Cybersecurity Curriculum Development Using AI and Decision Support Expert System

Rania Hodhod, Shuangbao Wang, and Shamim Khan

***Abstract*—Cybersecurity has become one of the most important challenges facing the world nowadays. The increasing incidence of cybersecurity attacks on both individuals and businesses underscores the need for IT security professionals who specialize in cybersecurity. Cybersecurity National Action Plan (CNAP) is a comprehensive plan that was developed by the US but can be applied worldwide to address the cybersecurity issues by taking actions to expand cybersecurity workforce, to enhance cybersecurity education and training, and to improve cybersecurity curriculum to meet the challenge. Given the lack of expertise needed to educate the youth and professionals in cybersecurity, intelligent systems can play an important role to expedite cybersecurity education and training by helping novice cybersecurity instructors develop cybersecurity curricula and training programs. This paper presents viCyber, a cloud-based visual and intelligent tool for rapid development of cybersecurity curriculum based on the Cybersecurity Workforce Framework developed by the National Initiative for Cybersecurity Education (NICE).**

***Index Terms*—Cybersecurity, curriculum development, NICE framework, intelligent systems.**

I. Introduction

Cybersecurity has become one of the most serious challenges facing countries around the world. According to Privacy Rights ClearingHouse, the number of records breached in 2017 alone reached more than ten billion [1]. Among them, incidents of credit card fraud, hacking or malware, insider threats, and portable devices have caused damages to individuals, corporations and governments. The Cybersecurity National Action Plan (CNAP) is an initiative in the US developed to address the rapidly growing cybersecurity challenge by expanding the nation's cybersecurity workforce through improved cybersecurity curriculum design and enhanced cybersecurity education and training [2]. In an effort to help inspire solutions and innovations in curriculum development, the National Institute of Standards and Technology (NIST), USA, published the National Initiative for Cybersecurity Education (NICE). It is a partnership between government, academia and the private sector focused on cybersecurity education, training, and workforce development [3]. The NICE framework consists of seven categories, 31 specialty areas, 369 Knowledge, Skills and Abilities (KSAs), 65 competencies, and 444 tasks under various specialty areas. Fig. 1 shows a diagram of the NICE Framework.

The NICE Framework [4] guides curriculum developers to choose the right knowledge areas that would serve the desired competencies. Two major difficulties faced in this regard are: 1) the lack of cybersecurity experts who can make use of the NICE Framework; 2) the large number of competencies in the NICE Framework, KSAs and tasks that need to be considered along with their relationships while developing the curriculum.

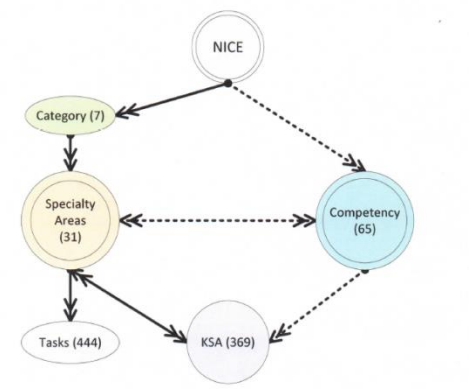

Fig. 1. NICE framework diagram.

This paper presents viCyber, an intelligent system capable of rapid cybersecurity curriculum and training development using visual mapping [5] and artificial intelligence technologies [6], [7]. ViCyber is based on a cloud computing approach which offers advantages such as simplified software installation and maintenance and centralized control over versioning. Moreover, end-users can access the service anytime, anywhere, share data and collaborate more easily, keeping the data safely in the infrastructure [8].

II. Related Work

The education of the cybersecurity workforce must include considerations of the security and privacy of urban and rural areas, curriculum development and rapid short-period training development. At the same time, teachers, K-12 students, college students, engineers, military personnel and government employees must be trained in cybersecurity. Cybersecurity curricula need to be revised constantly to reflect the most recent trends [9], [10]. Incorporating the Internet of Things (IoT) architecture and security into the current curricula will empower students to gain the knowledge of how IoT can be used in a smart cities setting, while also allowing them to master the skills necessary to design secure IoT systems. With the cybersecurity area emerging very fast and the current lack of expertise in this area, intelligent systems can come into play to help improve

Manuscript received May 19, 2018; revised August 17, 2018. This research is funded by a grant from National Security Agency (NSA) [S-004-2017]. The viCyber project is funded by the CAE Cybersecurity Grant Program.

