Journal of Cybersecurity Education, Research and Practice

Manuscript 1086

Security Simulations in Undergraduate Education: A Review

Joseph Simpson

Aaron Brantly

Security Simulations in Undergraduate Education: A Review

Abstract

Several decades of research in simulation and gamification in higher education shows that simulations are highly effective in improving a range of outcomes for students including declarative knowledge and interest in the topic being taught. While there appears to be a broad array of options to provide education in an undergraduate setting related to security, no previous reviews have explored computer-based simulations covering all facets of security. Given the increasing importance and adoption of interdisciplinary educational programs, it is important to take stock of simulations as a tool to broaden the range of problems, perspectives, and solutions presented to students. Our review provides an overview of computer-based simulations in U.S. undergraduate institutions published in academic journals and conferences. We identify strengths and limitations of existing computer-based simulations as well as opportunities for future research.

Keywords

Security, Simulations, Education

INTRODUCTION

There is an increasing demand for professionals with interdisciplinary, "hands on" experiences, particularly in fields related to cybersecurity (Emmersen, Hatfield, Kosseff, & Orr, 2019; Hosseni, Hartt, Mostafapour, 2019; Pencheva, Hallett, Rashid, 2020). All too often when students complete undergraduate curriculums they are filled with rote knowledge. They are well-versed in their field of academic study through years spend in lecture halls. Yet, as they enter the marketplace, they are ill-suited to deal with the demands of complex and often nuanced fields for which the best training is often experience. Often, students leave their disciplinary homes in departments of computer science and engineering, business or social science without an appreciation or comprehension of the interconnections of fields across disciplines. There is an increasing trend in academia towards interdisciplinary studies (Grillis, Driscoll, Hodgins, Fraser, & Jacobs, 2017; Holly, 2017). Often interdisciplinary programs are broad in nature, covering concepts related to mathematics to history. For years colleges and universities large, such as Virginia Tech or small such as Queens University of Charlotte have designed and developed programs that seek to augment the intellectual development of students through interdisciplinarity. Often these interdisciplinary programs harken back to the days of a holistic liberal arts education, yet within the larger university environment interdisciplinarity has grown in popularity as it has become apparent that complex problems cannot be solved from a single disciplinary perspective (Grillis et al., 2017).

Healthcare serves as an example of a field in which the conventional academic disciplines of computer science, medicine, sociology, biology, psychology, and others converge to address complex, multifaceted problems. Like healthcare, agriculture, economics, business, cybersecurity, environmental security, domestic politics, international relations and more require experts from disciplines ranging from psychology to engineering. Fields that touch on concepts of security are particularly in need of interdisciplinarity. Security defined as "the quality or state of being secure" is intrinsically multifaceted and transdisciplinary. Changes in relative security in one dimension can profoundly impact other dimensions. The challenges of protecting people, information, assets, and the environment require interdisciplinary programs that support interest in, and an appreciation and comprehension of the complexity issues across disciplines. We propose that the best way to achieve transdisciplinary perspectives through interdisciplinary education is through the utilization of simulations that are foundationally interdisciplinary in nature. Therefore, we seek to further expound upon the work of Payne, Mayes, Paredes, Smith, and Wu (2021) in interdisciplinary security education by examining the state-of-the-art regarding

security simulations that can be used in interdisciplinary security programs to potentially create high-impact educational opportunities.

The design, implementation and scaling of interdisciplinary programs is difficult. New fields of inquiry and new technologies have created a need for creative educational solutions that foster the value added of a higher education. Embedding a diversity of thought and perspective is one way to help combat what Tomlinson (2008) finds is a decline in the perceived value of university education. Moreover, there is an increasing demand for students with security-related training and education (McCauley, 2019). As professional educators, professors are caught between the disciplinary confines of their field of inquiry with its proscribed metrics for producing students who complete certain classes in line with a major or minor field of study and the demands of both students and the marketplace for increased diversity of thought, perspective, and experience. Simulations provide benefits that straddle these often-competing demands and address student and faculty needs including increased declarative knowledge and interest in the subject matter (Wilson, Bedwell, Lazzara, Salas, Burke, Estock, Orvis, & Conkey, 2009). Thus, it is important to identify computer-based simulations that can efficiently and effectively improve education in undergraduate studies in a variety of programs as well as attract students to learn more about security.

Decades of research on simulation and gamification in higher education have shown promise for improving a wide range of outcomes among students. Studies show that simulations improve educational outcomes ranging from knowledge and comprehension to enjoyment (see Wilson et al., 2009 for a review). The use of simulations and exercises has been identified as critical in fields as diverse as crisis management (Cottam & Preston, 1997) to nursing (Myler & Seurynck, 2016). Within the last decade, there has been increasing interest in simulations within various areas of security and more computer-based simulations are being introduced frequently.

