Modeling and Simulation Education for Behavioral Cybersecurity

Rebecca Leis, M.S., Karla A. Badillo-Urquiola, M.S.
Institute for Simulation & Training (IST)
University of Central Florida (UCF)
Orlando, Florida
rleis@ist.ucf.edu, kbadillo@ist.ucf.edu

Bruce D. Caulkins, Ph.D., Patricia Bockelman, Ph.D.
Institute for Simulation & Training (IST)
University of Central Florida (UCF)
Orlando, Florida
bcaulkin@ist.ucf.edu, pbockelm@ist.ucf.edu

ABSTRACT

Much of today's cybersecurity efforts focus on underlying technologies influencing cyberspace operations. Installing, operating, and maintaining cybersecurity-related technologies (e.g., firewalls, intrusion prevention systems) have consumed government and commercial sectors; but, this unilateral attention on the technology has led to significant oversight. Although cybersecurity requires emphasis on technology, exclusive focus on hardware and software leads to lapses in the area that is arguably a critical aspect of any given system—human users. Consequently, a more holistic cybersecurity education strategy must be developed to focus on the gaps between cybersecurity-related technologies and the human domain.

This paper investigates one of the key gaps within cyber-education: the lack of human-centric curricula. To address this gap, we first attempted to identify the relevance of both techno-centric and human-centric knowledge, skills, and abilities (KSAs) within cybersecurity. 117 participants completed an online survey capturing perceptions of KSA relevance for five different cybersecurity scenarios pulled from the IBM X-Force Threat Intelligence Report 2016. Results indicated that a majority of participants found Human Computer Interaction, Criminal Psychology, Sociological Behavior, and Human Performance *relevant* KSAs in most of the scenarios. Specifically, Criminal Psychology and Sociological Behaviors were considered *relevant* or *very relevant* in all five scenarios.

The paper next outlines a pilot education program launched at the University of Central Florida (UCF), designed to address the unique challenges of the human dimension in cybersecurity. The purpose of highlighting this pilot program is to provide an example of human-centric cyber-educational curriculum. It is our hope that the information presented in the present paper will serve as a launching point for further discussion about the human side of cybersecurity.

ABOUT THE AUTHORS

Rebecca Leis is currently working towards Ph.D. in Modeling and Simulation from the University of Central Florida and is interested in training and education. Rebecca investigates curriculum development and resource allocation models for graduate education. She additionally assesses tasks and job demands within operational environments. Specifically, Rebecca has worked on projects assessing Oil Rig Downhole Tool Operators and Nuclear Power Plant Reactor and Senior Reactor Operators. She hopes to ultimately contribute to the field by creating new training guidelines for safety-critical tasks, as well as improve education for M&S workforce development.

Karla A. Badillo-Urquiola is a Graduate Research Assistant at the Institute for Simulation and Training. She is pursuing her Ph.D. in Modeling and Simulation at the University of Central Florida and is a recipient of the McKnight Doctoral Fellowship Program. Karla leverages her background in Human Factors Psychology and Instructional Design to investigate several training and education topics, including: training effectiveness of virtual worlds, andragogy in simulation-based blended-learning environments, and patient-centered technologies. Her ultimate goal is to use interdisciplinary research approaches for enhancing relationships between individuals, as well as the interaction between technology and humans.

Bruce Caulkins is a Research Assistant Professor at the Institute for Simulation and Training at UCF, focusing on cybersecurity-related research and instruction. He is a retired Army Colonel with over 28 years of experience in tactical, operational, and strategic cyberspace operations. In his last military assignment, he was the Chief of the Cyber Strategy, Plans, Policy, and Exercises Division (J65) within the U.S. Pacific Command. Bruce previously led several cyber-related schools within the Army's Training and Doctrine Command. He earned his Ph.D. in Modeling and Simulation at UCF, focusing on anomaly detection within intrusion-detection systems.

