International Journal of Smart Education and Urban Society
Volume 13 • Issue 1

A Conceptual Learning Framework of Cybersecurity Education for Military and Law Enforcement:
Workforce Development

Abhijit Kumar Nag, Texas A&M University, Central Texas, USA
https://orcid.org/0000-0002-3520-2935
Vikram S. Bhadauria, Texas A&M University, Texarkana, USA
Camille Gibson, Prairie View A&M University, USA*
Ram C. Neupane, Texas A&M University, Texarkana, USA
Daniel Creider, Texas A&M University, Commerce, USA
https://orcid.org/0000-0002-5857-6622

ABSTRACT

To address cybersecurity threats that organizations are facing today, there is an urgent need for an interdisciplinary approach in educational programming to prepare the next generation of indispensable workers who are often dispersed, such as law enforcement and military personnel. Extensive data breaches and even low profile but high impact cybercrimes present immense challenges for law enforcement, military, and local government agencies. These agencies, by nature, are some of the primary targets of cyberattacks, and hence, cybersecurity awareness and cyber investigation-related education are crucial for meeting the demanding requirements of their job duties and responsibilities. This paper describes the pedagogy of current educational programs for military and law enforcement toward identifying existing gaps in the adult pedagogy used to prepare the workforce. The paper concludes with a proposed framework based on recommendations on domain-specific topics and pedagogical formats for the most effective cybersecurity learning for these dispersed groups.

KEYWORDS

Cyber Awareness, Cyber Investigation, Cyber Threats, Cybersecurity, Deep Learning, Gaming, Law Enforcement, Military, Online Education, Workforce Development

INTRODUCTION

Cyber attacks are prominent (Schjølberg & Ghernaouti-He´lie, 2009). In fact, about 61% of organizations were affected by malware activities in 2020 and 74% were impacted in 2021 (Cook, 2022). These statistics reveal the dire need to prepare our dispersed workforces through cyber security education, cutting-edge cyber investigation techniques, and high-quality cyber hygiene practices. Businesses and government organizations, along with private citizens, are at equal risk of cyber attacks. Even military and police departments are not immune to such threats. Increasingly, cyber

DOI: 10.4018/IJSEUS.309953 *Corresponding Author

criminals deploy novel techniques like ransomware to hack into systems, capture data, and demand a ransom to be paid in an untraceable cryptocurrency (Sganga et al., 2021).

Across the United States, state and local law enforcement organizations share the responsibility of responding to imminent threats to information technology (IT) systems and critical data infrastructures. Nevertheless, too many officers lack the expertise and knowledge to quickly mitigate and adequately investigate these cases, including when their own systems are targeted (Meehan, n.d.). Therefore, we must augment military and law enforcement personnel with the latest tools and resources to outsmart cyber criminals. Cyber threats prove to be dynamic and evolving. There is an urgent need to develop effective training modules designed to facilitate quick learning among adult learners. These types of strategies can better equip law enforcement personnel to face unforeseen challenges.

This article recommends an effective instructional approach to enhance the security of individuals, communities, and the nation, especially given the uptick in large-scale cyber attacks during and after the COVID-19 pandemic. First, the research addresses the gap between cutting-edge technology available to cyber criminals and the existing training of dispersed workers, particularly in U.S. law enforcement and the military. Second, the study presents a pathway to develop or enhance a training framework and methodology to promote puzzle-based learning, experiential learning, and deep learning among the targeted workforces. Indubitably, promoting and expanding cyber security education is essential to an adequately prepared next-generation workforce. Therefore, this article assesses the needs of a dispersed workforce, including those fields that encounter sensitive information and investigative work.

The following section highlights current trends in cyber security and explores existing cyber education for state and local law enforcement agencies and the military. Then, the article discusses game-based learning, deep learning, and experiential learning-based pedagogical techniques for cyber security education. It proposes a cyber security education framework for law enforcement and military workforces. The article concludes with a summary and suggestions for future work.

CURRENT TRENDS AND AFFAIRS IN CYBER SECURITY

The Internet of things (IoT), such as computers and mobile applications, is rapidly increasing (Bhardwaj, 2017). These applications and smart devices will only continue to expand and migrate into 5G networks (Saha et al., 2017). Along with the growing number of smart technologies comes increased security vulnerabilities like malware, distributed denial-of-service (DDoS) attacks, and socially engineered attacks (Humayun et al., 2020). For example, during the pandemic, sectors like education and commerce were largely forced online. Consequently, malicious attackers had a favorable environment to generate their attacks. Hence, there were growing numbers of attacks that involved ransomware, DDoS, malware, malicious domains, malicious Websites, spam e-mail, and malicious social media messaging. Malware and phishing Websites were identified as having the highest increase throughout 2020 (Khan et al., 2020). Hospitals and healthcare organizations were the top targets for these attacks (Hijji & Alam, 2021).

In 2021, public focus shifted to the impact of ransomware attacks, which may or may not have been made public. Some private entities that were unprepared paid the demanded ransom, hoping to keep their victimization private.

It is expected that IoT devices will increase from 20 billion in 2020 to 75 billion in 2025 (Georgiev, 2022). As shown in Figure 1, the global cyber security market was worth US$145 billion in 2018. It is set to increase to US$270 billion by 2026 (FIAL, 2018). Additionally, cyber crime will cost the world US$10.5 trillion annually by 2025 (Morgan, 2020). These trends signify that the need for a cyber security-aware and cyber security-skilled workforce continues to increase. It is particularly important, therefore, that workforce development efforts include effective training initiatives for existing dispersed workers, especially in law enforcement and the military. Such efforts will enhance the overall well-being of individuals, communities, and organizations.