While some studies on simulations have involved concepts such as cyber security (e.g., Cone, Irvine, Thompson, & Nguyen, 2007), none appear to be comprehensive and inclusive of security issues ranging from crime to national security. For example, Awojana & Chou (2019) provide a recent review of the state of cyber simulations in published research, but omit other areas of security that would be useful for interdisciplinary courses. Moreover, they only identified a handful of simulations that have been used in education that have been published in scholarly research. This dearth of research is important because courses in security, especially those related to national security, span topics ranging from managing teams of personnel during an incident to reacting to physical or environmental incidents – indicating a need for programs that expose

students to a broad range of topics that are relevant to security and also highlighting the need for interdisciplinary security programs.

The purpose of this literature review is to evaluate the current state of security simulations and their delivery platforms in undergraduate education via computer-based programs with an emphasis on discovering programs that are comprehensive of security issues ranging from cybersecurity to disaster response. By doing so, we can identify opportunities to integrate various simulations into interdisciplinary courses on security as well as opportunities for more research on simulations that are not examined here. Security as we define it in this paper is a spectrum from secure to insecure and constitutive of four interlocking fields that include digital security, economic/business security, environmental security and human security each contributing to what we refer to as integrated security. We recognize that when combined there is no perfect security, but rather a combination of securities to achieve efficient and equitable states. Managing security across these fields requires preparation for, response to, and recovery from incidents which might undermine any or all of these fields both discretely and concurrently.

To assess simulations and their utility in teaching students or practitioners how to balance the demands of competing fields of security we iteratively build our analysis over four sections below. First, we provide an overview of the use of security related computer-based simulations in higher education and their effect on student outcomes. Second, we provide a compendium of computer-based security simulations currently available for use. Third, we provide a review of security simulations in undergraduate education. A thorough review of existing platforms and methodologies is important in establishing the utility of and metrics for the evaluation and assessment of simulations as components of security education in university education. Finally, we review directions for future research and limitations of current platforms and methodologies.

EDUCATIONAL SECURITY SIMULATIONS: AN OVERVIEW

Simulations have been used in academic instruction for decades. Their creation and use in university settings is often tied to gamification, gaming, or serious games. For the purposes of this review, we are interested in computer-based simulations used in courses in academic settings. Stated differently, we review computer-based security simulations used specifically for education that appear in academic journals, regardless of whether they were developed for that purpose.

We broadly define simulations *as artificially constructed activities, with sets of rules, and constraints that attempt to represent potential real-world*

phenomenon, with the goal of providing non-lecture, non-wrote based quasi-experiential learning. This broad definition includes two types of simulations: computer-based simulations and non-computer-based simulations. Computer-based simulations include everything from computer games (e.g., SimCity) to computer software programs specifically designed for courses (e.g., CyberCEIGE). Non-computer-based simulations include a range of experiential learning activities targeted towards immersing students in simulated environments. For example, researchers have used escape rooms to teach cybersecurity concepts (e.g., Snyder, 2018) and scenario-based exercises for national security (Corbin, 2018). The key point is that learners are given experience through realistic situations in order to achieve learning objectives. While simulations can be non-computer based, this study focuses on computer-based simulations with an emphasis on those related to security. We did not limit our focus to individual simulations. Consequently, entire platforms that comprise simulations were included in our review (e.g., DETERLabs).

Below we provide an overview of how articles were collected and included as well as an overview of the major findings from research using computer-based simulations. Central to our analysis are the outcomes achieved through the utilization of simulations on computer-based platforms.

REVIEW OF SECURITY SIMULATIONS

Security simulations add an interesting dynamic to educational processes. In cybersecurity, in particular the "hands on" nature of simulations provides students with simulated experience most commonly gained through internships or first jobs. Because many of the skills necessary to function productively in cybersecurity environments often require the ability to adapt learn dynamically in complex digital environments there is a natural linkage between computer-based cybersecurity simulations and cybersecurity education. Second, due to functional familiarity students already studying computer science, computer engineering, or information technology are likely to adapt to computer-based simulations quickly. Similar synergies are also likely in fields that are heavily computer based but may not apply to other areas of security like physical security or disaster response.