Patricia Bockelman is an Associate Research Professor at the Institute for Simulation and Training at UCF, specializing in applied cognition with an emphasis on complex learning contexts. Her present work includes examining user responses to the Augmented Immersive Team Trainer, which uses augmented reality to provide virtual force-on-force effects for the U.S. Marine Corps. She also is collaborating with the E2I Creative Lab to examine intelligent behaviors associated with Downhole Tool Operation on oil rigs. Prior projects have included neurophenomenology, physiological cognition, and andragogy in blended learning environments. In addition to her ongoing research at IST, she teaches in Modeling and Simulation (M&S) Graduate program.

Modeling and Simulation Education for Behavioral Cybersecurity

Rebecca Leis, M.S., Karla A. Badillo-Urquiola, M.S.
Institute for Simulation & Training (IST)
University of Central Florida (UCF)
Orlando, Florida
rleis@ist.ucf.edu, kbadillo@ist.ucf.edu

Bruce D. Caulkins, Ph.D., Patricia Bockelman, Ph.D.
Institute for Simulation & Training (IST)
University of Central Florida (UCF)
Orlando, Florida
bcaulkin@ist.ucf.edu, pbockelm@ist.ucf.edu

INTRODUCTION

Cybersecurity career preparation focuses on teaching the technological knowledge, skills, and abilities (KSAs) relevant to general security challenges in cyberspace. However, recent studies suggest that cyber vulnerabilities and defenses have more to do with human elements than have historically been acknowledged (Waldrop, 2016). The U.S. Department of Defense (DoD) latest cyber strategy document outlines a series of goals that call for increased attention to human elements across a number of cybersecurity areas (DoD, 2015). For example, this cyber strategy calls for improved *recruitment* for cyber careers, improved options for *conflict resolution*, and advanced training for analytics (using *critical thinking* skills). These needs reach beyond the realm of hardware and software and highlight the deficit in human-centric cybersecurity. To address these shortcomings, the following questions should be considered:

1) What are we teaching/training now?
2) What should we be teaching/training?

The present paper aims to address this first consideration, sparking conversation by investigating typical graduate level cybersecurity curricula. We intentionally selected this level of education to scope the review and because the expectations are akin to mid- to high-level careers in cybersecurity. At the graduate-level student/trainees have advanced beyond foundational knowledge and are likely seeking or currently holding a management position.

The second consideration will require careful and reiterative reflection as cybersecurity is a rapidly emerging, dynamic field. Conversation and deliberation for accredited curricula should be led by both experienced professionals and academics as knowledge evolves through discussion with collaborators and peers. To initiate this discussion the present paper outlines results from a survey of cyber professionals. The survey asked professionals to examine real security events and rate the degree of relevancy of various techno-centric and human-centric KSAs.

Finally, we offer a template that established institutions can use to bridge that gap in cybersecurity education, moving toward a more holistic approach. This template demonstrates the way in which the University of Central Florida has supplemented existing technical programs by offering a graduate certificate in behavioral cybersecurity. This template is also presented to initiate discussion; thus, we encourage respectful debate.

CURRENT APPROACHES TO CYBER-EDUCATION

We conducted an informal survey of cyber programs at accredited universities and colleges and predictably, the vast majority of programs are embedded within or closely aligned with computer science and engineering-related departments.

We reviewed 33 U.S. post-secondary programs offering graduate-level instruction in cybersecurity. Programs were selected for review based on public availability of course requirements. Programs that did not use “cyber” in the title were not included for review. This review is not intended to act as a statistically generalizable study, but as a frame-of-reference within which we may contextualize the trends anecdotally accounted. We assessed each degree program according to the program’s curriculum and course information presented on the program’s website. Particularly, we

evaluated each program's course titles and descriptions for human elements including attacker motives, organizational management techniques, risk and threat analysis, ethics, policy and legal issues, and human factors.