CYBER SECURITY EDUCATION FOR LAW ENFORCEMENT AND MILITARY

Law Enforcement

Demonstration of the following knowledge is required for individuals who will work with cyber security in law enforcement and/or the military: cyber security law and ethics; memory analysis; digital and mobile device analyses; penetration testing; incident response; and reverse engineering (Tsado & Osgood, 2022). Given the national and international nature of cyber crime, most of the cyber security education available to law enforcement is coordinated by the International Association of Chiefs of Police (IACP)'s Law Enforcement Cyber Center (LECC). In addition to offering relevant and evolving training, the LECC facilitates access to the most common credentials for officers in the field of cyber work. According to a Burning Glass (2014) survey report, the most common certifications desired for cyber security law enforcement have been certified information systems security professional (CISSP), certified information systems auditor (CISA), computing technology industry association security+ (CompTIA Security+), certified information security manager (CISM), and global information assurance certification – security essential (GIAC-GSEC). The federally sponsored programs offered by the IACP include an online cyber and information technology certification program (CICP) for developing advanced technical skills.

Further, some of the more high-level specialized training required to perform the most advanced cyber work is provided by the Department of Homeland Security and the National Institute of Standards and Technology (NIST) through a National Initiative for Cybersecurity Education National Initiative for Cybersecurity Careers and Studies (NICE-NICCS) Cybersecurity Workforce Framework. The NICE-NICCS offers training in a federal virtual training environment (FedVTE), including topics like threat analyses, accessing national and international targets, evidence collection operations, and exploitation analyses. The Department of Justice's Computer Crime and Intellectual Property Section (CCIPS) trains state and local law enforcement on a range of cyber crime topics. However, it places emphasis on ethical and legal issues. For federal and military law enforcement officers, the Defense Cyber Crime Center (DC3) offers free online and in-person instruction on cyber crime prevention, foreign intelligence, and cyber-related fraud. Relatedly, the National White Collar Crime Center (NW3C) offers free instruction, financed by the federal government to regulators and law enforcement on topics like mobile and network forensics relevant to white collar crime investigations. For state and local agencies, the Federal Bureau of Investigation (FBI) Cyber Shield Alliance's Virtual Academy Cyber Certification Program offers free online training. This training includes a focus on using eGuardian (a repository of suspicious behavior reports), sharing information and working effectively with the National Cyber Investigative Joint Task Force in the organization's region. There is also instruction on InfraGard, a partnership between private companies and the FBI, that facilitates cyber security collaboration and strategy between private sector critical infrastructure leaders, law enforcement, and the military. Individual officers can register for this training after creating a Law Enforcement Enterprise Portal (LEEP) account.

The U.S. Secret Service facilitates task forces and working groups that assist law enforcement at various levels to partner with academics and the private sector to enhance knowledge on specific threats. They also manage the National Computer Forensic Institute, which offers instruction on cyber crime investigations and electronic evidence. Their training is for law enforcement, prosecutors, and judges. To investigate traditional crimes with cyber-related evidence, SEARCH, The National Consortium for Justice Information and Statistics, assists with cyber investigation training to address consensual crimes, drug offenses, homicide, and gang offenses.

These training opportunities represent substantial progress; however, the overall effectiveness for the broadly nontechnical law enforcement workforce is unclear. Formal education and certifications that reflect work-relevant experiences are necessary for law enforcement's success in cyber security, especially given the prevalence of global digital technologies post-2020 (Tsado & Osgood, 2022).

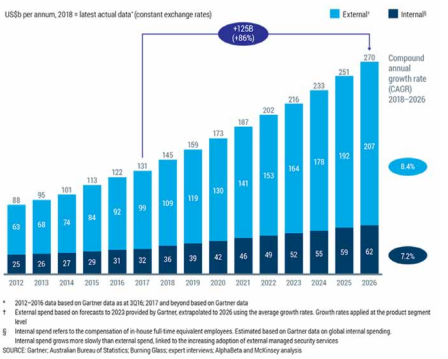
U.S. Military

The U.S. military cyber security concerns include the behaviors of its direct personnel and that of civilians who work closely with the organization, such as contractors. Given this, the Department of Defense (DoD) leads in efforts to build a cyber-aware military culture (DoD, 2018). DoD efforts are informed by academia through a university consortium for cyber security. This is coordinated by the National Defense University's College of Information and Cyberspace in Washington, DC. For military personnel who are active, reserve, National Guard, or civilian, a DC3 Cyber Training Academy offers cyber intelligence and digital forensics training. Indeed, some training begins early in places like the West Point Army Cyber Institute and Modern War Institute. For the U.S. Army, the Cyber Center of Excellence addresses cyber security readiness. Therein is a cyber school, cyber school command, training and education directorate, cyber technical college, cyber leader college, and electronic warfare college. These are responsible for the research and development of cyber-related training for their personnel worldwide. This includes cyber awareness and cyber security fundamentals, related policies, and certifications. The certification training includes CISSP, CISA, National Incident Management System (NMS), Network+, Security+, CompTIA Advanced Security Practitioner (CASP), CISM, and GIAC. The training incorporates the use of cyber challenges and virtual technology. Specific on-site training is available at Fort Bragg in North Carolina, Fort Gordon in Georgia, Fort Hood in Texas, Joint Base Lewis-McChord in Washington, Fort McCoy in Wisconsin, and Camp Robinson in Arkansas. The Defense Information Systems Agency, which offers combat support for dispatched military personnel, also ensures that soldiers and others are cyber-ready. Some training is offered in partnership with the private-sector SANS Institute. This includes common cyber certifications given the cyber workforce readiness expectations set in DoD Directive 8140.