The authors are with the Columbus State University (CSU), Columbus, Georgia, USA (e-mail: hodhod_rania@columbusstate.edu, wang_shuangboa@columbusstate.edu, khan_shamim@columbusstate.edu).

DOI: 10.7763/IJCTE.2018.V10.1209

the situation.

Intelligent systems, a.k.a. smart systems, is everywhere around us, starting from smart thermostats to smart cars. Adding intelligent features/capabilities to any system can reduce the workload on the human user and complement the user's efforts to achieve the desired tasks. Expert decision making systems are a widely used intelligent technique to support decision making in a specific domain. They have been used successfully in the medical domain to diagnose heart diseases [6], [11], [12], anemia [13], and diabetes [14]. Expert systems have been also used in engineering for fault diagnosis [15], [16], and many other domains including career guidance [17]. Expert systems are usually used to address lack of human and/or time resources. One example is an expert system for career guidance used in African high schools to address the shortage of human and time resources that the process of quality career guidance demands [17]. Other expert systems were developed for providing academic advice to students to address the shortage of capable human advisors [18], assist novice users in using new software [19], and help make decisions on appropriate public transport alternatives to the car in certain cities [20].

Although there are expert systems developed to help with designing courses in different areas, none of these systems targeted cybersecurity. As yet, there is no intelligent system that can make use of cybersecurity experts' knowledge and the NICE Framework to guide novice instructors and trainers with the development of cybersecurity courses and study programs.

III. ViCyber: An Intelligent Tool for Cybersecurity Curriculum Development

ViCyber is an intelligent visual tool that uses a decision making component to guide course design by instructors. It ensures that the course design is governed by the NICE framework by providing interactive feedback during the course design process and providing recommendation on how to improve the course. ViCyber provides a cloud-based platform, housed on an Amazon Web Services (AWS) virtual server. It will be accessible anywhere anytime through the Internet. In addition, educators in rural areas will be able to use viCyber off-line as a standalone application, if necessary.

ViCyber has two main components. The first component is the graphical user interface housed in the presentation layer. The second component is the decision support expert system with the inference engine, user model, and knowledge base housed in the second and third layers as shown in Fig. 2. A description of the viCyber system with its main components is given in the following subsections.

A. NICE Framework Database

Data in the NICE Framework is currently available on a master Excel file, which makes it hard for cybersecurity educators to navigate it. Our study shows that three types of framework mappings exist in the Excel sheet: one-to-one, one-to-many, and many-to-many. The spreadsheet format may be workable for one-to-one and one-to-many relationships, but not for many-to-many relationships since the spreadsheet would produce a large number of duplicates.

To make the NICE framework accessible to a broader community, we built a NICE database using SQL Server that contains the categories, specialty areas, work roles and KSAs as the base tables. We also built work roles with KSA mapping schema and generated commonly accessed queries as views. In contrast with the original Excel sheets, the NICE database makes it possible to query the framework, and also allows itself to be integrated into dynamic websites, machine learning knowledge bases, and other applications.

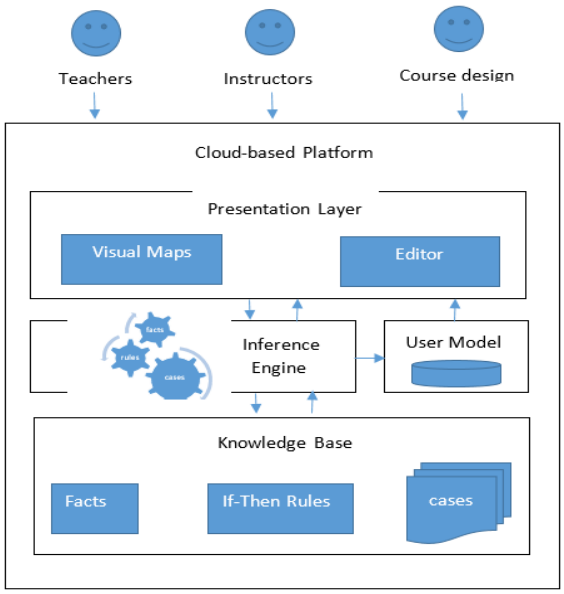

Fig. 2. ViCyber architecture.

