# Cyber Game-Based Learning for DoD CEs

**Jillian Valente and Mark Reith**
Air Force Institute of Technology, Wright-Patterson AFB, USA

jillian.valente.1@au.af.edu
mark.reith.3@au.af.edu

**Abstract:** Cyber competition and conflict remain an enduring concern for the Department of Defense (DoD). Positive control of cyberspace is crucial across the vast diversity of military operations and supporting activities. People play an important role in cyber prevention, detection, and remediation, but they receive relatively little training outside of the annual Cyber Awareness Challenge. While this gamified training is a reasonable baseline, it primarily addresses cybersecurity from the office worker's perspective. Other career fields within the DoD may benefit from specialized training in cybersecurity, in particular the civil engineering (CE) community supporting critical infrastructure protection. This paper surveys a range of contemporary cyber serious games and assesses each for potential inclusion into CE training. Furthermore, it suggests game elements and characteristics that are likely to benefit the CE community.

**Keywords:** Cyber, Game-Based Learning, DoD, Cyber Learning, Learning Objectives, Bloom's Taxonomy

## 1. Introduction

Cyber is critical in today's warfighting domain. Due to its low barrier of entry, it has leveled the playing field between the U.S. and its adversaries. Today, everything from personal addresses, social security numbers, and banking information to the military's intelligence operations, planning, and communication systems are all stored virtually. If an international conflict were to occur, a breach of data could be a contributing factor between success and failure. Due to its importance for maintaining global security, members of the Department of Defense (DoD) must be prepared to defend and respond in this dynamic battlespace. This requires service members to have a strong foundation of cyber skills.

Many methods are available for DoD members to advance their knowledge in cyber. One such way is the Cyber Awareness Challenge taken by all DoD members. This is important because cyber vulnerabilities are often exploited on the cyber-persona layer since human error is often the greatest weakness of cyberspace (USAF, 2023*)*. Another example are the techniques used to teach cyber operators. They use mainly classroom-based discussions and exercises in virtual environments (Galbraith, 2019). Benefits arise from these tactics, yet superior methods exist that can offer more thought-provoking and memorable ways to learn. Serious games offer a promising avenue for enhancing the cyber learning experience for DoD members by engaging them in interactive environments that promote active learning, critical thinking, and skill development. This will ultimately contribute to the readiness and effectiveness of the armed forces in the realm of cybersecurity. The paper focuses on a particular military career field: civil engineering (CE) students at the Air Force Institute of Technology (AFIT) at Wright Patterson AFB. All CE professionals in the Air Force, prior to achieving the rank of Technical Sergeant, must attend the Advanced Control Systems Cybersecurity (WENG 270) program. It is a four-day, thirty-two credit hour course. Topics included in the syllabus are risk management, malicious logic, and basic networking cybersecurity principles (Kulesza, 2023). The course themes are mapped to key domains of Security+ and Certified Information System Security Professional (CISSP) certifications. The curriculum focuses on operational technology (OT) devices such as programmable logic controllers (PLCs), heating, ventilation, and air conditioning (HVAC) systems, and waste management.

OT is an increasingly relevant domain within cybersecurity. Vault Typhoon is the recent surge of malicious activities associated with the People's Republic of China on U.S. critical infrastructure (CISA, 2023). A primary tactic used by the actor is the living off the land (LOTL) attack. It allows the actor to blend in with the system operations to evade detection (CISA, 2023). Vault Typhoon is one of many instances of U.S. critical infrastructure attacks. It demonstrates the urgent need of OT educated workers in the DoD to recognize and defend against these attacks.

This paper merges a variety of survey, hypothesis, and design of experiment papers to answer the following research question:

RQ: What learning concepts are currently represented in modern cyber serious games?

The contribution of this paper is the proposition of using cyber serious games focused on OT devices in the DoD. The paper is organized as follows: Section 2 discusses background research and defines learning and serious

games. Section 3 describes different types of serious games used in the DoD. Section 4 proposes a cyber learning game that incorporates OT devices that would be beneficial for DoD CE students. Section 5 concludes the paper and provides information for further research.

## 2. Background

Cyber knowledge is important to the DoD's ability to function not only in the warfighting domain but also in routine operations. Millions of emails are sent over the DoD network each day, displaying the importance of communication. Cyber is also used to maintain and upgrade the software of everything from fighter jets and satellites to myPay and LeaveWeb. For this reason, DoD members need to be educated on how to prevent the exploitation of these systems. The following subsections will introduce the concepts of learning and serious games, and how these are the basis for increasing cyber learning among DoD members.