Specialized cyber units will receive more advanced cyber preparation. For the U.S. Navy, the U.S. Fleet Cyber Command/U.S. 10th Fleet manages Navy cyber networks and intelligence. Similarly, the San Antonio, Lackland-based 16th Air Force (Air Force Cyber) leads in cyber Air Force warfare activity. The U.S. Marines have U.S. Marine Corp Cyberspace Command. The U.S. Coast Guard has the Coast Guard Cyber Command.

However, there is no one universal or national indicator of how well the military has done in making its varied workforce effectively cyber aware and cyber secure. Nevertheless, some educators perceive that the dominant NIST-NICE framework, which was designed for the government, is not a perfect work context fit for the nature of cyber security in law enforcement and the military. Toward these efforts, however, this review offers insights on how to make broadly applied cyber security workforce development efforts for dispersed military workers impactful whether these workers are technically or nontechnically inclined.

Figure 1. Global cyber security spendings (Source: Gartner, Australian Bureau of Statistics)



PRIVATE-SECTOR TRAINING ALTERNATIVES

Much of the credentialing for the cyber-ready worker is in the hands of the private sector. Relatedly, there are several U.S.-based vendors who offer cyber security instructions. First, they may increase the cyber security awareness of an institution's general workforce (given that many employees engage with devices that connect to a network or work remotely). Second, they may assist with the credentialing of cyber security professionals.

Table 1 presents examples of well-known vendors in cyber security instruction. For the professionals, much of the instruction includes the following: hands-on, interactive simulated instruction and practice of cases on cyber ranges; risk assessments of company networks and procedures; and preparation for a variety of industry certification credentials. Most of these certifications are good for three years, requiring retesting or continuing education credits to retain the credential. These U.S. credentials are highly esteemed worldwide; however, they cost hundreds of dollars. Besides passing the examinations, individuals typically need a specific number of years of relevant cyber security experience to be fully credentialed or certified. Often, private sector vendors will charge hundreds to thousands of dollars for training programs to prepare individuals for certification examinations. That may, in fact, be cost prohibitive. In some cases, the vendors will bundle the training and the cost of the examination.

Table 1. Examples of leading providers of cyber work-ready instruction in the U.S.

Company	Headquarters	Service Scope	Cyber Awareness	Ranges or Practice	Trainings	Risk Assessments	Certification Preparation
Digital Defense Inc.	San Antonio, TX	Global	X	X	X	X	
KnowBe4	Clearwater, FL	Global	X	X	X	X	
Inspired eLearning	Los Angeles, CA	Global	X				
Security University	Herndon, VA	Global	X	X	X	X	X
InfoSec	Madison, WI	Global	X	X	X	X	X
Secure Ninja	Washington, DC	National		X	X	X	X
Global Information Assurance Certification	Bethesda, MD	Global		X	X	X	X
EC-Council	Albuquerque, NM	Global	X	X	X	X	X

Private vendors have flourished by filling existing gaps, even in the education offered by the most common universities in the field of cyber security. Topics include: (1) collection and operation; (2) analysis; and (3) investigation. These three areas are important in developing cyber security information, testing the usefulness of the knowledge, and the overall investigation of cyber crime IT systems. These categorical gaps can be seen in the U.S. government workforce's field of cyber security. Additionally, to improve the existing cyber skillset in the military environment, there should be a multidisciplinary approach that includes mastering teamwork (Krasznay & Ha´mornik, 2019). More importantly, very few workforce leaders have the operational background to make the best critical decisions in times of cyber crises (Caulkins et al., 2016).

To close the worldwide skill gap in the cyber security workforce, it is essential to increase the number of individuals in the field of cyber security. Organizations should look to university students, IT professionals, and other interested individuals to attract and retain the brightest persons in the cyber domain. Law enforcement and national security communities must also invest in their workforce to bolster their cyber security abilities. This is possible through education and training (Vogel, 2016).

All officers need a range of knowledge about cyber operations. Still, highly technical officers and cyber leaders need a deeper understanding of mathematical knowledge relative to cyber space (Arney et al., 2016). Cyber education should, therefore, include three main levels: (1) what cyber leaders should know; (2) what all officers or military personnel should know; and (3) what highly technical personnel should know. To address the cyber threats, it is appropriate to implement a multilevel and multidiscipline approach to cyber education in the military academy so that individuals can be efficient in their service (Sobiesk et al., 2015).

Creating hands-on exercises can boost cyber security knowledge (Tikk-Ringas et al., 2014). It is a practical method to develop a strong ability for critical thinking. Individuals should practice utilizing encryption and decryption algorithms to master these tools and secure messages using matrix algebra. For instance, a transformation matrix can be applied to encrypt the ciphertext. The matrix inverse of the transformation is used to decrypt the plaintext. Further hands-on cyber security training is an impressive way to raise both soft and hard skills in the cyber security domain. This training is crucial to educating the workforce for mastery and long-term retention.

Visual analytics models can be implemented for these training using a game-like approach (Osˇlejsˇek et al., 2020). In fact, hands-on training for cyber professionals has been moving toward gamification (Zides, 2021). Treiblmaier et al. (2018) defined gamification as:

... using game-design elements in any non-game system context to increase users' intrinsic and extrinsic motivation, help them process information, help them to better achieve goals, and/or change their behavior. (p. 6)

The academic community has been inspired to adopt gamification in its learning. Some theories and associated practices are involved in the process of learning. Bozkurt and Durak (2018) noted that gamification can make teaching and learning more enjoyable by engaging and motivating the gamer toward changes in sustainable behaviors. Results show that gamified learning activities produce positive effects in achieving cognitive knowledge. For example, students are very successful in learning C-programming (Ibanez et al., 2014) and password security awareness (Scholefield & Shepherd, 2019) in gaming learning environments.