Of the 33 sampled, 3 programs specifically covered attacker motives, 17 covered organizational management techniques, 14 covered risk and threat analysis, and 21 covered ethics, policy, and legal issues. Only 4 of the 33 programs reviewed required a course dedicated specifically to human-centric aspects within cybersecurity. These four programs include course titles such as "Human Aspects of Cybersecurity," "Human Organizational Aspect of Cybersecurity," "Human Factors," and "Human Factors in Computer Security and Privacy." This contextualizing review suggests human-centric KSAs, while important to successful cybersecurity career performance, are not generally emphasized in cybersecurity career preparation.

Colleges and universities must prepare students for professional demands. Can current training and education curricula provide learners with appropriate opportunities to obtain the required KSAs? If the KSAs include human elements, then these elements must be included in core curricula for cyber professionals. Subject matter experts provide the most reliable insight regarding KSAs. To better understand cyber professional's perceptions of relevancy of techno-centric and human-centric KSAs, researchers conducted the following qualitative study.

NEEDED KSAs FOR CYBERSECURITY

Participants

117 participants (105 males and 12 females) were recruited via invitation on 53listserve, an online community for cyber professionals (see Figure 1). Participant ages ranged from 23 to 64 (M = 45.97). Participants were required to be over the age of 18 and received no compensation for participation.

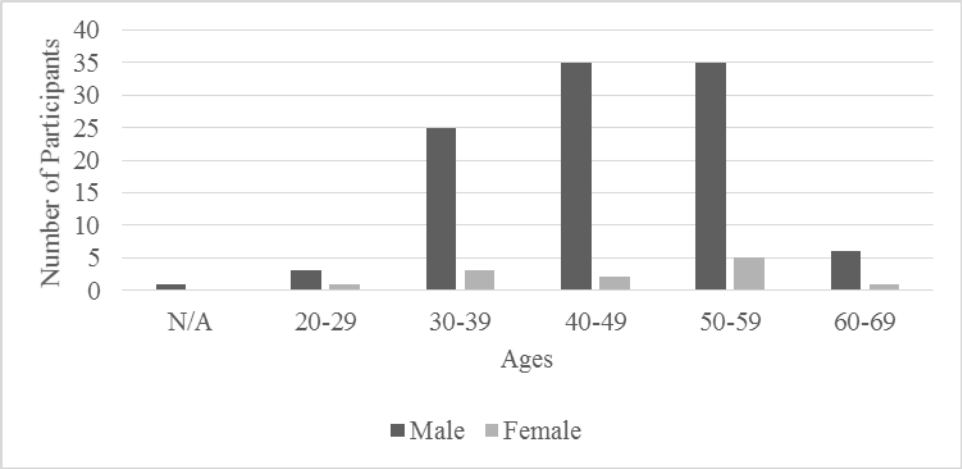

Figure 1. Histogram of Female and Male Ages

Materials

Survey. The survey was developed in house by the research team. It included a demographic section as well as five case studies.

Case Studies. Researchers used the case studies outlined within the IBM X-Force Threat Intelligence Report 2016. The cases briefly describe a range of significant high-profile cyber incidents across the globe (X-Force, 2016), and they present different kinds of threats. The case studies provided examples of the following cyber security issues:

Table 1. Case study cyber concern areas

CASE STUDY	CYBER AREA
A	Distributed Denial of Service (DDoS) against banks, government agencies, and private websites
B	Hacking attack by "cyber jihadists" against a French television channel
C	Bank robberies via spear phishing to install Carbanak malware
D	Personal data leak from Japan Pension Service
E	Former employee accessed approximately 2,200 General Motors Finance customers identification

Study Design

Participants completed the study via Qualtrics, an online survey platform. Participants completed an informed consent prior to the data collection. The study included demographic data collection followed by the presentation of case studies; participants could opt out of answering any portion of the survey. Participants were randomly presented three out of the five case studies. Following each case study, participants answered a series of Likert-style questions designed to capture the perception of relevance for techno-centric and human-centric KSAs (See Table 2). The survey included constructs and KSAs beyond those listed, however, these 10 KSAs (5 techno-centric and 5 human-centric) were identified *a priori* to address the present research question.