### 2.1 Learning

The rapid onset of technology has not changed the human ability to process information, but it can be used to aid and accelerate the learning process. One of the theoretical perspectives for human learning is cognitivism. This theory considers the different types of memory and how information is encoded into the brain. The three types of memory are sensory, working, and long-term. For working memory to be transferred into long-term memory, it needs to be encoded through visual, auditory, verbal, semantic, or episodic cues (Craig, 2020). The cognitive load theory (CLT) is another key concept in cognitivism. It theorizes that an overload of sensory stimuli can inhibit memory retention in the cognitive system (Craig, 2020). This is important to consider when creating a game framework to ensure that there are not unnecessary components that overload the brain and reduce the learning effect. Learning cyber through the usage of serious games requires a level of self-regulated learning (SRL) (Craig, 2020). Even though it may be mandated as part of a curriculum for DoD members, it takes time to learn the game's structure, rules, and to develop a strategy. SRL is shown to improve learning outcomes, making it another benefit of using serious games as a platform for achieving cyber learning objectives (Craig, 2020). The usage of cyber games within the DoD is meant to be a supplement to the education program, not a replacement. This level of technology implementation is known as augmentation. Its purpose is to improve current learning methods (Craig, 2020).

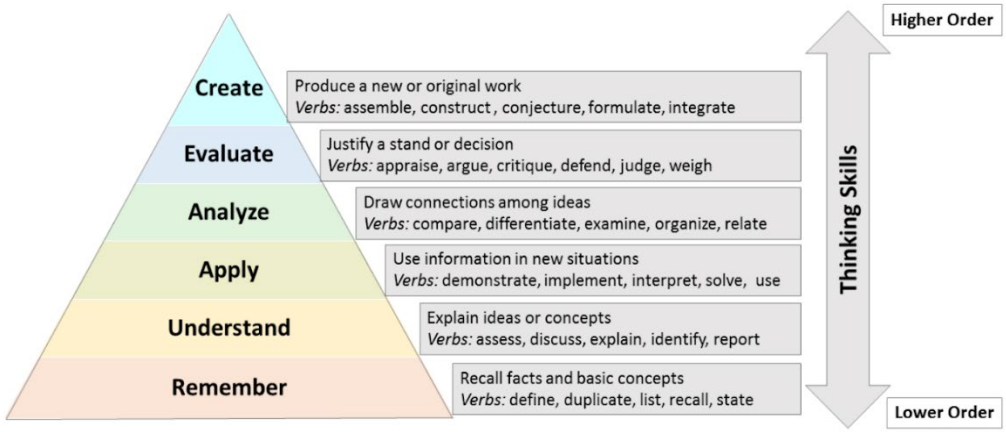


**Figure 1: Revised Bloom's Taxonomy of Learning (Ruhl, 2022*)***

Bloom's Taxonomy of Learning is a model used to categorize learning objectives in increasing complexity. The creator of the model, Benjamin Bloom, discovered during his research that learning is best achieved through a variety of teaching methods and individualized plans (Ruhl, 2022*)*. Using serious games as a learning mechanism diversifies the learning experience and may satisfy many of the hierarchy levels.

### 2.2 Serious Games

Serious games are developed primarily for educational purposes but are also meant to be an enjoyable and engaging method of learning. The literature suggests that this type of learning is beneficial for long-term knowledge retention as opposed to traditional learning (Flack, 2020). This is likely due to the memorable situations that the player encounters. Games utilizing the serious game framework can develop military

members' skills for a particular subject (Flack, 2020). The mission impact of replacing these games in the training pipeline is that it will better equip the DoD to respond to cyber conflicts.

## 3. Serious Games for Teaching Cyber Concepts

Many serious games are currently employed to teach cyber skills. Studies show that scenario-based games with clear learning objectives are the most beneficial for long-term learning retention (Hendrix, 2016) (Yamin, 2021). A learning gap of OT devices that satisfy the needs of WENG 270 have been identified within these games. The curriculum focuses on programmable logic controllers (PLCs), heating, ventilation, and air conditioning (HVAC) systems, and waste management. Addressing deficiencies is critical in order to best equip the DoD's CEs with the correct cyber resources. The next section describes a variety of serious games that could be used in the CE curriculum. The research method for inclusion of these cyber serious games is all games that teach cyber concepts at a high school to masters-level education, have been found using the IEEE, ACM, or recommended by a DoD research partner, and could potentially fit the requirements and time constraints for a classroom-based learning environment.