Coull et al. (2016) used the gamification approach to create computer game technology aimed at training law enforcement officers to tackle cyber crime. The police officer participants already demonstrated relevant skills to face cyber crime. The participants were evaluated as they played serious games in hypothetical scenarios. After measuring the effectiveness of the training, it was found that the gamification has a strong potential for success in investigating cyber crime. Beyond enhancing skills, it enhances a person's ability to investigate the location of evidence and think proactively about upcoming criminal incidents. This requires a certain level of knowledge given the number of digital devices (i.e., CCTV cameras and IoT) used to store digital evidence that is crucial to today's criminal investigations.

PROPOSED FRAMEWORK BASED ON GAMING, DEEP LEARNING, AND EXPERIENTIAL LEARNING CONCEPTS

Gaming in Cyber Security Education

The creation of an effective educational environment is required to avoid cyber victimization. The use of an applied exercise base is an effective educational practice for preparing users to defend against current threats (Shin & Seto, 2020). Game-based and puzzle-based applied and interactive learning environments could be implemented to minimize challenges of security threats. For example, Jin et al. (2018) implemented a game-based learning method, Cyber Defense Tower Game, for high school students' cyber security education. Students engaged in playing a game, using defensive practice to

prevent their virtual computer server from succumbing to waves of cyber attacks. Jin et al. (2018) noted that this learning method would attract the future cyber security workforce by inspiring high school students interested in college-level cyber security education. Chen et al. (2020) supported this course of action, concluding that game design cyber security practices strongly promote self-efficacy and response efficacy. This, in turn, enhances a more secure environment than nongame-related efforts.

Understanding gaming requires understanding graphs. A graph is a set of vertices connected with edges. It is possible to analyze network traffic by constructing a graph representation. Furthermore, with sufficient training, graphs make it possible to identify potential suspects or victims and pieces of evidence. Graph theory is a well-known mathematical method to evaluate relationships among components of social networks. It can also be applied to create relevant mathematical models of investigation (Easttom, 2017). Recent computer network technologies are interconnected worldwide. This network is represented by a graphic structure. For example, computer hardware like routers and Internet infrastructures can represent multiple nodes. The connections among nodes can be represented by the edges. Graph-based simulation models can be applied to determine the different points of attack (Dawood, 2014).

Li et al.'s (2019) graphical evolutionary game model has demonstrated how viruses are propagated on the cyber network of a power system. A simulation algorithm is also proposed to estimate the infection probability. Then, the cyber security risk is evaluated to measure the security level. Wang et al. (2016) formulated a dynamic game model with a game tree. In this model, the defenders create complete preventive strategies for the sequential actions created by the attractors. The model was validated using case studies.

An attack graph is an application of graph theory in cyber security. This study provides the vulnerability graph model associated with the attack graph. Eventually, in the process of finding a global path search, the optimal attack path is determined (Wang et al., 2018). Understanding a cyber attack is a challenge. Therefore, more effective techniques are needed to minimize this challenge. It was found that the attack modeling techniques (AMTs) and attack graphs method are more effective for visualizing and comprehending the sequence of events that generate a cyber attack (Lallie et al., 2017).

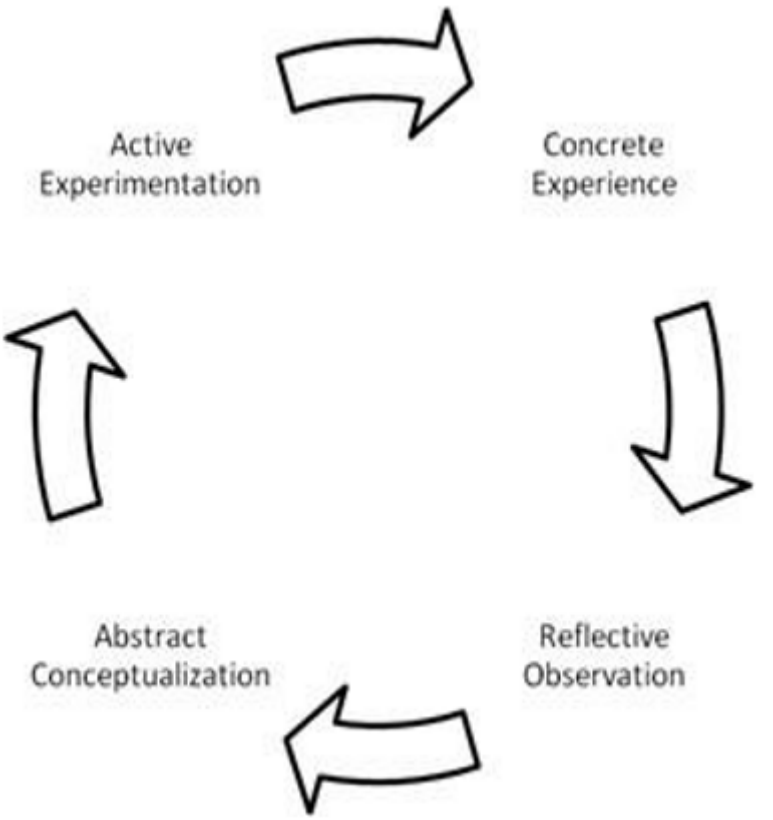
A graph-based analysis enables the visualization of complex problem structures and graph-based methods are used in solving complex cyber security problems (Bi et al., 2017). Given ransomware's popularity, Rosli et al. (2020) investigated and proposed an approach associated with graph theory. In this approach, the ransomware behaviors are analyzed and visualized in a graph-based pattern via Neo4j, a graph database tool. It is possible to recognize the type of ransomware and most impactful graph base node during the analysis (Rosli et al., 2020). Ding et al. (2018) implemented the graph-based method to detect malware, particularly the behavior matching algorithm of the maximum weight subgraph. Their experimental results showed that the proposed graph-based method was highly effective to detect malware variants.