In this review, we searched academic libraries (e.g., EBSCO Host), Web of Science and Google Scholar to identify research on the topic of security and simulations within the last few years. We omitted from the search any articles or conference presentations on the topic of medicine and hospitals. I did so because searches of simulations on these topics resulted in tens of thousands of studies. For example, searching "emergency response" and "simulation" in Google Scholar returned more than 63,000 results. Consequently, we attempted to narrow

the list by adding additional Boolean operators to searches (e.g., "undergraduate") to ensure that searches returned only relevant results. Furthermore, we limited studies occurring since 2015 given the explosion of research on simulation and gamification in recent years, including the creation of simulation specific journals. Limiting the search to recent years was also important because older computer programs used for simulations on security are likely to be depreciated or abandoned over newer simulations, which was the case in many situations. Another omission criterion was that the simulation was digital or computer-based. The final omission criteria was that the simulation developed or used had to be used in an undergraduate setting in the United States.

Research on security simulations in undergraduate education are predominantly cybersecurity centric. Consequently, most of the studies on such simulations focus on or emphasize cybersecurity concepts. Yamin and Gkioulos (2019) provide a comprehensive review of studies on cyber ranges and security testbeds, comprising nearly one hundred articles, with many consisting of older and non-U.S. based technologies or platforms and very few of these studies examining their use in educational settings. While there may be many tools available for teaching cybersecurity, few have been evaluated in research settings in recent years.

Perhaps the most important element in the utilization of security simulations in undergraduate education is to ensure that the simulation facilitates or directly improves knowledge and understanding of the topic being studied. Many studies identified in this review examined the effect of simulations on knowledge and engagement. Several studies examined the effect of security simulations on knowledge and understanding. For example, in their study of the simulation, Tracer FIRE, Namin and colleagues (2016) found that the simulation improved cybersecurity knowledge, confidence, team-based skills and knowledge. Similarly, Weanquoi and colleagues (2018) evaluated the use of Bird's Life on student test scores for identification of phishing attacks. The authors found that the simulation significantly increased students' scores. Similarly, Burris, Deneke and Maulding (2018) found that their unnamed simulation increased both awareness and knowledge of phishing attempts.

Taken together, these studies provide evidence that security simulations are an effective mechanism for increasing knowledge and comprehension of security-related concepts. However, some caution should be provided. Scholarly research tends to focus on results that are statistically significant and supported. Consequently, simulations that result findings that are not statistically significant are unlikely to be published. Moreover, while many of these simulations are effective for increasing knowledge of specific cybersecurity concepts, there is

little research on the effect of simulations on other areas of security (e.g., national security).

Ensuring increased knowledge and understanding of a specific concept when using a simulation may be most important, but if students are not interested in a simulation, they will be unlikely to derive the most benefit from its use. An important component in the development and utilization of simulations in undergraduate education is to ensure that students are interested in the simulation. Several studies examined the effect of a simulation on level of engagement (e.g., McBurnett, Hinrichs, Seager, & Clark (2018), confidence (e.g., Namin, Aguirre-Munoz, & Jones, 2016), and enjoyment (e.g., Weanquoi, Johnson & Zhang, 2018). For example, Sigholm, Falco, & Viswanathan (2019) studied the use of High-Fidelity Live Exercises (HiFliX) and found that their exercise increased participant satisfaction and students' preference for this method of instruction was greater than traditional methods. Other studies have examined the impact of simulations on interest in the field of cybersecurity (e.g., Mountrouidou, Li, & Burke, 2018), indicating that some simulations may be most appropriate as recruitment tools for high school and entering undergraduates. Interest in the topic is especially important regarding issues such as safety training and education, hence the need for simulations that engage students in other fields such as emergency response (e.g., Brown & Poulton, 2018).

On the cutting-edge of technology as of 2020, Seo, Bruner, Payne, Gover, McMullen, & Chakravorty (2019) examined the benefits of virtual reality in enhancing recollection as well as perceptions of the benefits from respondents in cybersecurity education. Only one study utilized Virtual Reality (VR), suggesting that VR technologies in cybersecurity education are nascent.

Most of the studies used small sample sizes with some studies using samples as small as 13 students. Table 1 below provides an overview of the studies I identified.