### 3.1 Cyber Serious Games

Battlespace Next (BSN) is a serious game developed to teach wargaming based on objectives valued by the U.S. military. The game contains multi-domain operations that challenge the player to perform within different realms of warfighting (Flack, 2020). Within the cyber domain, it contains themes of attack and defense. It uses learning objectives aligned with Bloom's Taxonomy of Learning to show that all educational standards can be met through this game (Flack, 2020). A cyber serious game must have learning objectives that match the DoD cyber strategy and cyber operation goals. These objectives can also be used to convince senior leadership that the game is worth military resources and time. BSN was evaluated based on a series of survey and open-response questions. The results of the game played by students within an educational environment were largely positive. Most players enjoyed the game and believed that it increased their knowledge of military strategy and concepts (Flack, 2020). Flack was concerned that BSN would be too complicated, but player feedback suggested that it was acceptable. Games with a high learning curve could be a cause of concern when implementing a cyber serious game and should be considered in terms of time commitment and alignment to the WENG 270 curriculum.

Cyber Protect is another serious game used to teach cyber concepts. The premise of the game is for players to create a secure local area network that can withstand randomly generated attacks. Each attack affects a different level or aspect of the network infrastructure. The player is assessed quarterly based on whether the attack was able to penetrate the network (Carney, 2010). It teaches the player about different types of attacks that can occur on a network, what security features can prevent attacks, and the potential motivations behind attacks. The game also gives advice after an attack has occurred to help the player recover their systems. The limitations of the game is that it only teaches IT concepts and does not consider OT devices.

Cyber Threat Defender is a multiplayer physical and virtual card game that teaches students about cybersecurity information and defense strategies. The deck contains four types of cards: Assets, Defense, Event, and Attack. It develops students' cyber terminology and contains important topics such as network infrastructure and cyber attack and defense relationships. The winner is determined by the player that has the best strategy for protecting the network against their opponent (CIAS, 2016).

The U.S. Cyber Games is a yearly capture the flag event (CTF) open to everyone. It includes activities involving cryptography, forensics, reverse engineering, binary exploitation, and exploiting web-based applications. Based on scores, select players are invited to participate in the U.S. Cyber Combine. This experience has virtual learning opportunities, exercises, and competitions during a 2-month time frame. Then, players are drafted by coaches and prepare for the International Cybersecurity Championship via scrimmaging and training camps. This game provides many real-world opportunities for the player to gain cyber knowledge and experience (US Cyber Games, 2024).

The National Cyber League is a collegiate cybersecurity competition. It helps students prepare for a career in cyber or computer science. The primary objective is to promote diversity and inclusion in the cyber industry. Students can prepare and test their skills against cyber challenges that are present in the workforce. These include analyzing forensic data, pentesting, and recovering from ransomware attacks (Cyber Skyline, 2024).

The Cybersecurity Leadership TableTop Simulation was created by a SANS instructor and included in multiple SANS courses. Players improve the state of security for an organization. There are time, money, and resource constraints, all of which mimic real world situations. Events within the game can cause delays or even ruin a planned strategic initiative. Players are scored from 1-5 based on how they performed in the round (Kim, 2022).

TryHackMe is a learning environment that develops skills for players pursuing a cyber career. It teaches skills for all levels through a wide range of lesson modules. Players can choose a structured learning path that suits their needs for a specific job or certification. It contains most topics within the cybersecurity realm. Some of these paths include red teaming, defending a network, security engineering, web fundamentals, hardware components, and offensive pentesting (TryHackMe, 2024).

CyberStart is composed of hacking challenges and puzzles that teach cybersecurity skills. It has over 200 simulations for players to choose from. The game allows the player to acquire a toolkit of industry-recognized skills. Experts help expand the players' knowledge through tutorial videos and walkthrough guides in the Field Manual. CyberStart provides a safe environment to hack into networks and websites legally (CyberStart, 2022).