Graph theory tools like incidence matrix, adjacency matrix, and degree matrix can be used to understand the nature of cyber attacks. An incident matrix represents the row for each vertex and a column for each edge. The adjacency matrix provides information about whether the pair of vertices are adjacent. The degree matrix gives information on how the multiple vertices are connected. When modeling the computer network, for example, different routers represent the vertices. The connectivities can represent the edges. In a graph of a computer virus outbreak, it is important to measure the level of connectivity between routers. This can represent the number of file uploads or downloads. Connecting the information on cyber attacks to these matrices provides an efficient way to understand the actual nature of the attack. The higher the degree, the stronger the connection. Another way to model cyber attacks is to determine the radius, the minimum vertex eccentricities, the diameter, and the maximum vertex eccentricities. The rate of change of diameter gives the rate of virus spread. It is effectively described by using differential equation modeling (Easttom, 2020).

Experiential Learning and Deep Learning for Cyber Security Education

The fundamental premise for knowledge acquisition in a learner is through direct experience emanating from experimentation. This perspective also promotes engagement and focus. Kolb (2007) propounded the experiential learning theory, claiming that learning follows a continuous cycle marked by four distinct stages: (1) concrete experience; (2) reflective observation; (3) abstract conceptualization; and (4) active experimentation. This, again, feeds into a substantial experience.

Figure 2. Experiential learning model (adapted from Kolb, CMR, 1976)



As shown in Figure 2, the four stages yield twin sets of parameters, which results in two dimensions. The first dimension encompasses the conceptual foundations of a proactive agent. It builds on past concrete experiences to come up with abstract conceptualization. This is termed the "solution formulation stage." The second dimension comprises the reflective behavior, ranging from active experimentation to reflective observation. Learning occurs as a learner interchanges these roles, getting more and more engaged in solving the problem.

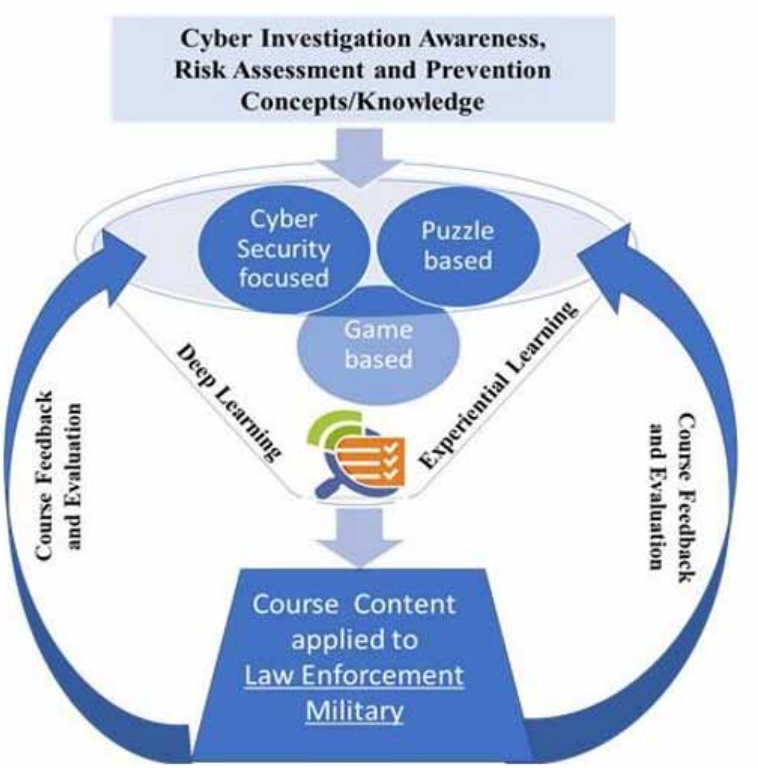
Sendall et al. (2019) emphasized the following conclusions in their review of experiential learning theory and practice within the technology fields. The learner must be actively engaged in and contribute to the learning process in which the experiential activity is directly related to the curriculum outcomes and assessment. The instructor must provide appropriate feedback, allowing the learner to reflect on the experience. As is the case with all learning environments, subsequent activities are built on prior experiences. The knowledge acquisition is cumulative and successful.

This type of learning is greatly enhanced in an adaptive and gamified content environment. These recommendations reflect a recognition that learning is guided by the following dominant paradigms: behaviorism and cognitivism.

Behaviorism, based on Skinner's operant conditioning, ignores the internal mechanisms and states of mind central to cognitivism (to enable and facilitate learning). Both perspectives are relevant for law enforcement personnel because most of their duties involve hands-on, active engagement. For both groups, cyber security investigation is a hands-on activity for which action learning provides a useful framework (Kishen & Ramiro Sweeney, 2015; Pedler, 2011). Action learning is most suitable for adults because it does not emanate strictly from teaching. Rather, it is tackling problems and questioning one's approach (and those of others), thereby building the capability to tackle more complex future problems. Double loop learning occurs when actions and reflection work in tandem to solve complex problems (Nerur & Balijepally, 2007).