Table 1. Studies on Security Simulations in Undergraduate Education

Author	Year	Journal or Outlet	Outcome(s) evaluated	Notes
Sigholm, Falco, & Viswanathan	(2019)	Hawaii International Conference on System Sciences	• Participant Satisfaction • Perceived Difficulty • Preference over other instruction	Choose your own adventure style game Critical Success Factors:

			methods and activities • Competence	• Support team • Remote virtualized environment No availability for exercise outside of MIT/NASA JPL
Buckley, Zalewski, & Clarke	(2018)	International Journal of Advanced Computer Science and Applications,	• Improvement in test scores	Software Engineering and Programming Cyberlearning Environment (SEP-CyLE)
Burris, Deneke, & Maulding	(2018)	HCI in Business, Government, and Organizations	• Test scores • Identification of phishing attacks	Students using the simulation increased recognition of phishing when using the experiential learning activity.
McBurnett, Hinrichs, Seager, & Clark	(2018)	Simulation & Gaming	• Cognitive engagement • Affective engagement • Intrinsic motivation • Understanding	LA Water Game University Specific Some students expressed strong intrinsic motivation
Mcdonald, Hansen, Balzotti, Tanner,	(2019)	Proceedings of the 52nd Hawaii International	• Interest in cybersecurity	Cybermatics

Winders, Giboney, & Bonsignore		Conference on System Science	• Confidence in career • Understanding of penetration testing • Leadership • Communication • Adaptability • Problem Solving • Ethics • Programming • Self-learning • Leadership	University specific
Herr & Allen	(2015)	Proceedings of the 2015 ACM SIGMIS Conference on Computers and People Research	• Not Applicable	Marine Doom America's Army Virtual Combat Convoy Trainer Outlines the effective attributes of a video game for cyber warriors
Seo, Bruner, Payne, Gover, McMullen, & Chakravorty	(2019)	Journal of Computational Science	• Recollection • Perceived Benefit of VR technology	CiSE-ProS Virtual Reality Simulator
Saiya	(2016)	Journal of Political Science Education	• Simulation did not affect foreign policy attitude	Statecraft

			• Induced moderation among students who were initially hawkish or dovish	
Weiss, Turbak, Mache, & Locasto	(2017)	IEEE Security & Privacy	• Student enjoyment	EDURange Describes benefits of EDURange
Arends, Deussen, Green, Rush, Mache, and Weiss	(2018)	Proceedings of the International Conference on Security and Management (SAM)	• No outcomes examined	EDURange National Cyber League
Brown & Poulton	(2018)	International Conference on Applied Human Factors and Ergonomics	• Satisfaction • Excitement • Challenge	Harry's Hard Choices
Mountrouidou, Li, & Burke	(2018)	Proceedings of the 23rd Annual ACM Conference on Innovation and Technology in Computer Science Education	• Interest in Cybersecurity • Perceptions of Cybersecurity • Knowledge • Problem-solving • Confidence	Interdisciplinary course Cyberpaths University specific
Namin, Aguirre-Munoz, Jones	(2016)	Annual International Conference On Computer Science Education:	• Cyber knowledge • Team-based knowledge	Tracer Fire

		Innovation & Technology	• Cyber skill confidence • Team skill confidence	
Chisholm	(2015)	Doctoral Dissertation	• Perceived Usefulness	Metasploitable 2.0 Kali Linux Virtual Lab
Weanquoi, Johnson, & Zhang	(2018)	Journal of Cybersecurity Education, Research and Practice	• Test scores • Enjoyment • Difficulty • Motivation • Effort • Interest	Bird's Life Sample of computer science students
Peruma, Malachowsky, & Krutz	(2018)	ACM/IEEE 1st International Workshop on Security Awareness from Design to Deployment	• Interest in cybersecurity • Willing to recommend • Realism • Adoption (faculty)	PLASMA

SECURITY SIMULATION SOFTWARE

Security simulations are categorized into four categories based on common features or focus: information or cyber security, general security, disaster response and preparedness, and national security, war and wargaming. The first category, information or cyber security, deals with simulations primarily focused on the protection of information assets. For example, simulations dealing with information threats (e.g., hackers), attack detection (e.g., sniffers), and response (e.g., data breach response) are included in this category. The second category emphasizes general security simulations not primarily focused on information or cyber threats. For instance, simulations focused on physical asset protection are

included in this category. Similarly, intrusion detection and response not related to cyber security are also included. The third category includes disaster response and preparedness simulations. These simulations include natural disasters and emergency management activities. Examples include weather-related incidents like hurricanes and response to terrorist attacks. The key difference here between general security and disaster response and preparedness is *who* is the focus of the activities. More specifically, the focus of general security is security-related personnel (e.g., law enforcement) while the focus of disaster response and preparedness is emergency responders (e.g., fire departments). We recognize that some simulations emphasize both. In such cases, we opted to include the simulation under the category that emphasized one more than the other. For example, simulations typically had a clear majority of actions or activities related to law enforcement *or* emergency management. Finally, we included national security, war and war gaming for our final category of simulations. These simulations were focused on war-related activities from an individual (e.g., soldier) to unit (e.g., brigade, division, or branch) level of war to national security and global policy activities.