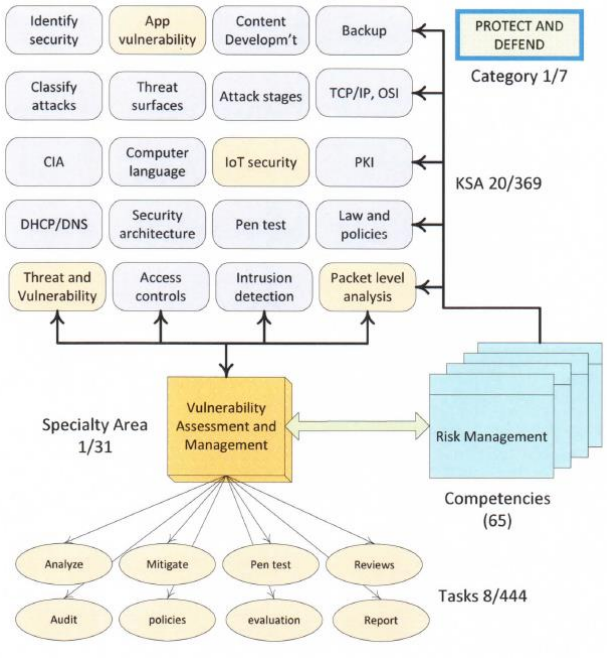

Fig. 3. Specialty area to KSA mapping.

B. Knowledge Gathering and Visual Mapping

ViCyber uses a two dimensional visual mapping technique that maps specialty areas to competencies and KSAs. The curriculum visual mapping connects knowledge units to skills and abilities based on the NICE framework. The NICE framework lists knowledge, skills, and abilities (KSAs) needed to successfully complete cybersecurity tasks for students or cyber professionals. We consider competencies in

NICE framework as assessments. Mapping specialty areas to competencies will make sure the content discussed in a course is assessed. Fig. 3 shows a visual representation of the mapping of the Vulnerability Assessment and Management specialty area with corresponding competencies.

The knowledge base in viCyber is derived from the following sources:

1) Available curricular guidelines on cybersecurity education. Two principal sources to be used for this are the NICE Framework and the latest curricular guidance to be released by the Joint Task Force on Cybersecurity Education, CSEC 2017 [21].
2) Knowledge acquired from cybersecurity experts is represented in the form of rules. The case-base in ViCyber will consist of existing cybersecurity curricula from leading educational institutions that meet the above-mentioned curricular guidelines. Example facts that represent the connections between the specialty areas in the knowledge-base are:

```
connect_cat_sa_sa_wt("PR", "CDA", "CIR", 0.67)
connect_cat_sa_sa_wt("PR", "CDA", "VAM", 0.32)
connect_cat_sa_sa_wt("PR", "INF", "CDA", 1)
connect_cat_sa_sa_wt("PR", "INF", "CIR", 0.32)
```

The above facts are defined by the relation `'connect_cat_sa_sa_wt'`, where, the first parameter indicates the category name, second and third parameters indicate the specialty areas of interest and the fourth parameter is the strength of the connection (1 indicates maximum possible connection strength). This information is used later by the graphical user interface for visualization purpose.

C. User Modeling and Decision Support System

User modeling is the subdivision of human computer interaction, which describes the process of building up and modifying a conceptual understanding of the user [22]. The main goal of user modeling is the customization and adaptation of systems to the user's specific needs. The user model in viCyber aims to track the user performance and build a model for the user performance. It will provide the necessary information to the expert system component in viCyber, upon request, to allow the system to reason about the user's performance and provide tailored feedback to the user. Fig. 4 shows the interactions between the different parts of the decision support expert system in viCyber.

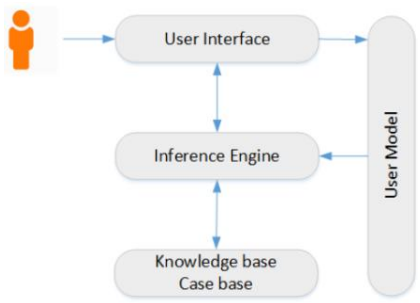

Fig. 4. Decision support system diagram.

