting might be ambiguous; the Knowledge, Skills, and Abilities (KSAs) could have been covered in course curricula in school but additionally learned from self-learning or on-the-job. Questions on the survey asked what medium of instruction was most beneficial to their learning; so multiple forms of learning for the same KSA could apply. The only KSA associated with programming logic and structures did participants rate a school environment as being most beneficial to their learning for exercising job performance [14].

There is a need for colleges and universities to develop pathways to the workforce and partnerships with industry to give students the skills they need to succeed in the workforce [12]. Working towards a secure digital infrastructure through cybersecurity can be seen as a public good and akin towards providing safety for society [15]. Building communities of responsible computer users will rely on extending cyber awareness beyond computer science curriculum into other disciplines of study and contexts [11]. Research relating to digital citizenship builds upon this notion that users must take some ownership of their role in digital society [16]. Raising awareness of the benefits, risks and consequences of participating in digital interactions is increasingly becoming common in K-12 educational environments [17]. Institutions that embrace and teach digital citizenry concepts may have an advantage in incorporating deeper cybersecurity related content into the curriculum.

III. Cyber Curriculum Development

Developing materials for cyber training comes with many challenges. The shifting landscape means that materials must undergo improvement cycles for relevance in real world scenarios. Individuals cannot expect to come prepared to the field of cyber for each and every scenario that may occur; instead educators must focus on the bestowing relevant skills needed to excel in the field from both hard and soft skill points of view [14]. Further research shows that hands-on exercises and case studies can be very beneficial to improving understanding and retention of cyber trainings in general. Those in the field of cyber must develop a diverse set of skills to tackle the wide array of topics that exists in real-life scenarios and try to align learning objectives to that of the workforce. An underlying theme that individuals should keep in mind is that there is little research to show that cyber curricula meet the needs of the industry [11].

Professional certifications may hold a key to shaping cybersecurity curricula. Industry certifications help qualify that individuals have the knowledge, skills and abilities for work in the job field. Educators can find value by shaping and refining curriculum based on certifying organizations and their pursuits to remain relevant in a changing landscape to the needs of the cybersecurity workforce. Many certifications exist across many different subject areas; but educators should not focus to any one certification. Maintaining knowledge of respected industry certifications, and how they evolve to meet the needs of industry, could provide great insights for those wishing to create and refine cyber curriculum to meet the needs of the workforce. Certifying bodies that undergo regular updates to maintain content for relevancy to the field may help educators stay relevant. It is important for educators to acknowledge that education should not focus on qualifying individuals for a particular certification or test; but instead bestow the skills and abilities needed to learn new techniques and trends [18].

Some curriculum developers suggest that cyber education programs need to extend beyond the traditional classroom environment to entail more extracurricular activities and partnerships with local industries requiring individuals with cyber skills. These partnerships and learning opportunities can help develop new opportunities for learners to practice the skills they need to succeed in the industry [13]. Expanding beyond computer-related disciplines, proponents of cyber literacy may begin to run into new issues spreading awareness of topics in today's world. The digital divide for knowledge pertaining to Information and Communications Technologies (ICTs) continues to separate not only those with the skills and abilities to perform simple computer-related tasks; but for individuals to bridge the barrier between not just being consumers of technology, but those that really understand how it works in-depth [19]. Technology proliferation continues to evolve as more people gain access to the Internet; but assuming all learners have access to such ICT devices is still premature [8]. The rise in mobile devices and faster mobile broadband speeds holds high potential as a possible conduit for reaching out to individuals in bridging the digital divide but cost of such devices and access continues to be a limiting factor for many individuals [20]. Capitalizing on

OER and mobile device access continues to be an interesting area of study for furthering educational goals for those who did not have access to it before [10].