Table 2. KSAs analyzed

Techno-centric	Human-centric
Antivirus Software	Human-computer interactions
Firewalls	Criminal psychology
Hardware	Biomechanics/ergonomics
Computer Programming	Sociological behaviors
Encryption technologies	Human performance

Research Question 1. Do cyber-professionals perceive a similar need for human-centric as techno-centric KSAs?
Rationale: if there is a similar requirement for techno-centric and human-centric KSAs, then there is an obligation for institutional training to address those needs.

Research Question 2. Are human-centric KSAs more relevant to *certain* cyber security issues than others are?
Rationale: training and education programs can customize career development for specific industry needs and industries can identify qualified personnel according to their prioritized vulnerabilities.

RESULTS

The following results are organized by case study with frequency counts (larger frequency counts were bolded for emphasis) for the perception of human-centric and techno-centric KSA relevancy within each study. Then, the results for KSA perceptions by category (techno-centric vs. human-centric) are presented. As participants were permitted to refrain from answering any item, the number of responses varied by question. Consequently, frequency rates must be contextualized by the independent responses.

Case Study A: DDOS

Participants indicated "Firewalls" and "Encryption Technologies" most frequently at the "very relevant" level (n = 37) in the DDOS case, Case A (Table 3). The second most frequent response was "Criminal Psychology," positioned at the "relevant" level, n = 24. The third most frequent response was for "Biomechanics/Ergonomics," n = 22 for "N/A."

Table 3. Case Study A perceptions of relevancy by KSA

	Question	0 = N/A	1 = minimally relevant	2 = relevant	3 = very relevant	N Responses
Techno-Centric	Antivirus Software	6	15	20	12	53
	Firewalls	1	3	12	**37**	53
	Hardware	3	5	22	20	50
	Computer programming	2	12	19	18	51
	Encryption Technologies	3	2	11	**37**	53
Human-Centric	Human-Computer Interaction	9	19	14	10	52
	Criminal Psychology	6	10	**24**	12	52
	Biomechanics Ergonomics	**22**	17	11	3	53
	Sociological Behaviors	6	17	21	7	51
	Human Performance	11	20	15	6	52

Case Study B: Hacking attack

For Case B, where the participants read about a hacking attack on a media outlet, the most frequent response was given for "Antivirus Software" as "very relevant" (n = 41). The next frequent response was "Firewalls" at the "very relevant" level, n = 35 (Table 4). Overall, the third most frequent response was for "Biomechanics/Ergonomics," which again received a "N/A" rating, n = 27. For KSAs that ranked as relevant, "Criminal Psychology" and "Sociological Behaviors" received the third most frequent counts (n = 24); with relevancy levels of "relevant" and "very relevant," respectively. Further, "Sociological Behaviors" was the only KSA that received no "N/A" ranking.

Table 4. Case Study B perceptions of relevancy by KSA

	Question	0 = N/A	1 = minimally relevant	2 = relevant	3 = very relevant	N Responses
Techno-Centric	**Antivirus Software**	1	5	9	**41**	56
	Firewalls	1	5	15	**35**	56
	Hardware	7	17	19	12	55
	Computer programming	4	13	18	20	55
	Encryption Technologies	4	19	15	17	55
Human-Centric	Human-Computer Interaction	5	13	18	18	54
	Criminal Psychology	2	11	**24**	18	55
	Biomechanics/ Ergonomics	**27**	23	6	-	56
	Sociological Behaviors	-	13	19	**24**	56
	Human Performance	10	17	14	15	56

Case Study C: Phishing robbery

Respondents rated techno-centric KSAs at the highest relevancy levels for Case C, bank robberies involving phishing (Table 5); "Firewalls" (n = 30), "Antivirus Software" (n = 28), and "Encryption Technologies" (n = 24). Researchers noted that "Criminal Psychology" had the highest number of respondents for "relevant" and "very relevant" combined (n = 41). "Antivirus Software" was the only KSA receiving no "N/A" ranking.