The Cyber Awareness Challenge is an annual DoD required set of online modules used to teach basic cyber skills. It focuses on threat mitigation and vulnerabilities within DoD information systems to create user awareness of potential consequences that their actions may have (DoD Cyber Exchange, 2024). It highlights aspects within cybersecurity such as phishing attacks, malicious email attachments, using proper security measures when dealing with controlled unclassified information (CUI) and personally identifiable information (PII), and attacks that can occur when physical access to a system is achieved. The module content is considered critical for DoD members and is enforced by Congress, the Office of Management and Budget, the Office of the Secretary of Defense, and the Cyber Workforce Advisory Group (DoD Cyber Exchange, 2024).

CyberCIEGE is a computer and network security-focused video game using a similar model as employed in SimCity™ (Naval Postgraduate School, 2024*)*. Players in the virtual world operate and defend a network. They are able to spend virtual money to enhance the networks and protect them against cyber attacks (Naval Postgraduate School, 2024*)*. The game syllabus contains information for each of the cyber modules. The cyber components listed are information assurance and security policies, identification and authentication, access control, network security, system assurance and certification, applied cryptography, and public key infrastructure. It also teaches the user about a variety of cyber attacks such as trap doors, corrupt insiders, Trojan horses, viruses, denial of service, and exploitation of weakly configured systems (Naval Postgraduate School, 2024*)*. The US Navy, the Naval Education and Training Command, and the Office of Naval Research are a few of the DoD organizations that find this game valuable to implement in an educational environment.

The NICE challenge is composed of a narrative-driven scenario, business environment, and a set of technical objectives and deliverables. These components are used to provide a real-world simulated experience for the player. It also provides ample feedback for the educator or employer about the player's readiness for the cyber workforce (NICE Challenge Project, 2019*)*. The narrative-driven scenario is composed of conversations with fictional co-workers to develop the player's understanding of cyber in the workforce and the challenges that may arise. The business environment is a workspace with functional servers, services, workstation, and networks available to the player to use for solving the challenges. Lastly, there is a set of technical objectives and deliverables that the player must complete in order to finish a challenge (NICE Challenge Project, 2019*)*. The challenges consist of activities such as installing security software, altering running configurations, and remediating errors. The objectives within the challenges match the NIST SP 800-181, the NICE Framework, and the National Centers of Academic Excellence in Cybersecurity Knowledge Units (NICE Challenge Project, 2019*)*.

Circadence™ is a cybersecurity environment that provides training for users across multiple disciplines. The platform provides specific modules for users in academia, enterprise, government, and military sectors (Circadence, 2024*)*. The cybersecurity training engages the user through gamified, cyber-range practice labs. The concepts and skills taught in these games include the cyber kill chain, ports and protocols, Linux basics, Windows fundamentals, PowerShell, and Wireshark, as well as red and blue team lab scenarios.

CyberFire™ is an OT-focused course with a combination of lectures and hands-on cyber exercises. It develops user knowledge of industrial control systems and physical protection systems. It provides a baseline of cybersecurity information related to OT devices and how they are implemented into various operational industries. There is also an opportunity to learn about the OT network topology, the consequences of an OT cyberattack, how field controllers are different from typical PCs, and OT reconnaissance techniques (CyberFire,

2024*)*. The problem with this learning platform is that it takes multiple days to complete and must be done while the online lectures are broadcasted.

Thales™ is an OT cyber defense game available online and on mobile devices. The player's objective is to dodge cyber attacks and respond to OT security questions. It reinforces the idea that OT devices are increasingly vulnerable to cyber attacks and the consequences that may arise. The game is played similarly to Temple Run or Subway Surfer - the player's virtual avatar is physically dodging cyber threats. About every 20 seconds, an OT question is presented to the player. If answered correctly, the player will advance to the next level (Thales, 2021*)*.

### 3.2 Game Classification Based on Bloom's Taxonomy of Learning

The cyber serious games have been classified into levels based on Bloom's Taxonomy of Learning. Buchanan has identified game elements that relate to a particular level (Buchanan, 2024). It should be acknowledged that there are multiple methodologies for categorizing serious games using Bloom's Taxonomy of Learning, but this paper uses Buchanan's implementation. Most of the games fall within the lower two levels of Bloom's Taxonomy of Learning: Remember and Understand. Some games can be elevated to the Apply level if post-game questions are added to assess a player's knowledge. Games classified within the Remember level demonstrate skills such as remembering ideas and information. The Understand level requires the player to interpret, discuss, and compare their knowledge. In order for a game to be on the Apply level, it must test the player's ability to solve problems or use skills in difficult situations (Buchanan, 2024).