IV. Pathways to Mass Education

Open Educational Resources (OER) provide educators unique opportunities to transform learning for individuals across the world [9]. Since 2002, the United Nations Educational Scientific and Cultural Organization (UNESCO) and other proponents of OER continue to embrace the development and adoption of open learning materials to supply and improve learning [21]. Many free resources exist for students and educators to help them improve student learning and engagement. Educators should be encouraged to seek out new resources on materials and build their own content as a sum of parts [22]. Development and adoption of OER resources continues to increase among educators and institutions wanting to leverage benefits to embracing OER [23]. This research will focus on UNESCO's definition of OER described as "teaching, learning, and research materials in any medium, digital or otherwise, that reside in the public domain or have been released under an open license that permits no-cost access, use, adaptation, and redistribution by others with no or limited restrictions."

For what OER can help to improve learning environments, there are some limitations that adopters should consider when adopting OER. As identified in [24], three main tensions exist for educators using a mixed methodology when engaging with OER resources. The barriers include tensions between organizational policies and needs of the individual educator, institutional responsibility to maintain academic integrity, and the balance between cost efficiency and learning objectives for students. Educators can spend as much or more time building course materials when using open materials [25] and developing a sustainable financial and evaluation models for continuous improvement over time eludes many institutions [26]. Ultimately, the decision to adopt OER must be up to the individual and institutions should consider its use; but not mandate educators conform to no-cost course resource options [27].

The Resource Inspection, Selection, and Enhancement (RISE) Framework is a useful mechanism for helping educators streamline the process for finding, selecting and enhancing OER resources fulfill learning outcomes using continuous improvement [28]. The feedback loops in the model help drive future development as materials are refined over time and constant tweaking applied to improve pedagogy and deliver of materials. This process may help alleviate tensions that OER is not of academic and professional quality. Although this research is not yet complete, it holds great promise to laying a foundational framework for evaluating student performance in OER contexts. Students also are open to using open learning materials for coursework to replace traditional purchased textbooks and exhibit higher engagement rates than with traditional learning materials [29]. However, students do exhibit barriers when it comes to accessibility on online materials and the quality of material that they learn. Overall most individuals may consider OER resources to at least as good as traditional textbook usage in a learning environment [25]. Research into using OER has drastically increased in recent years with academic and research communities becoming more receptive to incorporating OER [30].

V. Conclusion

Exploring the literature, there is a strong need for cooperation between governments, industry, and educational institutions to collaborate on building a workforce that can adapt to changing needs in the field of cybersecurity. As the field of cyber continues to grow; evolving new topics on critical infrastructures, creating resilient systems, and extending cybersecurity principles to all technology users is of increasing importance to securing society's digital infrastructure. Technical training is not enough to satisfy the needs of the workforce; analytical, problem solving, and communications skills need to complement technical skills so that individuals can adapt to changing environments. New possibilities are introduced by OER to shape learning environments for many individuals across the globe. Limitations and misconceptions of OER play a role in adoption and creation; but OER can provide new and engaging opportunities for learners to tackle new topics. Encouraging cyber professionals, industry leaders, and educators to create, contribute, and adopt open learning materials could help bring a more mature and safe digital society.

References

[1] European Union Agency for Network and Information Security (ENISA). (2019). *ENISA Threat Landscape Report 2018: 15 Top Cyber-Threats and Trends*. Heraklion: ENISA. [Online]. Available: https://doi.org/10.2824/622757

[2] M. Myauo, "The U.S. department of defense cyber strategy: A call to action for partnership," *Georgetown Journal of International Affairs*, vol. 17, no. 3, pp. 21–29, 2016.

[3] J. Pauli and P. Engebretson, "Filling your cyber operations training toolbox," *IEEE Security & Privacy*, vol. 10, no. 5, pp. 71–74, 2012.

[4] D. E. Krutz and T. Richards, "Cyber security education: why don't we do anything about it?" *ACM Inroads*, vol. 8, no. 4, pp. 5–5, 2017.

[5] L. O. Mailloux and M. Grimaila, "Advancing cybersecurity: The growing need for a cyber-resiliency workforce," *IT Professional*, vol. 20, no. 3, pp. 23–30, 2018.