To examine the state of security simulations in undergraduate research available as of this study, we examined the availability of existing simulations. Table 2 provides an overview of the simulations identified in this study and the ease of access to them. Surprisingly, many simulations used in undergraduate education are university specific, require fees, or are simply no longer available. Indeed, of the 28 simulations we identified, only nine were completely free and available for use online.

Table 2. Computer-based Security Simulations used in Undergraduate Education

Name	**Available?**
Information or Cyber security	
CyberCIEGE	Yes - Faculty must register
Bird's Life	Not Available
CyberNexs	Not Available
CyberProtect	Yes - Free
GenCyber	Yes – Faculty must register
SecurityCom	Not Available

CyberAware	Yes- Paid service
PLASMA	Yes -
Software Engineering and Programming Cyberlearning Environment (SEP-CyLE)	Yes - Faculty must register (now STEM-CYLE)
CiSE-ProS VR	Not Available
EDUrange	Yes - Faculty must register
SEED Labs	Yes - Free
DeterLabs	Yes - Faculty must register
SMALLWorld	Not Available (Italy)
Tracer FIRE	Yes- In person only
Metasploitable	Yes - Free
Cyberpaths	University Specific
General Security	
Cold Case	University Specific
Crime Scene	University Specific
Bioattack	University Specific
Disaster and Emergency Response and Preparedness	
LA Water Game	Not Available
Harry's Hard Choices	Yes - Paid Service
Disaster in my backyard	Not Available
National Security, War and Wargaming	
Statecraft	Yes - Paid Service
US Navy's Massive Multiplayer Online War Game Leveraging the Internet	Not available
America's Army	Yes - Free
Virtual Combat Convoy Trainer	Not Available
Marine Doom	Not Available

From the simulations still available in Table 2, we further explored their coverage across concepts (categories) of security in Table 3. Coverage was established based on one of three criterion across multiple categories. University specific and not available programs were not evaluated in this table.

Table 3. Evaluation of simulations

	Topic				
Simulation Name	**National Security**	**General Security**	**Cyber Security**	**Disaster and Emergency Response and Preparedness**	**Notes**
CyberCEIGE	NC	SC	CC	NC	Most Coverage Dated technology and interface Limited Number of Scenarios Scenarios often require in-depth knowledge
GenCyber	NC	NC	CC	NC	Camp-based education focused on K-12 level
Statecraft	CC	SC	NC	SC	265 Universities Foreign policy and national

					security focused
SEED Labs	NC	NC	CC	NC	30 Labs University focused Beginner to advanced focused
America's Army	CC	NC	NC	NC	Primarily a recruitment tool for the U.S. Army
EDURange	NC	NC	CC	NC	Education-based
CyberAware	NC	NC	SC	NC	Primarily Phishing focused
Metasploitable	NC	NC	CC	NC	Vulnerable Linux Virtual Machine
SEED Labs	NC	NC	CC	NC	Wide adoption in universities
Harry's Hard Choices	NC	NC	NC	SC	Narrow focus on mining operations
DeterLabs	NC	NC	CC	NC	Wide adoption in universities
STEM-CYLE	NC	NC	CC	NC	Integrative platform
PLASMA	NC	NC	CC	NC	Focused on mobile and app security

CyberProtect	SC	NC	SC	NC	Department of Defense

CC – Moderate to Complete Coverage of topic

SC – Some Coverage

No – Coverage

Cyber Security Simulations

Awojana & Chou (2019) provided a recent review of various cybersecurity simulations and games. They identified eight cybersecurity games used in higher education settings in their review that had been published or presented at conferences. These games are shown in Table 2. They note several disadvantages and a lack of comprehensiveness across cyber security domains among many of the games. Specifically, while some games covered topics such as awareness, they omitted defensive or attacker strategies. Conversely, some games covered defensive strategies while omitting awareness. Exceptions to this include InCTF and GenCyber. However, both simulations are not available to the general public.

This review identified several additional simulations used in undergraduate research. Drawing from the studies identified in Table 1, most simulations focused on wholly or primarily on cybersecurity concepts with 17 of 28 simulations in this category. CyberCEIGE is the most comprehensive simulation in its coverage of security concepts, with broad emphasis on concepts related to cybersecurity (e.g., setting up a firewall) to physical security (e.g., controlling access to classified or restricted areas). Most simulations within information or cybersecurity emphasize a range of topics and issues. For example, SEED and DETER labs both cover elements of cybersecurity ranging from encryption to various cyberattacks. An exemplar of immersive simulations was the CiSE-ProS VR simulation mentioned previously. One study using W4IPS, showed promise for application in use for security in undergraduate education, but it was unclear whether students experienced a security issue as part of their simulation experience (Mao, Huang, & Davis, 2019). Other simulations were very limited in focus, likely due to their use to teach a specific concept (e.g., phishing). An example of such a simulation includes Bird's Life. Additionally, most labs were not immersive or aesthetically pleasing.