The experiential learning process facilitates double loop learning. Both action and reflection are essential components. Deep learning (a nonmachine learning technique in the field of education) takes the concept further, involving the understanding of complex ideas, interpreting the ideas based on prior experiences, integrating the ideas with the existing knowledge base, and applying the newly acquired knowledge in novel scenarios. Formative assessment, a technique for deep learning, focuses on in-process assessment (Rushton, 2005). Continuous testing and integrating learning from testing in developing new strategies is an effective approach to building superior solutions (Bhadauria et al., 2020). Given that adult dispersed workforce learners are likely to have significant prior experience, contextualizing the new knowledge is facilitated by direct feedback. Engagement is fostered through the gamification of course modules.

Figure 3. Focus of this conceptual work



PROPOSED FRAMEWORK

Figure 3 illustrates the overarching guidance framework, depicting the proposed adult-focused pedagogy for imparting cyber security training modules to law enforcement and military workforces in dispersed locations. The focus of the training includes general information about cyber security concepts and specific knowledge about cyber investigation, risk assessment, and prevention. Interwoven into the fabric of the training will be puzzle and game-based experiences, along with deep learning to facilitate the training for the intended workforce. Feedback from the participants is essential to the effectiveness of the training. The feedback can improve course content when used in conjunction with the developer's evaluation of the course material. The course modules will periodically be revised based on further feedback and new cyber threats.

Law enforcement and military personnel fall under the dispersed workforce. Hence, properly aligned hands-on exercises and training related to duties are critical for their learning. In this proposed framework (shown in Figure 3), the topics are selected based on a user survey of military and law enforcement officers. The inclusion of deep learning and experiential learning-based curriculum will significantly enhance their knowledge of the topics and prepare them to become cyber aware as they protect citizens across the world. A sample scenario of encryption technique implementation is highlighted.

A 3D gaming platform is designed to practice the concept of Caesar cipher. The puzzle-based learning paradigm allows users to interact with predefined simulated environments and provide responses to the challenges. Depending on responses, future scenarios will be presented to augment users' learning concepts and existing difficulty levels. If users complete the first two challenges, they will be provided with a hard scenario (final assessment). The overall score will be higher compared to a scenario where a participant does not provide the correct answer in the first two challenges.

CONCLUSION AND FUTURE WORK

This article focuses on existing cyber security and cyber investigation-related topics for military and law enforcement officers. There have been a significant number of cyber security-related incidents in the last decade. Therefore, it is vital to revamp the existing cyber security curriculum, making it relevant to specific segments of the workforce. Integration of adult learning pedagogy with game-based concept design will provide a deep learning-focused environment.

Owing to the nature of the work schedules of the indispensable workforce, the course content should be delivered via an online platform. This availability ensures that all members of the indispensable workforce can strengthen their cyber security and cyber investigation knowledge base and apply the new skills in their career.

A comprehensive user study is planned to capture the interest surrounding various topics from military, law enforcement, and border patrol officials. In addition, future studies will implement multiple course modules on puzzle-based and deep learning concepts (per feedback from the study).

ACKNOWLEDGMENT

This research is supported by the 2019 Texas A&M Engineering Experiment Station (TEES) Annual Research Conference Award. The opinions suggested in this article are the authors; they do not necessarily represent the official views of the TEES.

REFERENCES

Arney, C., Vanatta, N., & Nelson, T. (2016). Cyber education via mathematical education. *The Cyber Defense Review*, *1*(2), 49–60.

Bhadauria, V. S., Mahapatra, R. K., & Nerur, S. P. (2020). Performance outcomes of test-driven development: An experimental investigation. *Journal of the Association for Information Systems*, *21*(4), 2. doi:10.17705/1jais.00628

Bhardwaj, A. (2017). Ransomware: A rising threat of new age digital extortion. In Online banking security measures and data protection (pp. 189-221). IGI Global. doi:10.4018/978-1-5225-0864-9.ch012

Bi, S., Jun, Y., & Zhang, A. (2017). Graph-based cyber security analysis of state estimation in smart power grid. *IEEE Communications Magazine*, *55*(4), 176–183. doi:10.1109/MCOM.2017.1600210C

Bozkurt, A., & Durak, G. (2018). A systematic review of gamification research: In pursuit of homo ludens. *International Journal of Game-Based Learning*, *8*(3), 15–33. doi:10.4018/IJGBL.2018070102

Burning Glass. (2014). *Job market intelligence: Report on the growth of cyber security jobs.* https://www.americanbar.org/content/dam/aba/administrative/law_national_security/WebPage.pdf

Caulkins, B. D. (2016). Cyber workforce development using a behavioral cybersecurity paradigm. 2016 International Conference on Cyber Conflict (CyCon US) (pp. 1–6). IEEE. doi:10.1109/CYCONUS.2016.7836614

Chen, T. (2020). Hacked time: Design and evaluation of a self-efficacy-based cybersecurity game. *Proceedings of the 2020 ACM Designing Interactive Systems Conference*, 1737–1749. doi:10.1145/3357236.3395522

Cook, S. (2022, July 3). Malware statistics and facts for 2022. *Comparitech*. https://www.comparitech.com/antivirus/malware-statistics-facts/

Coull, N. (2016). On the use of serious games technology to facilitate large-scale training in cybercrime response. *European Police Science and Research Bulletin, 3*, 123.

Cukier, M. (2007). *Study: Hackers attack every 39 seconds*. University of Maryland.

Dawood, H. A. (2014). Graph theory and cybersecurity. In *3rd International Conference on Advanced Computer Science Applications and Technologies* (pp. 90–96). IEEE.