A modified Bloom's Taxonomy of Learning diagram is shown in Figure 2. It maps each game to an associated level. CyberStart, the Cyber Awareness Challenge, Circadence, CyberFire, and Thales are all on the Remember level. These games are all module-focused that require the user to define and recollect information. The following games have been identified under the Understand level: Battlespace Next, Cyber Protect, Cyber Threat Defender, the Cybersecurity Leadership TableTop Simulation, CyberCIEGE, and the NICE Challenge. The games listed are all simulation-focused; the player must interpret their knowledge in a real-world context. The games that are on the Apply level are the U.S. Cyber Games, National Cyber League, and TryHackMe because the player must demonstrate the ability to solve problems in advanced scenarios.

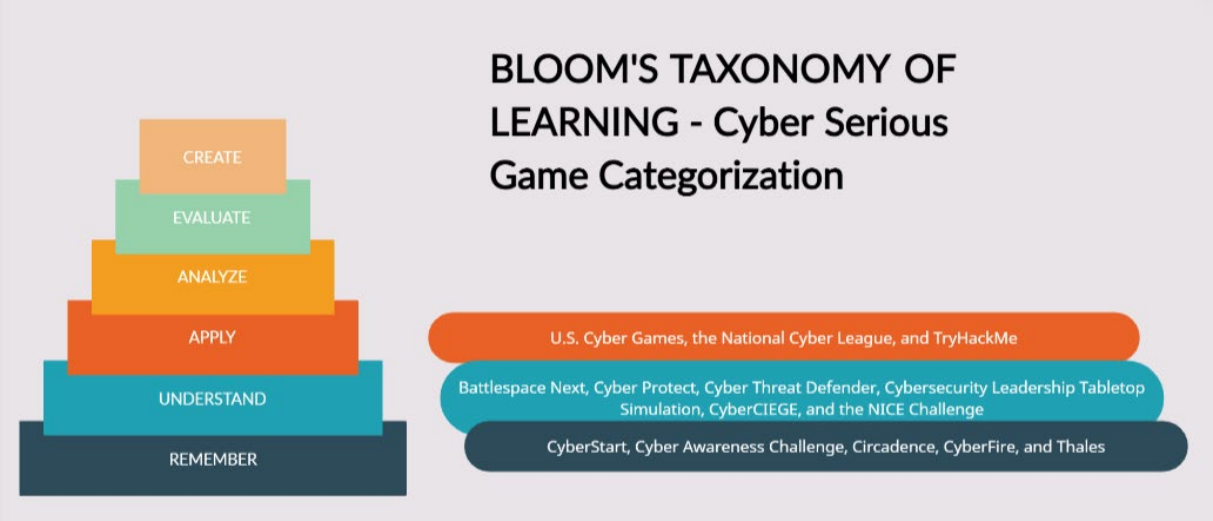


**Figure 2: Bloom's Taxonomy of Learning - Cyber Serious Game Categorization**

The diagram maps the cyber serious games described in Section 3.1 to a corresponding level.

Remember level criteria: Module-focused. Player defines and recollects information.

Understand level criteria: Simulation-focused. Player interprets knowledge in a real-world context.

Apply level criteria: Player demonstrates ability to solve problems in advanced scenarios.

## 4. Propositions to Improve Cyber Game-based Learning

Table 1 shows the different domains of cyber that are demonstrated in the games described in Section 3.1. The sub-disciplines of cyber in the "Domain of Cyber" columns were determined according to Cremer et al. (2022),

Karjalainen et al. (2020), and Maalem et al (2020). A clear absence of OT within most cyber learning games is shown. TryHackMe, the Cyber Awareness Challenge, the NICE Challenge, CyberFire, and Thales are the only games that contain a section of critical infrastructure or hardware modules within cybersecurity. As the dependence on OT increases in the CE career field, these learning modules will not be sufficient. An in-depth assessment of each OT game and its applicability to the WENG 270 curriculum is mentioned in the following paragraphs. It would be beneficial to create a game that teaches about OT devices to fill this gap.