When reviewing these eight games, we noted that many were dated, materials for instructors were often limited, and some were no longer in existence or required on-site support from the providing entity.

General Security

General security refers to protection of information, assets, and people. Concepts covered include physical security, crime prevention and forensics, physical protection, and access controls, among others. One simulation, CyberCEIGE covers some concepts related to security such as physical security requirements, but the primary emphasis is on cybersecurity. Although some simulations covered concepts of security (e.g., crime), none were publicly available for use. Examples of general security simulations included Cold Case, Crime Scene, and Bioattack.

Disaster and Emergency Response and Preparedness

While there are many more computer-based simulations related to disaster and emergency response and preparedness than displayed in Table 2, most were documented in courses prior to 2015 (outside of the scope of this review), developed or researched outside of the U.S., or not included in undergraduate coursework. Only one was still available and is available as a paid service, Harry's Hard Choices.

National Security, War and Wargaming

Two simulations for national security, war and wargaming are used in undergraduate education based on the inclusion criterion of this review. One simulation, Statecraft, covers national security, but the focus of the simulation places emphasis on political science as a general field. Consequently, national security represents an often-minor element of the simulation. The other simulation, America's Army, focuses on education and recruitment of future soldiers.

REVIEW OF SIMULATIONS

Our review of each of the areas of security simulations in undergraduate research revealed several limitations of existing platforms. First, many platforms no longer exist or are publicly unavailable. Many of the simulations were developed specifically for a course at a specific university. Second, no simulation that we identified comprised all elements of security. Third, in our searches even targeted searches of military simulations were inundated with results related to nursing and education. Fourth, while government and industry simulations for education and application to security scenarios exist, few have been evaluated in undergraduate education in journals or conferences. Moreover, many of the tools developed to train and educate users about security, especially cybersecurity, are developed and maintained by commercial vendors. This structure increases the costs for students and limits their ability to access content.

Several limitations of current simulations platforms and their adoption exist. While many of the programs were interesting, all lacked elements of interest

covering all topics of security. This presents a significant limitation for universities attempting to standardize curriculum.

The program that showed the most promise and most rigor in terms of use for security education in undergraduate courses is CyberCEIGE. CyberCEIGE, a program designed and run out of the Naval Post-Graduate School offers students a visually interactive, SimCity simulacra tailored to cybersecurity and information security related constructs. While CyberCEIGE is visually and functionally one of the most promising programs, the projects by SEED Labs and DETERLabs were the most polular platforms, as evidenced by their use across 250 institutions (Du, 2015), and 103 universities (Arends, Deussen, Green, Rush, Mache, & Weiss, 2018) respectively, but is not user friendly for non-technical focused programs. SEEDLab was the outgrowth of a 2002 NSF grant and according to its creators has been tried or implemented in more than one thousand educational institutions.

The CyberPaths program developed by College of Charleston and Johns Hopkins University is tailored to liberal arts programs and offers an easy entry point to a diverse cybersecurity curriculum (Mountrouidou et al., 2018; Mountrouidou and Li, 2019). The program was employed as a course-based delivery of cybersecurity, political science, and humanities. The course uses a combination of labs, readings and projects to increase security education among first-year liberal arts students. Students in the course developed their own projects and simulations. Post simulation engagement, a formal rubric for assessing the completion of learning objectives was not apparent within the scholarly literature, but a further analysis of the project pages itself, highlights a both objective and subjective measurement tools in the form of projects and homework tasks.

DISCUSSION

This review identified that most security simulations focus on cybersecurity and revealed there is a dearth of research on computer-based simulations focusing on other categories of security in the United States. When starting this review, we expected there to be considerably more computer-based simulations that have been examined in research on undergraduate courses on the topic of security. However, many platforms and tools have not been evaluated despite their apparent use in undergraduate education. Moreover, many tools are lacking in coverage, potentially leaving undergraduates with incomplete knowledge in cybersecurity. Consequently, what is needed is a unified platform for conducting simulation-based assignments across the spectrum of security issues in undergraduate education coupled with a substantial body of research backing its effectiveness in achieving stated learning objectives for each concept.