Ding, Y., Xia, X., Chen, S., & Li, Y. (2018). A malware detection method based on family behavior graph. *Computers & Security*, *73*, 73–86. doi:10.1016/j.cose.2017.10.007

DoD. (2018). *Department of Defense Cyber Strategy*. https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF

Easttom, C. (2017). Applying graph theory to modeling investigations. *IOSR Journal of Mathematics*, *13*(2), 47–51. doi:10.9790/5728-1302054751

Easttom, C. (2020). On the application of algebraic graph theory to modeling network intrusions. In *10th Annual Computing and Communication Workshop and Conference (CCWC)* (pp. 424–430). IEEE. doi:10.1109/CCWC47524.2020.9031224

FIAL. (2018). *Sector competitiveness plan: Food and agribusiness growth sector.* Food Innovation Australia Limited. https://www.voced.edu.au/content/ngv%3A81579

Georgiev, D. (2022). *Internet of Things statistics, facts & predictions*. https:// review42.com/resources/internet-of-things-stats/

Hijji, M., & Alam, G. (2021). A multivocal literature review on growing social engineering based cyber-attacks/threats during the COVID-19 pandemic: Challenges and prospective solutions. *IEEE Access: Practical Innovations, Open Solutions*, *9*, 7152–7169. doi:10.1109/ACCESS.2020.3048839 PMID:34786300

Humayun, M., Niazi, M., Jhanjhi, N. Z., Alshayeb, M., & Mahmood, S. (2020). Cyber security threats and vulnerabilities: A systematic mapping study. *Arabian Journal for Science and Engineering*, *45*(4), 3171–3189. doi:10.1007/s13369-019-04319-2

Ibanez, M., Di-Serio, A., & Delgado-Kloos, C. (2014). Gamification for engaging computer science students in learning activities: A case study. *IEEE Transactions on Learning Technologies*, *7*(3), 291–301. doi:10.1109/TLT.2014.2329293

Jin, G., Tu, M., Kim, T.-H., Heffron, J., & White, J. (2018). Evaluation of game-based learning in cybersecurity education for high school students. *Journal of Education and Learning*, *12*(1), 150–158. doi:10.11591/edulearn.v12i1.7736

Khan, N. A., Brohi, S. N., & Zaman, N. (2020). *Ten deadly cyber security threats amid COVID-19 pandemic.* https://www.techrxiv.org/articles/preprint/Ten_Deadly_Cyber_Security_Threats_Amid_COVID-19_Pandemic/12278792

Kishen, J. R., & Ramiro Sweeney, R. (2015). Information technology use as a learning mechanism. *Management Information Systems Quarterly*, *39*(3), 615–642. doi:10.25300/MISQ/2015/39.3.05

Kolb, D. A. (2007). *The Kolb learning style inventory*. Hay Resources Direct.

Krasznay, C., & Ha'mornik, B. P. (2019). Human factors approach to cybersecurity teamwork: The military perspective. *Advances in Military Technology*, *14*(2), 291–305. doi:10.3849/aimt.01296

Lallie, H. S., Debattista, K., & Bal, K. (2017). An empirical evaluation of the effectiveness of attack graphs and fault trees in cyber-attack perception. *IEEE Transactions on Information Forensics and Security*, *13*(5), 1110–1122. doi:10.1109/TIFS.2017.2771238

Li, B., Chen, Y., Huang, S., Yao, R., Xia, Y., & Mei, S. (2019). Graphical evolutionary game model of virus-based intrusion to power system for long-term cyber-security risk evaluation. *IEEE Access: Practical Innovations, Open Solutions*, *7*, 178605–178617. doi:10.1109/ACCESS.2019.2958856

Meehan, E. (n.d.). Cybersecurity – An emerging challenge for all law enforcement. *Police Chief Magazine*. https://www.policechiefmagazine.org/cybersecurity-an-emerging-challenge-for-all-law-enforcement/

Morgan, S. (2020). Cybercrime to cost the world 10.5 trillion annually by 2025. *Cybercrime Magazine, 13*. https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

Nerur, S., & Balijepally, V. G. (2007). Theoretical reflections on agile development methodologies. *Communications of the ACM*, *50*(3), 79–83. doi:10.1145/1226736.1226739

Osˇlejsˇek, R. (2020). Conceptual model of visual analytics for hands-on cybersecurity training. *IEEE Transactions on Visualization and Computer Graphics*, *27*(8), 3425–3437. PMID:32142443

Pedler, M. (2011). *Action learning in practice*. Gower Publishing, Ltd.

Rosli, M. S. (2020). Ransomware behavior attack construction via graph theory approach. *International Journal of Advanced Computer Science and Applications*, *11*(2). Advance online publication. doi:10.14569/IJACSA.2020.0110262

Rushton, A. (2005). Formative assessment: A key to deep learning? *Medical Teacher*, *27*(6), 509–513. doi:10.1080/01421590500129159 PMID:16199357

Saha, H. N., Mandal, A., & Sinha, A. (2017). Recent trends in the Internet of Things. In *IEEE 7th annual computing and communication workshop and conference (CCWC)* (pp. 1–4). IEEE.