D. Graphical User Interface

The user interface allows the user to interact with viCyber. It also provides an editor for the user to design their courses. The editor is divided into two areas as shown in Fig. 5. The left side of the window shows a hierarchical tree structure for the categories, specialty areas, and KSAs (tasks are not considered in the current implementation). The right side shows the interface for building an incremental tree that represents a cognitive map [23] with the user's choices of categories, specialty areas, and KSAs.

The user will select specialty areas and KSAs according to the skills that students should master in order to succeed in the cybersecurity job market. When the user clicks on a node in the tree hierarchy, the node is added to the incremental tree in the right side of the editor. The facts in the knowledge base are used to determine the strength of the relationships (edges) in the incremental tree; a thick line indicates strong association and a thin line indicates weak association (see Fig. 5).

The user will then be able to explore and interact with the visual incremental tree; they can hide branches, and click on a node for a detailed description of the node. The user's actions will be monitored and tracked by the user model present in viCyber. ViCyber is then able to evaluate the course design and use the information in the user model to provide feedback to the user. For example, it would point out that one of the specialty areas does not have strong associations with the rest of the specialty areas, and recommend a list of other specialty areas that can be better used in that particular course. It is up to the user to follow viCyber's advice and make changes to the course, or leave the course as is.

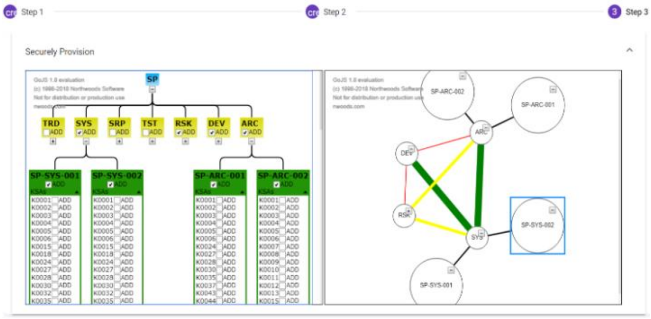

Fig. 5.ViCyber graphical user interface.

E. Curriculum Evaluation

Each new curriculum created in viCyber is represented as an incremental tree (See Fig. 5) which is then transformed and saved as a concept map that holds all the curriculum components, strength of connections, and course tags. The curriculum evaluation component in viCyber provides an overall evaluation for the concept map in which a final score is computed based on the strength of the connections between the different components including specialty areas, work roles and KSAs. This score provides a measure of how good the curriculum design is.

An overall feedback that explains the score is also provided to the user, in addition to recommendations on how to make the design better; for example, information is provided on specialty areas and/or KSAs that can be added or removed from the current design to enhance the curriculum design. The user has the freedom to apply the recommendations or leave the course as is.

The output module of the viCyber tools gather data from

the newly created curriculum and push to the Amazon AWS CloudFront so the static and dynamic web content is delivered to users with best performance. At the same time, it generates a PDF file for the finalized curriculum outline.

F. Curriculum Re-usability

A powerful feature in viCyber is its ability to re-use existing curricula so the user does not have to build a curriculum from scratch. The user can enter key words and the curriculum evaluation component can retrieve the highest matching curriculum, which will then be displayed to the user. The retrieval process uses the nearest neighbor classification algorithm to compare each course's tags and the key words entered by the user to retrieve the highest matching curriculum. The user can edit the curriculum, which accordingly updates the incremental tree and the associated concept map. The user can then save the new curriculum under a new name.

IV. Experiments and Results

Currently we have finished building the NICE database, knowledge base, user modeling and decision support system and visual mapping. The process of implementing and testing the user interface is in progress. The NIST NICE office has requested access to the NICE database and has shared it to a number of companies, universities and government agencies under the Department of Homeland Security (DHS) and the National Security Agency (NSA). The knowledge base has been connected to the system for evaluating the quality of curriculum development. The visual mapping view of the user interface uses thick lines to represent strong connections and uses thin lines to represent weak connections between the specialty areas and work roles. The corresponding KSAs can be expanded with a selection of any particular KSA or all KSAs under the work role (Fig. 5). Users can generate reports in PDF format from the completed curricula including specialty areas, work roles, and KSAs.