Table 5. Case Study C perceptions of relevancy by KSA

	Question	0 = N/A	1 = minimally relevant	2 = relevant	3 = very relevant	N Responses
Techno-Centric	**Antivirus Software**	-	9	10	**28**	47
	Firewalls	2	4	11	**30**	47
	Hardware	5	9	17	16	47
	Computer programming	6	4	19	18	47
	Encryption Technologies	6	6	9	**24**	45
Human-Centric	Human-Computer Interaction	1	10	16	20	47
	Criminal Psychology	2	4	**21**	**20**	47
	Biomechanics/ Ergonomics	17	16	10	4	47
	Sociological Behaviors	1	10	13	23	47
	Human Performance	7	11	12	17	47

Case Study D: Personal data leak

The most frequent response to the data leak scenario described in Case D (Table 6), was for "Antivirus Software," which was seen as "very relevant" (n = 39). "Biomechanics/Ergonomics" rated as "N/A" (n = 32). Both "Encryption Technologies" and "Sociological Behaviors" received ratings of "very relevant" (n = 27). Researchers noted that "Criminal Psychology" had the highest number of respondents for "relevant" and "very relevant" combined (n = 46). No participants assigned "N/A" to "Criminal Psychology" or "Sociological Behaviors."

Table 6. Case Study D perceptions of relevancy by KSA

	Question	0 = N/A	1 = minimally relevant	2 = relevant	3 = very relevant	N Responses
Techno-Centric	**Antivirus Software**	2	8	10	**39**	59
	Firewalls	5	11	20	23	59
	Hardware	14	22	12	10	58
	Computerprogramming	11	26	8	14	59
	Encryption Technologies	8	15	9	**27**	59
Human-Centric	Human-Computer Interaction	8	11	20	20	59
	Criminal Psychology	-	12	**20**	**26**	58
	Biomechanics/ Ergonomics	**32**	19	6	2	59
	Sociological Behaviors	-	17	15	**27**	59
	Human Performance	12	13	22	12	59

Case Study E: Former employee access

Participants who responded to Case E (Table 7), involving a former employee accessing personal data from a corporate system, responded that "Encryption Technologies" was "very relevant" most frequently (n = 31). Although they received the same count (n = 26), "Antivirus Software" and "Biomechanics" were ranked as "N/A," whereas "Criminal Psychology" went the other direction receiving a "very relevant" rank. "Criminal Psychology" received the most responses for "relevant" and "very relevant" combined (n = 50).

Table 7. Case Study E perceptions of relevancy by KSA

	Question	0 = N/A	1 = minimally relevant	2 = relevant	3 = very relevant	N Responses
Techno-Centric	**Antivirus Software**	**26**	25	3	3	57
	Firewalls	12	20	11	13	56
	Hardware	16	24	12	5	57
	Computer programming	14	20	19	4	57
	Encryption Technologies	4	8	14	**31**	57
Human-Centric	Human-Computer Interaction	11	20	12	14	57
	Criminal Psychology	2	5	**24**	**26**	57
	Biomechanics/ Ergonomics	**26**	19	8	4	57
	Sociological Behaviors	2	15	22	18	57
	Human Performance	13	15	15	14	57

Human-centric by Case

The rankings from each case affirm the importance of techno-centric KSAs, especially Anti-virus software, Firewalls, and Encryption Technologies. However, the impetus of the study was to examine the possible value of additional KSA attention for human-centric competencies in cyber training. Consequently, researchers examined the percentages of respondents who reported each KSA as critical.

Table 8. Percentage of cyberspecialists who indicated that these human-centric KSAs are "relevant" or "very relevant" combined

	Case A	Case B	Case C	Case D	Case E
	DDOS	**Hacking attack**	**Phishing robbery**	**Personal data leak**	**Former employee access**
Human-Computer Interaction	46.2	66.7	76.6	67.8	45.6
Criminal Psychology	69.2	76.4	87.2	79.3	87.7
Biomechanics/ Ergonomics	26.4	10.7	29.8	13.6	21.1
Sociological Behaviors	54.9	76.8	76.6	71.2	70.1
Human Performance	40.4	51.8	61.7	57.6	50.9

Not only did the human-centric KSAs (Table 8) all receive some respondents finding them relevant in every scenario, but a majority of participants found HCI, Criminal Psychology, Sociological Behavior, and Human Performance relevant KSAs in most scenarios. Criminal Psychology and Sociological Behaviors were relevant or very relevant in all 5 scenarios.