[6] J. Arquilla and M. Guzdial, "Crafting a national cyberdefense, and preparing to support computational literacy," *Communications of the ACM*, vol. 60, no. 4, pp. 10–11, 2017.

[7] Organisation for Economic Co-operation and Development (OECD). (2018). Skills on the move: Migrants in the survey of adult skills. *OECD Skills Studies*. Paris: OECD Publishing. [Online]. Available: https://doi.org/10.1787/9789264307353-en

[8] J. Rowsell, E. Morrell, and D. E. Alvermann, "Confronting the digital divide: Debunking brave new world discourses," *The Reading Teacher*, vol. 71, no. 2, pp. 157–165, 2017.

[9] T. Richter and M. McPherson, "Open educational resources: Education for the world?" *Distance Education*, vol. 33, no. 2, pp. 201–219, 2012.

[10] M. Ally and M. Samaka, "Open education resources and mobile technology to narrow the learning divide," *The International Review of Research in Open and Distributed Learning*, vol. 14, no. 2, p. 14, 2013.

[11] H. Santos, T. Pereira, and I. Mendes, "Challenges and reflections in designing cyber security curriculum," in *Proc. the 2017 IEEE World Engineering Education Conference (EDUNINE 2017)*, Santos, Brazil, 2017, pp. 47–51.

[12] S. E. Goodman, "Building the nation's cyber security workforce: Contributions from CAE colleges and universities," *ACM*

Transactions on Management Information Systems, vol. 5, no. 2, pp. 1–9, 2014.
[13] B. Woodward, T. Imboden, and N. L. Martin, "An undergraduate information security program: More than a curriculum," *Journal of Information Systems Education*, vol. 24, no. 1, pp. 63–70, 2013.
[14] K. S. Jones, A. S. Namin, and M. E. Armstrong, "The core cyber-defense knowledge, skills, and abilities that cybersecurity students should learn in school: Results from interviews with cybersecurity professionals," *ACM Transactions on Computing Education*, vol. 18, no. 3, pp. 1–12, 2018.
[15] A. Asllani, C. S. White, and L. Ettkin, "Viewing cybersecurity as a public good: The role of governments, businesses, and individuals," *Journal of Legal, Ethical and Regulatory Issues*, vol. 16, no. 1, pp. 7–14, 2013.
[16] R. Hollandsworth, L. Dowdy, and J. Donovan, "Digital citizenship in K-12: it takes a village," *TechTrends*, vol. 55, no. 4, pp. 37–47, 2011.
[17] R. Hollandsworth, J. Donovan, and M. Welch, "Digital citizenship: You can't go home again," *TechTrends*, vol. 61, no. 6, pp. 524–530, 2017.
[18] K. J. Knapp, C. Maurer, and M. Plachkinova, "Maintaining a cybersecurity curriculum: Professional certifications as valuable guidance," *Journal of Information Systems Education*, vol. 28, no. 2, pp. 101–113, 2017.
[19] S. E. Rogers, "Bridging the 21st century digital divide," *TechTrends*, vol. 60, no. 3, pp. 197–199, 2016.
[20] U. S. Department of Commerce: National Telecommunications and Information Administration, "Exploring the digital nation: Embracing the mobile internet," *Journal of Current Issues in Media & Telecommunications*, vol. 6, no. 4, pp. 417–461, 2014.
[21] United Nations Educational Scientific and Cultural Organization (UNESCO). (2002). *Forum on the Impact of Open Courseware for Higher Education in Developing Countries: Final Report*. (Report No. CI-2002/CONF.803/CLD.1). Paris: UNESCO. [Online]. Available: http://unesdoc.unesco.org/images/0012/001285/128515e.pdf
[22] D. Johnson, "Open educational resources: On the web and free," *Educational Leadership*, vol. 71, no. 6, pp. 85–87, 2014.
[23] A. Adams, T. Liyanagunawardena, N. Rassool, and S. Williams, "Use of open educational resources in higher education," *British Journal of Educational Technology*, vol. 44, no. 5, pp. 149–150, 2013.
[24] H. Kaatrakoski, A. Littlejohn, and N. Hood, "Learning challenges in higher education: An analysis of contradictions within open educational practice," *Higher Education*, vol. 74, no. 4, pp. 599–615, 2017.
[25] T. Bliss, T. J. Robinson, J. Hilton, and D. A. Wiley, "An OER COUP: College teacher and student perceptions of open educational resources," *Journal of Interactive Media in Education*, vol. 2013, no. 1, art. 4, 2013.
[26] D. Annand, "Developing a sustainable financial model in higher education for open educational resources," *The International Review of Research in Open and Distributed Learning*, vol. 16, no. 5, pp. 1–15, 2015.
[27] E. Masterman, "Bringing open educational practice to a research-intensive university: Prospects and challenges," *Electronic Journal of E-Learning*, vol. 14, no. 1, pp. 31–42, 2016.
[28] R. Bodily, R. Nyland, and D. Wiley, "The RISE framework: Using learning analytics to automatically identify open educational resources for continuous improvement," *The International Review of Research in Open and Distributed Learning*, vol. 18, no. 2, pp. 103–122, 2017.
[29] B. L. Lindshield and K. Adhikari, "Online and campus college students like using an open educational resource instead of a traditional textbook," *MERLOT Journal of Online Learning and Teaching*, vol. 9, no. 1, pp. 26–38, 2013.
[30] V. R. Paragarino, I. F. Silveira, and M. Llamas-Nistal, "Open educational resources: A brief vision from IEEE topics," in *Proc. the 2018 IEEE Global Engineering Education Conference (EDUCON 2018)*, Tenerife, Spain, 2018, pp. 2076–2081.