Limitations and Future Research Directions

There are several limitations of this study. First, our focus was limited to computer-based simulations used in undergraduate education. Many programs may be available that are not used in undergraduate education that are adequate for education. Second, our search criteria were narrowly focused and may have omitted other platforms that have been used in undergraduate research.

Additionally, our review was limited to studies within the last few years. Consequently, universities may have identified superior computer-based simulations to use in their curriculum that have previously been validated. For example, SEEDLabs have been used in undergraduate education for well over a decade but were not mentioned in more recent reviews. Similarly,

Fourth, because the review included specific terms such as "simulations" and "serious games", computer-based programs where developers and authors avoided such terminology may be omitted. For example, these simulations may be described as "labs" or "virtualization." Searches were conducted for each of these as well, but there may be more variants of terminology for simulations that were not used for the searches in this manuscript.

During the review, several areas for future research emerged. First, much more research is needed in evaluating the effectiveness of simulations on comprehension and interest for other areas of security such as national security. Second, more research is needed evaluating whether existing simulations are adequate for teaching security concepts that cover multiple areas of security. For example, simulations are needed for much higher-level concepts such as responding to national disasters and international conflicts on cybersecurity. While students may currently be exposed to one of these concepts, there appear to be no existing simulations that explores knowledge integrating the two areas.

Although it was not the primary focus of this literature review, we found it interesting that the instructor or adoption of simulations in this realm are notably limited in research. Perhaps one of the most important questions given the problems we identified in the introduction of this manuscript is that if a simulation is too complex and the learning curve too high for instructors, then wide-spread adoption will fail. Consequently, they will not benefit from its use in their courses. Stated differently, if students like the program but instructors will not adopt it, then the simulation is useless.

REFERENCES

Arends, R., Deussen, R., Green, B., Rush, J., Mache, J., & Weiss, R. (2018). Get a Clue: A Hands-On Exercise for Password Cracking. In *Proceedings of the International Conference on Security and Management (SAM)* (pp. 117-121). The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp).

Awojana, T., & Chou, T. S. (2019). Overview of Learning Cybersecurity Through Game Based Systems. In *Proceedings of the 2019 Conference for Industry and Education Collaboration.* American Society for Engineering Education.

Brown, L. D., & Poulton, M. M. (2018, July). Improving Safety Training Through Gamification: An Analysis of Gaming Attributes and Design Prototypes. *In International Conference on Applied Human Factors and Ergonomics* (pp. 392-403). Springer, Cham.

Buckley, I. A., Zalewski, J., & Clarke, P. J. (2018). Introducing a Cybersecurity Mindset into Software Engineering Undergraduate Courses. *International Journal of Advanced Computer Science And Applications, 9*(6), 448-452.

Burris, J., Deneke, W., & Maulding, B. (2018, July). Activity Simulation for Experiential Learning in Cybersecurity Workforce Development. In *International Conference on HCI in Business, Government, and Organizations* (pp. 17-25). Springer, Cham.

Chisholm, J. A. (2015). *Analysis on the perceived usefulness of hands-on virtual labs in cybersecurity classes.* (Doctoral dissertation, Colorado Technical University).

Cone, B. D., Irvine, C. E., Thompson, M. F., & Nguyen, T. D. (2007). A video game for cyber security training and awareness. *Computers & Security, 26*(1), 63-72.

Corbin, T. B. (2018). Teaching Disaster Management Using a Multi-Phase Simulation. *International Journal of Mass Emergencies & Disasters*, *36*(3), 297-312.

Cottam, M.,& Preston, T. (1997).An overview of the value and use of simulations in the academic, business and policy communities. *Journal of Contingencies and Crisis Management*, *5*(4), 195-197.

Du, W. (2015, February). SEED Labs: Using Hands-on Lab Exercises for Computer Security Education. In *Proceedings of the 46th ACM Technical Symposium on Computer Science Education,* (pp 704-704), ACM.

Emmersen, T., Hatfield, J. M., Kosseff, J., & Orr, S. R. (2019). The USNA's interdisciplinary approach to cybersecurity education. *Computer, 52*(3), 48-57.

Gillis, D., Nelson, J., Driscoll, B., Hodgins, K., Fraser, E., & Jacobs, S. (2017). Interdisciplinary and transdisciplinary research and education in Canada: A review and suggested framework. *Collected Essays on Learning and Teaching, 10*, 203-222.

Herr, C., & Allen, D. (2015, June). Video games as a training tool to prepare the next generation of cyber warriors. In *Proceedings of the 2015 ACM SIGMIS Conference on Computers and People Research*, (pp. 23-29). ACM.