Table 9. Percentage of cyberspecialists who indicated that these techno-centric KSAs are "relevant" or "very relevant" combined

	Case A	Case B	Case C	Case D	Case E
	DDOS	**Hacking attack**	**Phishing robbery**	**Personal data leak**	**Former employee access**
Antivirus Software	60.4	89.3	80.9	83.1	10.5
Firewalls	92.5	89.3	87.2	72.9	42.9
Hardware	84	56.6	70.2	37.9	29.8
Computer programming	72.5	69.1	78.7	37.3	40.4
Encryption Technologies	90.6	58.2	73.3	61.1	78.9

As anticipated, respondents affirmed the relevance of techno-centric KSAs in every case (Table 9). However, only one techno-centric KSA received more than 50% indicating relevance in Case E, encryption technologies.

Limitations

The data presented above represent frequency counts from Likert-style data. Further, a compelling argument for the interdependence of the KSAs introduces potential violations of the essential assumptions of independence required for a chi-squared test with the present sample size. As such, it is essential to interpret them as descriptive, rather than inferential, statistical results.

Discussion

The study results suggest that cyber-specialists apply KSAs from the human-centric domain, although they are not all applied with equal importance to all circumstances. For example, “Biomechanics/Ergonomics” scored lower than the other human-centric KSAs in all cases. This may be an effect of little ergonomic principles genuinely at play. However, it should be noted that none of these cases involved vulnerabilities introduced through the internet of things. As more households embrace online appliances and other smart devices that engage humans in a distinctly embodied fashion, this perception may change.

Two cases demonstrated that the human-centric KSAs may be more relevant for certain cyber vulnerabilities. Case D reflected greater relevancy for HCI, Criminal Psychology, Sociological Behaviors, and Human Performance than Hardware or Computer Programming. Case E provided a clear example of the criticality of human-centric KSAs, with Criminal Psychology, Sociological Behaviors, and Human Performance all scoring higher rates of relevancy than all the studied KSAs except Encryption Technologies.

Specialists assigned consistently high levels of relevancy to Criminal Psychology and Sociological Behaviors across all of the cases. Clearly both of these are broad categories that demand nuanced consideration. For example, for criminal psychology to be taught, what kinds of fundamental psychology instruction is required as well? What aspects of sociology are most relevant to understanding cybercrime? How do we modify technical approaches to prevention and response based on human-centric principles?

None of the cases in this survey demonstrated exclusively technological needs. This validates the central assertion of the present paper—if we know that human-centric competencies are essential for holistic cyber security, how can we support interdisciplinary programs that embrace these associated KSAs?

A TEMPLATE TO BRIDGE EXISTING PROGRAMS TO MEET PRESENT AND FUTURE NEEDS

We recommend that cybersecurity programs intentionally engage in efforts aimed at developing holistic curricula to prepare the cyber workforce for the dynamic challenges of the field by considering the following:

1. **Acknowledge across domains the need for new cyber-security approaches.** Cyber-education programs in the U.S. military, private sector, and academia cannot continue to focus exclusively on computer science skills and standards, but need to expand their curricula to cover human-centric aspects (Pfleeger & Caputo, 2012), such as the gaps in cyber-leader development (Conti et al., 2014).
2. **Require human-centric coursework**. Cyber-education programs for graduate-level professionals should include training in areas (e.g., sociology, HCI, and criminal psychology) that contribute to better understanding of perpetrator behaviors. These are the KSAs, which if better understood could support more accurate prediction and prevention of cybercrime.
3. **Teach the tech in respect to the human**. Cyber-education must approach the challenges of security from an interdisciplinary or transdisciplinary perspective, so that technological solutions are executed with consideration of human factors. This approach requires the elimination of stovepipes and acknowledges the short-comings inherent to exclusively techno-centric training.