Alan Stines received his bachelor's degree in information technolgy from Middle Geogia State University (MGA), Macon, GA in 2007, and the master's degree in applied computer science from Columbus State University, Columbus, GA in 2013, and is currently pursuing his doctorate degree in cyber operations from Dakota State University, Madison, SD. Mr. Stines served as an applications administrator at MGA for eight years, building, managing, and collaborating on websites and developing web applications. After a brief stint as an adjunct professor, in 2015 he accepted his current role as a lecturer in the School of Information Technology at MGA. Previous publications include research into student and faculty perceptions of the use of video conferencing technologies in the classroom, and in 2016, he participated in an Affordable Learning Georgia Textbook Transformation Grant to develop an Open Educational Resource providing no-cost textbooks for undergraduate web development courses.

Houssain Kettani received the bachelor's degree in electrical and electronic engineering from Eastern Mediterranean University, Cyprus in 1998, and the master's and doctorate degrees both in electrical engineering from the University of Wisconsin at Madison in 2000 and 2002, respectively. Dr. Kettani served as faculty member at the University of South Alabama (2002-2003), Jackson State University (2003-2007), Polytechnic University of Puerto Rico (2007-2012), Fort Hays State University (2012-2016), Florida Polytechnic University (2016-2018) and Dakota State University since 2018. Dr. Kettani has served as a staff research assistant at Los Alamos National Laboratory in summer of 2000, visiting research professor at Oak Ridge National Laboratory in summers of 2005 to 2011, visiting research professor at the Arctic Region Supercomputing Center at the University of Alaska in summer of 2008 and visiting professor at the Joint Institute for Computational Sciences at the University of Tennessee at Knoxville in summer of 2010. Dr. Kettani's research interests include computational science and engineering, high performance computing algorithms, information retrieval, network traffic characterization, number theory, robust control and optimization, and Muslim population studies. He presented his research in over seventy refereed conference and journal publications and his work received over five hundred citations by researchers all over the world. He chaired over hundred international conferences throughout the world and successfully secured external funding in millions of dollars for research and education from US federal agencies such as NSF, DOE, DOD, and NRC.