V. Conclusion

This paper presents work in progress to develop viCyber, an intelligent system to develop cybersecurity curricula in a rapid and reliable way. The viCyber research project contributes to changing the current status of cybersecurity education by helping instructors anywhere in the world to develop cybersecurity curricula and/or training programs. Our research builds on user modeling and adaptation in the areas of software design and intelligent systems. The culmination of this work will be a robust, fully usable online curriculum development tool that can be used by both novice as well as experienced cybersecurity educators. ViCyber evaluates every curriculum design with the NICE framework with a normalized score to indicate the closeness the curriculum to the framework. The system stores peer reviewed curricula as templates. Initial tests show the system can guide users to develop curricula following NICE framework using artificial intelligence. The automatic evaluations of the syllabi provides users with the confidence of the design.

References

[1] Privacy Right Clearinghouse. (Feb. 28, 2018). [Online]. Available: https://www.privacyrights.org/data-breaches

[2] Cybersecurity National Action Plan. (April 8, 2017). [Online]. Available: https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/cnap-letter_11-2016.pdf

[3] NIST. (April 8, 2017). [Online]. Available: https://www.nist.gov/

[4] National Initiative for Cybersecurity Education. (2017). [Online]. Available: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-181.pdf

[5] S. Wang and W. Kelly, "IoT architecture and security - a case study in cybersecurity curriculum development with the nice framework," in *Proc. NICE*, 2016.

[6] A. B. M. Salem, M. Roushdy, and R. A. HodHod, "A case based expert system for supporting diagnosis of heart diseases," *AIML Journal*, vol. 5, no. 1, pp. 33-39, 2005.

[7] R. A. HodHod, H. Fleenor, and S. Nabi, "Adaptive augmented reality serious game to foster problem solving skills," in *Proc. Workshop on Hyperrealistic Intelligent Environments*, 2014, pp. 273-284.

[8] V. Vergara, K. Lagos-Ortiz, M. Aguirre-Munizaga, M. Aviles, J. Medina-Moreira, J. Hidalgo, and A. Munoz-Garcıa, "Knowledge-based model for curricular design in ecuadorian universities," in *Proc. the Second International Conference on Communications in Computer and Information Science, Technologies and Innovation, CITI 2016*, Guayaquil, Ecuador, November 23-25, 2016, pp. 14-25.

[9] S. Wang, W. Kelly, and J. Zhang, "Using novel video indexing and data analytics tool to enhance interactions in e-learning," in *Proc. E-Learn: World Conference on E-Learning in Corporate, Government, Healthcare, and Higher Education*, 2015, pp. 1919-1927.

[10] P. Wang and W. Kelly, "A novel threat analysis and risk mitigation approach to prevent cyber intrusions," *Colloquium for Information System Security Education (CISSE)*, vol. 3, pp. 157-174, 2015.

[11] A, B. M. Salem and R, A, HodHod, "A hybrid expert system supporting diagnosis of heart diseases," in *Proc. Intelligent Information Processing*, 2002, pp. 301-305.

[12] A. H. M. Ragab, K. A. Fakeeh, and M. I. Roushdy, "A medical multimedia expert system for heart diseases diagnosis & training," in *Proc. the 2nd Saudi Science Conf*., 2004, pp. 31-45.

[13] N. I. Birndorf, J. O. Pentecost, J. R. Coakley, and K. A. Spackman, "An expert system to diagnose anemia and report results directly on hematology forms," *Computers and Biomedical Research*, vol. 29, no. 1, pp. 16-26, 1996.

[14] C. S. Lee and M. H. Wang, "A fuzzy expert system for diabetes decision support application," *IEEE Transactions on Systems, Man, and Cybernetics*, vol. 41, no. 1, pp. 139-153, 2011.

[15] F. Filippetti, M. Martelli, G. Franceschini, and C. Tassoni, "Development of expert system knowledge base to on-line diagnosis of rotor electrical faults of induction motors," in *Proc. Industry Applications Society Annual Meeting*, pp. 92-99, 1992.