With these recommendations in mind, we provide the following pilot program as an example of integrated options for cyber training.

HUMAN-CENTRIC EDUCATION IN CYBERSECURITY: A TEMPLATE

A pilot graduate-level certificate program at UCF provides a template of our holistic approach. For example, the UCF certificate supplements techno-centric courses from programs such as Modeling and Simulation or Engineering. Students of the Modeling and Simulation of Behavioral Cybersecurity Certification are required to complete 13 credit hours, which include:

- **Cybersecurity: A Multidisciplinary Approach** (3 credit hours) – This course is described as "[i]nterdiciplinary [modeling and simulation] fundamentals as applied to cybersecurity including operating system installation and administration for hardware, network architectures, configurations, behavioral aspects, organizational continuity planning, security management" (UCF, 2016).
- **Cyber Operations Lab** (3 credit hours) – This course is described as "[p]rogramming, software, and hardware components for cybersecurity operations related to system administration, firewalls, cyber attack, cyber defense, security, secure architectures at network and computer level" (UCF, 2016).
- **Behavioral Aspects of Cybersecurity** (3 credit hours) – This course is described as "[i]nterdisciplinary human, social, and behavioral issues related to cybersecurity. Management techniques, motives for cyber crimes, risk and threat analysis, and ethics and legal issues" (UCF, 2016).
- **Emerging Cyber Issues** (1 credit hour) – This course is described as "[i]nterdisciplinary discussion of emerging issues with expert speakers from industry. Preparation of topic and required resources to complete a multi-disciplinary Modeling & Simulation capstone project" (UCF, 2016)
- **Simulation Research Methods and Practicum** (3 credit hours) – This course is described as "[i]nterdisciplinary teams of students conduct fundamental and applied research on contemporary issues in modeling, simulation, and training" (UCF, 2016).

These courses are specifically designed to teach student techniques for approaching authentic and complex tasks that mirror real-world problems. Table 10 demonstrates the ways in which the courses from the Modeling and Simulation of Behavioral Cybersecurity Certificate map to the three present and future needs.

Table 10: Mapping of courses in the Modeling and Simulation of Behavioral Cybersecurity Certificate to needs identified

Need/Course	**Cybersecurity a Multidisciplinary Approach**	**Cyber Operations Lab**	**Behavioral Aspects of Cybersecurity**	**Emerging Cyber Issues**	**Simulation Research Methods and Practicum**
Need 1: inter/multi/trans-disciplinary cybersecurity approaches	X	X	X	X	X
Need 2: require human-centric coursework			X	X	X
Need 3: teach tech in respect to the human		X			X

Specific details concerning the Modeling and Simulation of Behavioral Cybersecurity Certificate are presented so that educators can use the certificate program as a template available for replication. Additionally, we present the details of the specific courses within the program as a means of initiating discussion. We encourage others to take an in-depth look into these details and provide constructive feedback with justification. Inter/Multi/Trans-disciplinary work does not occur in a vacuum. Without respectful discussion, education can potentially lead to siloed training. We intend to increase program transparency in hopes of enhancing cybersecurity education overall.