**Table 1: Popular Cyber-learning Games Mapped to Domains within Cybersecurity**

| Cyber Game/Domain of Cyber | Networking/Internet Usage | Cyber Attacks | Defense/ Prevention | Recovery Techniques/ Mitigation | Operational Technology/ Hardware/ Infrastructure | Miscellaneous |
|---|---|---|---|---|---|---|
| Battlespace Next | | ✓ | ✓ | | | -Multi-domain operations |
| Cyber Protect | ✓ | ✓ | ✓ | ✓ | | -Motivation |
| Cyber Threat Defender | ✓ | ✓ | ✓ | | | -Cyber Terminology |
| U.S. Cyber Games | | ✓ | ✓ | ✓ | | |
| National Cyber League | | ✓ | ✓ | ✓ | | |
| Cybersecurity Leadership TableTop Simulation | | | ✓ | | | |
| TryHackMe | ✓ | ✓ | ✓ | ✓ | ✓ | -Linux/Windows fundamentals<br>-Cyber Terminology<br>-Career Paths |
| CyberStart | ✓ | ✓ | | | | |
| The Cyber Awareness Challenge | ✓ | ✓ | | | ✓ | -CUI and PII proper security measures |
| CyberCIEGE | ✓ | ✓ | ✓ | | | |
| NICE Challenge | ✓ | | | | ✓ | |
| Circadence | ✓ | ✓ | ✓ | | | -Cyber Kill Chain<br>-Linux/Windows fundamentals |
| CyberFire | ✓ | ✓ | | | ✓ | |

| Cyber Game/Domain of Cyber | Networking/Internet Usage | Cyber Attacks | Defense/ Prevention | Recovery Techniques/ Mitigation | Operational Technology/ Hardware/ Infrastructure | Miscellaneous |
|---|---|---|---|---|---|---|
| Battlespace Next | | ✓ | ✓ | | | -Multi-domain operations |
| Cyber Protect | ✓ | ✓ | ✓ | ✓ | | -Motivation |
| Cyber Threat Defender | ✓ | ✓ | ✓ | | | -Cyber Terminology |
| U.S. Cyber Games | | ✓ | ✓ | ✓ | | |
| Thales | | | | | ✓ | |

Limited cyber training resources exist on OT devices. This could be due to the fact that, in the past, OT was much more difficult to attack due to air gapping. It is also important to note that OT devices cannot be protected the same way as IT devices due to their design. Today, these OT devices are often connected to the internet, bridging the gap between OT and IT. A classic example of this is the Stuxnet attack from 2010 that was able to degrade Iran's nuclear centrifuges in an air-gapped system (Yang, 2015). It is even simpler to attack OT devices that are connected to the internet. The Vault Typhoon case study mentioned in the Introduction also demonstrates the relevance of OT in modern cyberwarfare.

The proposition to improve game-based learning for the CE students is to increase the usage of OT devices as opposed to information technology (IT) to make a game that is most relevant to their curriculum. The cyber domains consisting of Networking/Internet usage, Cyber Attacks, Defense/Prevention, and Recovery Techniques/Mitigation are all considered IT. TryHackMe is not sufficient for the CE curriculum because it does not have modules for the OT devices prioritized by the course director. The CyberAwareness Challenge is required for all DoD members, so it is already implemented in the CE curriculum. Also, the OT concepts in this challenge are too basic for the knowledge requirements of CEs. There is potential for the NICE challenge to be modified in order to provide the necessary OT components for the CE curriculum, but further testing is needed. CyberFire is not a feasible option as a game that can be implemented into the WENG 270 curriculum due to the time constraints of the course. Thales is focused on OT technology and asks thought-provoking questions to the user, but does not provide any learning material or feedback for incorrect answers. The game format may also be distracting in a classroom environment. Future research in this field will require the alignment of the WENG 270 course learning objectives and the construction of a cyber learning game that utilizes OT devices.

## 5. Conclusion

This paper advocates for the enhancement in cyber training within the DOD, emphasizing the crucial role of OT devices. It defines types of learning, Bloom's Taxonomy of Learning, and serious games. Cyber serious games are described and categorized based on a level according to Bloom's. The paper addresses the research question by recognizing the inadequacy of current serious games in covering OT concepts. A focused approach directed at CE students in the DoD is proposed. By addressing the identified learning gaps and integrating OT devices into cyber learning games, CEs will be more equipped to respond in the dynamic realm of cybersecurity.