[16] H. J. Lee, D. Y. Park, B. S. Ahn, Y. M. Park, J. K. Park, and S. S. Venkata, "A fuzzy expert system for the integrated fault diagnosis," *IEEE Transactions on Power Delivery*, vol. 15, no. 2, pp. 833-838, 2000.

[17] O. Winston and M. Lawrence, "Career guidance using expert system approach," *Fountain Publishers Kampala*, p. 123, 2008.

[18] O. Daramola, O. Emebo, I. T. Afolabi, and C. K. Ayo, "Implementation of an intelligent course advisory expert system," *International Journal of Advanced Research in Artificial Intelligence*, vol. 5, no. 4, 2014.

[19] J. Shrager and T. W. Finin, "An expert system that volunteers advice," in *Proc. National Conference on Artificial Intelligence Pittsburgh*, 1982, pp. 339-340.

[20] R. Mackett and M. Edwards, "An expert system to advise on urban public transport technologies," *Computers, Environment and Urban Systems*, vol. 20, no. 4, pp. 261-273, 1996.

[21] D. Burley, M. Bishop, S. Kaza, D. S. Gibson, and S. Buck, "Joint task force on cybersecurity education," in *Proc. ACM Technical Symposium*, 2017.

[22] D. Benyon and D. Murray, "Applying user modeling to human-computer interaction design," *Artificial Intelligence Review*, vol. 7, no. 3, pp. 199-225, 1993.

[23] M. S. Khan and M. Quaddus, "Group decision support using fuzzy cognitive maps for causal reasoning," *Group Decision and Negotiation*, vol. 13, no. 5, pp. 463-480, 2004.

Rania Hodlod received the Ph.D. in computer science at University of York, UK. From 2011-2013, Rania was a postdoctoral research fellow at the Adaptive Digital Media (ADAM) Lab in the Georgia Tech School of Literature, Media and Communication, where she researched and developed a computational model for shared mental models in digital improvisation environments, in addition to the development of a new context-based structural retrieval algorithm for cognitive scripts. In 2013, Rania joined the Entertainment Intelligence Lab in the Georgia Tech School of Interactive Computing, where she researched procedural generation of computer game content, commonsense knowledge bases, and computational creativity.

Rania is the assistant chair of TSYS School of Computer Science, Columbus State University (CSU). She teaches and supervises undergraduate and graduate students. Rania's research interests span a range of areas including artificial intelligence, expert systems, serious games, interactive narrative, and computational creativity. She has published over 45 refereed articles and two book chapters in these areas. Her current research work on intelligent systems is supported by the National Science Association (NSA).

Dr. Hodhod is the holder of the CSU Teaching and Learning Award 2017 and was a finalist for the Faculty Research and Scholarships Award at CSU 2016. She also held the Columbus State University Outstanding Teacher of Writing Award and Recognition of Excellence: Graduate Faculty Award in 2015.

Shuangbao (Paul) Wang received the Ph.D. in computer science at George Mason University at Fairfax, Virginia USA under the guidance of Dr. Robert Ledley, the inventor of body CT scanner in 2004.

Paul is a professor and TSYS endowed chair in cybersecurity. He was previous the chief information and technology officer (CIO/CTO) of the National Biomedical Research Foundation (NBRF). He has been speakers to many major cybersecurity and IoT conferences. His research areas are secure architecture, IoT/CPS, cryptography, and video indexing.

Prof. Wang is the recipient of Advanced Simulation and Training Award by the Link Foundation. He was directly involved in drafting of the National Initiative of Cybersecurity Education (NICE) framework. In addition to books, referred publications, conference speakers and numeral grant activities, Paul has four patents; three of them have been licensed to the industry.

Shamim Khan earned his BS and MS in applied physics & electronic from Rajshahi University in Bangladesh, and a Ph.D. in computer science from the University of Manchester, UK for his work on parallel image processing.

Dr. Khan taught computer science at the National University of Singapore and Murdoch University in Australia. He is currently a professor and director of graduate studies at the TSYS School of Computer Science, Columbus State University.

Apart from computer vision, Dr. Khan's current research interests include the application of artificial intelligence techniques for knowledge representation and decision support, computer science education and cybersecurity. He has numerous publications in refereed journals and conference proceedings in the areas of soft computing, intelligent decision support, computer vision, and computer science education.