REFLECTIONS OF THE PILOT CERTIFICATE AND FUTURE WORK

The pilot certificate program expects the inaugural cohort to receive the degree December 2016. However, the graduate program has collected perceptions and ongoing feedback from the students and observers to the program, noting several insights. Firstly, these stakeholders are confirming that the program is indeed necessary. The vast majority of cyber educational programs at colleges and universities worldwide focus almost exclusively on the tools and technical aspects of cybersecurity. While necessary, this approach is incomplete. Second, graduate students will be involved heavily in shaping this new human-centric approach. Graduate students are expected to take responsibility for their own learning and to make an impact on their domain with ongoing research in behavioral cybersecurity. The students' work will inform the research of the major professors and in turn, shape the curriculum as it develops. IST is currently conducting initial research into the non-technical, cognitive aspects of cybersecurity but expansion will be required in the near- and long-terms. Specifically, we plan to identify necessary KSAs further, creating a fully comprehensive list for future publication. This list will include generalizable "soft" skills encouraging problem-solving, communication, leadership, innovation, and creativity. Third, recruitment effort towards female applicants should be prioritized. As noted above only 12 out of the 117 respondents were female. Additionally, 100% of the 13 students enrolled in the pilot certificate program at present are male. This finding reflects the shortage of females in technical fields (Shumba et al., 2013, June), and could *possibly* contribute to the tendency to approach cyber-issues from a wholly technical standpoint. However, it could be argued that particular individuals are drawn to specific fields based on *personality* traits rather than gender. Thus, future research should address gender differences and personality traits of cyber-operators and how these characteristics affect techno-centric versus holistic problem-solving within cyber-issues. Further, efforts to verify and validate the survey used in this research are needed. We plan to address this in future publications. Finally, a broader cyber-education framework and standards need to be developed to support the program over the long run.

Although every aspect related to cybersecurity is inseparable from human behavior (*human* hackers attack *human* victims) training to prevent or respond to attacks focuses heavily on technical aspects and fails to prioritize human elements. "The cyber content is very important, but as a means to an end, not the end in itself" (McDade-Morrison, 2014). Emphasizing technical aspects within cyber-education prepares trainees to respond to only part of the problem. The breadth of content available within cyber-education makes it difficult to cover all essential knowledge, skills, and abilities (KSAs) necessary to the field and each specialization (e.g., specific tools). Thus, emphasis should be placed on "softer" more human-centric skills, fostering innovation, problem-solving, and self-directed inquiry (McDade-Morrison, 2014). Current efforts within the U.S. government are adequate but must continue to evolve and expand to meet the non-technical, behavioral challenges within cyberspace. Only then can we begin to turn the corner and get ahead of the cyber threats and vulnerabilities that exist in today's cyber-dependent world.

ACKNOWLEDGEMENTS

We would like to acknowledge the efforts of our Bird-dog, Leslye McDade-Morrison. Thank you, Leslye for your feedback, direction, and for keeping us accountable. We would also like to acknowledge the efforts of Sabrina Gordon for assisting us with the demographic data from the UCF Modeling and Simulation of Behavioral Cybersecurity Certification.

REFERENCES

Conti, G., Weigand, M., Skoudis, E., Raymond, D., Cook, T., & Arnold, T. (2014). Towards a Cyber Leader Course Modeled on Army Ranger School. *Small Wars Journal*.

DoD. (2015). *The Department of Defense Cyber Strategy*. Retrieved from http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.

McDade-Morrison, L. (2014). *Cyber Space Engineer Learning Lab: Facilitators Guide to Course Methodology and Innovation.*

Pfleeger, S. L., & Caputo, D. D. (2012). Leveraging behavioral science to mitigate cyber security risk. *Computers & security*, *31*(4), 597-611.

Shumba, R., Ferguson-Boucher, K., Sweedyk, E., Taylor, C., Franklin, G., Turner, C., & Hall, L. (2013, June). *Cybersecurity, women and minorities: findings and recommendations from a preliminary investigation.* Paper presented at the ITiCSE working group reports conference on Innovation and technology in computer science education-working group reports.

X-Force. (2016). *IBM X-Force Threat Intelligence Report 2016*. Retrieved from http://www-03.ibm.com/security/xforce/downloads.html

University of Central Florida (UCF), (2016). Graduate Catalogue 2016-2017: Modeling and Simulation of Behavioral Cybersecurity Certificate. Retrieved from https://www.graduatecatalog.ucf.edu/programs/program.aspx?id=11981&program=Modeling%20and%20Simulation%20of%20Behavioral%20Cybersecurity%20Certificate

Waldrop, M. M. (2016). How to hack the hackers: The human side of cybercrime. Nature, 533(7602), 164–167. http://doi.org/10.1038/533164a