## References

Buchanan, L. (2024). Blending Bloom's Taxonomy and Serious Game Design. *Secure Decisions Division*.
Carney. (2010). *CyberProtect – SGS&C*. Retrieved November 1, 2023, from http://sgschallenge.com/cyber-protect/
CIAS. (2016). *Cyber Threat Defender – The UTSA CIAS*. https://cias.utsa.edu/ctd/
Circadence. (2024). *Gamified Cybersecurity Training Solutions*. Circadence Corporation. https://circadence.com/

CISA. (2023, May 24). *People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection | CISA*. https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-144a

Craig, S. D., Schroeder, N. L., & Roscoe, R. D. (2020). Science of Learning and Readiness. *U.S. Advanced Distributed Learning (ADL) Initiative*.

Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F., & Materne, S. (2022). Cyber risk and cybersecurity: A systematic review of data availability. *The Geneva Papers on Risk and Insurance. Issues and Practice*, *47*(3), 698–736. https://doi.org/10.1057/s41288-022-00266-6

CyberFire. (2024). *Cyber Fire Operational Technology*. https://cyberfire.energy.gov/classes/ot/

Cyber Skyline. (2024). *National Cyber League*. https://nationalcyberleague.org/

CyberStart. (2022). *Play fun hacking cyber security games, for free*. https://cyberstart.com/

DoD Cyber Exchange. (2024). *Cyber Awareness Challenge 2024 – DoD Cyber Exchange*. https://public.cyber.mil/training/cyber-awareness-challenge/

Flack, N., Lin, A., Peterson, G., & Reith, M. (2020). Battlespace Next(TM): Developing a Serious Game to Explore Multi-Domain Operations. *International Journal of Serious Games*, *7*(2), Article 2. https://doi.org/10.17083/ijsg.v7i2.349

Galbraith, Jean. U.S. Military Undergoes Restructuring to Emphasize Cyber and Space Capabilities. (2019). *American Journal of International Law*, *113*(3), 634–640. https://doi.org/10.1017/ajil.2019.39

Hendrix, M. (2016). Game based cyber security training: Are serious games suitable for cyber security training? *International Journal of Serious Games*.

Karjalainen, M., & Kokkonen, T. (2020). Comprehensive Cyber Arena; The Next Generation Cyber Range. *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, 11–16. https://doi.org/10.1109/EuroSPW51379.2020.00011

*Kim, Frank. Cyber42 Cybersecurity Leadership Simulation Games | SANS Institute | Cyber Security Leadership.* (2022). https://www.sans.org/blog/cyber42/

Kulesza, N. (2023). *WENG 270 Lesson Objectives*. The Civil Engineer School.

Maalem Lahcen, R. A., Caulkins, B., Mohapatra, R., & Kumar, M. (2020). Review and insight on the behavioral aspects of cybersecurity. *Cybersecurity*, *3*(1), 10. https://doi.org/10.1186/s42400-020-00050-w

Naval Postgraduate School. (2024). *CyberCIEGE - Center for Cybersecurity and Cyber Operations—Naval Postgraduate School*. https://nps.edu/web/c3o/cyberciege

NICE Challenge Project. (2019). *NICE Challenge Project – The Workforce Experience Before the Workforce*. https://nice-challenge.com/

Ruhl, Charlotte. *Bloom's Taxonomy of Learning | Domain Levels Explained*. (2022, November 3). https://www.simplypsychology.org/blooms-taxonomy.html

Thales. (2021). *Launch IT/OT Cyber Defense Game*. https://connect.thalesgroup.com/en/news/lancering-it-ot-cyber-defense-game

TryHackMe. (2024). *TryHackMe | Cyber Security Training.* https://tryhackme.com

USAF. (2023). CYBERSPACE OPERATIONS. *AIR FORCE DOCTRINE PUBLICATION 3-12.*

*US Cyber Games.* (2024). *https://www.uscybergames.com/*

Yamin, M. M., Katt, B., & Nowostawski, M. (2021). Serious games as a tool to model attack and defense scenarios for cyber-security exercises. *Norwegian University of Science and Technology*.

Yang, J., Liu, X., & Bose, S. (2015). Preventing Cyber-induced Irreversible Physical Damage to Cyber-Physical Systems. *Proceedings of the 10th Annual Cyber and Information Security Research Conference*, 1–4. https://doi.org/10.1145/2746266.2746274