Schjølberg, S., & Ghernaouti-He'lie, S. (2009). *A global protocol on cybersecurity and cybercrime.* https://www.cybercrimelaw.net/documents/A_Global_Protocol_on_Cybersecurity_and_Cybercrime.pdf

Scholefield, S., & Shepherd, L. A. (2019). Gamification techniques for raising cyber security awareness. In *International Conference on Human-Computer Interaction* (pp. 191–203). Springer. doi:10.1007/978-3-030-22351-9_13

Sendall, P. (2019). Experiential learning in the technology disciplines. *Proceedings of the EDSIG conference*. http://proc.iscap.info/2019/pdf/4968.pdf

Sganga, N., Legare, R., & Pegues, J. (2021, October). *U.S. seizes over* 6 *million from ransomware attacks*. https://www. cbsnews.com/news/ransomware-attacks-united-states-6-million/

Shin, S., & Seto, Y. (2020). Development of IoT security exercise contents for cybersecurity exercise system. In *13th International Conference on Human System Interaction (his)* (pp. 1–6). IEEE.

Sobiesk, E. (2015). Cyber education: A multi-level, multi-discipline approach. In *Proceedings of the 16th annual conference on information technology education* (pp. 43–47). doi:10.1145/2808006.2808038

Tikk-Ringas, E., Kerttunen, M., & Spirito, C. (2014). Cyber security as a field of military education and study. *JFQ: Joint Force Quarterly*, *75*, 57–60.

Treiblmaier, H., Putz, L., & Lowry, P. B. (2018). Setting a definition, context, and theory-based research agenda for the gamification of non-gaming applications. *Association for Information Systems Transactions on Human-Computer Interaction*, *10*(3), 129–163. doi:10.17705/1thci.00107

Tsado, L., & Osgood, R. (2022). *Exploring careers in cybersecurity and digital forensics*. Rowman & Littlefield.

Vogel, R. (2016). Closing the cybersecurity skills gap. *Salus Journal*, *4*(2), 32–46.

Wang, C., Hou, Y., & Ten, C. (2016). Determination of Nash equilibrium based on plausible attack- defense dynamics. *IEEE Transactions on Power Systems*, *32*(5), 3670–3680. doi:10.1109/TPWRS.2016.2635156

Wang, H., Chen, Z., Zhao, J., Di, X., & Liu, D. (2018). A vulnerability assessment method in industrial internet of things based on attack graph and maximum flow. *IEEE Access: Practical Innovations, Open Solutions*, *6*, 8599–8609. doi:10.1109/ACCESS.2018.2805690

Zides, M. (2021, May 12). *Why implement gamification into your cybersecurity training?* eLearning Industry. https://elearningindustry.com/why-implement-gamification-into-cybersecurity-training

Abhijit Kumar Nag is an assistant professor in Computer Information Systems department at Texas A&M University-Central Texas since 2017. He obtained his Ph.D. in Computer Science from the University of Memphis. Previously he received his master's in Computer Engineering from the University of Memphis. His primary research interest includes various authentication approaches, mainly continuous authentication and multi-factor authentication systems. His other research interests include evolutionary algorithms, internet of things, cloud computing, bio-inspired/nature-inspired computing, and big data. He is an inventor of a utility patent on Adaptive Multi-factor Authentication system. He is a co-author of a graduate-level textbook- Advances in User Authentication. Dr. Nag serves as a reviewer for many reputable peer-reviewed journals and conferences. Dr. Nag provided a tutorial talk on Computational Intelligence in User Identity Management in IEEE SSCI conference in 2017. He recently received a TEES grant as a lead PI for the project titled "Powering up: Cybersecurity Education for a Dispersed Workforce."

Vikram S. Bhadauria is an assistant professor of MIS at Texas A&M University in Texarkana, Texas. He received his PhD in information systems from the University of Texas at Arlington. His current research interests include IT4D, sustainability, security, blockchain, IoT, and self-driving technology adoption. His research publications appear in Journal of the Association for Information Systems, Journal of Database Management, Computers in Human Behavior, Industrial Management & Data Systems, Journal of Emerging Technologies in Accounting, International Journal of Productivity and Quality Management, Management Research Review, Supply Chain Management: An International Journal, and other journals. He has also presented papers at several international conferences.

Camille Gibson, Ph.D., C.R.C., is the Interim Dean of the College of Juvenile at Prairie View A&M University and Executive Director of the Texas Juvenile Crime Prevention Center. She began in higher education teaching at Brooklyn College in Political Science, and concurrently at John Jay College of Criminal Justice in Public Administration. Thereafter, she has served at Prairie View A&M University. Her research focus includes cybercrime and youth engagement with social media. Her professional memberships include the American Society of Criminology and the Academy of Criminal Justice Sciences (previously with elected Board service). She is a past President of the Southwestern Association of Criminal Justice in which capacity she represented many criminal justice educators in Texas, Oklahoma, Arizona, Arkansas, New Mexico, and Colorado. She is also a recipient of the esteemed Felix Fabian Award and the Niederhoffer Memorial Fellowship.

Ram Neupane received a Ph.D. degree in applied mathematics from Utah State University, Utah, USA in 2016. Dr. Neupane has more than 15 years of teaching experience in the area of Mathematics in a multicultural environment. He is currently an assistant professor of mathematics at Texas A&M University-Texarkana. His research interest includes Mathematical modeling, Mathematical ecology; biology, and applied mathematics. Recently, he is interested to investigate the mathematical modeling perspective in the field of cybersecurity.

Daniel Creider is an Associate Professor in the Department of Computer Science and Information Systems at Texas A&M University-Commerce. He has been teaching in the CS department since 1978 and has taught graduate and undergraduate courses and served as the coordinator for the Master's program for more than ten years. Dr. Creider received a PhD in Experimental Psychology from Baylor University and a second Masters in Computer Science from East Texas State University now A&M-Commerce. During his time at TAMUC he has been the thesis chair for 20 students and has served on many dissertation committees in other departments. His main areas of interest in the field of computer science are programming efficiency, data structures, and big data.