Holley, K. (2017). Interdisciplinary curriculum and learning in higher education. *In Oxford research encyclopedia of education,* 1-44.

Hosseini, H., Hartt, M., & Mostafapour, M. (2019). Learning is child's play: game-based learning in computer science education. *ACM Transactions on Computing Education (TOCE), 19*(3), 1-18.

Mao, Z., Huang, H., & Davis, K. (2019). W4IPS: A Web-based Interactive Power System Simulation Environment for Power System Security Analysis. *arXiv preprint arXiv:1909.06952*.

McBurnett, L. R., Hinrichs, M. M., Seager, T. P., & Clark, S. S. (2018). Simulation gaming can strengthen experiential education in complex infrastructure systems. *Simulation & Gaming*, *49*(6), 620-641.

McCauley, A. (2019). How to meet the growing demand for cybersecurity professionals. Securitymagazine.com. Retrieved from https://www.securitymagazine.com/articles/90203-how-to-meet-the-growing-demand-for-cybersecurity-professionals.

Mcdonald, J., Hansen, D., Balzotti, J., Tanner, J., Winters, D., Giboney, J., & Bonsignore, E. (2019, January). Designing Authentic Cybersecurity Learning Experiences: Lessons from the Cybermatics Playable Case Study. In *Proceedings of the 52nd Hawaii International Conference on System Sciences*.

Mountrouidou, X., Li, X., & Burke, Q. (2018, July). Cybersecurity in liberal arts general education curriculum. In *Proceedings of the 23rd Annual ACM Conference on Innovation and Technology in Computer Science Education* (pp. 182-187). ACM.

Mountrouidou, X., & Li, X. (2019, February). Cyber Security Education for Liberal Arts Institutions. *Journal of The Colloquium for Information System Security Education*, *6*(2), 17-17).

Myler, L. A., & Seurynck, K. (2016). Student evaluation of simulation in a new hospital-based simulation center. *Nursing Education Perspectives*, *37*(6), 335-336.

Namin, A. S., Aguirre-Muñoz, Z., & Jones, K. S. (2016). Teaching cybersecurity through competition. *In Annual International Conference on Computer Science Education: Innovation & Technology* (pp. 98-104).

Payne, B. K., Mayes, L., Paredes, T., Smith, E., Wu, H., & Xin, C. (2021). Applying High Impact Practices in an Interdisciplinary Cybersecurity Program. *Journal of Cybersecurity Education, Research and Practice, 2020(*2), 4.

Pencheva, D., Hallett, J., & Rashid, A. (2020). Bringing cyber to school: Integrating cybersecurity into secondary school education. *IEEE Security & Privacy*, *18*(2), 68-74.

Saiya, N. (2016). The statecraft simulation and foreign policy attitudes among undergraduate students. *Journal of Political Science Education*, *12*(1), 58-71.

Seo, J. H., Bruner, M., Payne, A., Gober, N., & Chakravorty, D. K. (2019). Using Virtual Reality to Enforce Principles of Cybersecurity. *Journal of Computational Science*, *10*(1).

Snyder, J. C. (2018), "A Framework and Exploration of a Cybersecurity Education Escape Room." Theses and Dissertations. 6958. https://scholarsarchive.byu.edu/etd/6958

Sigholm, J., Falco, G., & Viswanathan, A. (2019). Enhancing Cybersecurity Education through High-Fidelity Live Exercises (HiFLiX). In *Hawaii International Conference on System Sciences* (pp. 7553-7562).

Tomlinson, M. (2008). 'The degree is not enough': students' perceptions of the role of higher education credentials for graduate work and employability. *British Journal of Sociology of Education*, *29*(1), 49-61.

Weanquoi, P., Johnson, J., & Zhang, J. (2019). Using a Game to Improve Phishing Awareness. *Journal of Cybersecurity Education, Research and Practice*, *2018*(2), 2.

Weiss, R., Turbak, F., Mache, J., & Locasto, M. E. (2017). Cybersecurity education and assessment in EDURange. *IEEE Security & Privacy*, *3*, 90-95.

Wilson, K. A., Bedwell, W. L., Lazzara, E. H., Salas, E., Burke, C. S., Estock, J. L., ... & Conkey, C. (2009). Relationships between game attributes and learning outcomes: Review and research proposals. *Simulation & Gaming*, *40*(2), 217-266.

Yamin, M. M., Katt, B., & Gkioulos, V. (2019). Cyber Ranges and Security Testbeds: Scenarios, Functions, Tools and Architecture. *Computers & Security*, 101636.