A Survey of Learning Technology Integration in Information Warfare Education

Matthew Douglas and Mark Reith
Air Force Institute of Technology, Wright-Patterson AFB, Ohio, United States of America

matthew.douglas@afit.edu
mark.reith@afit.edu

Abstract: Information and communication technologies (ICTs) are enduringly important in today's world. From paying for morning coffee at the local cafe to receiving a text message from a loved one, ICTs are a part of everyday life. On a larger scale, entire nations are dependent on ICTs. From power grids to the storage of classified documents, nations have come to rely on ICTs. This dependence on ICTs has increased information warfare's importance as a warfighting domain. In order to effectively conduct information warfare operations, operators must first be properly trained on how to be successful in this domain. The use of learning technologies could be useful to train information warfare forces. This paper surveys the current state of learning technology integration into information warfare education. Learning technologies have become commonplace in today's professional world. Many topics in organizations are taught through learning technologies such as interactive computer-based trainings, educational videos, and more complex serious games. This is no different for information warfare professionals. Learning technologies can provide alternative ways to teach important information warfare concepts such as the roles, assets, and capabilities that are necessary to succeed in this domain. The use of artificial intelligence, game-based learning, gamification, and simulation-based learning to enhance the training of information warfare forces is discussed in this survey. Additionally, the effect of adding learning technology into information warfare education curriculum as well as the key elements for each type of learning technology integrated are analysed. This paper also identifies areas of future research to further develop this topic. These findings are useful to information warfare educators who are developing curriculum or looking for ways to introduce new technologies into existing curriculum. Artificial intelligence, game-based learning, gamification, and simulation-based learning are all great options to support information warfare education, and there are even more options that have yet to be researched that present further opportunities to study in this area.

Keywords: Information Warfare, Learning Technology

1. Introduction

Information warfare, characterized by the strategic use of information and communication technologies for offensive or defensive actions, has become a critical topic in an era where nations heavily rely on information and communication technologies (ICTs) (Taddeo, 2012). Recognizing the importance of preparing individuals for this domain, the incorporation of learning technologies provides opportunities to more effectively organize, train, and equip information warfare professionals. Learning technologies, a wide array of hardware, rules, and systems, has become an important resource to support the learning process (An & Oliver, 2021). In today's increasingly digital world, the use of technology allows for education to be more interactive and dynamic, therefore increasing engagement from learners. This shift away from more traditional means of education, such as pure lecturing, becomes particularly relevant when applied to complex subjects such as information warfare. Complex topics can be hard to effectively teach solely through lecture-based instruction methods. Learning technologies provide alternate ways of training individuals on such complex topics (An & Oliver, 2021). One potential of utilizing learning technologies in information warfare education is the chance to gain knowledge directly in a simulated environment that resembles the one they will apply their knowledge in later (Plass, Mayer & Homer, 2020). This paper focuses on the intersection of information warfare education and learning technologies, exploring the potential this integration could hold in shaping the future of national security and education.

2. Research Questions

This survey is guided by the following research questions:

(RQ1) How have learning technologies been integrated into information warfare education?

(RQ2) What is the effect of adding learning technologies into information warfare education curriculum?

(RQ3) What are the key elements of successful integration into information warfare education for each type of learning technology?

This paper introduces the concepts of information warfare and learning technology, surveys past and current methods of learning technology integration into information warfare education, analyses the effect of adding learning technologies into information warfare education, and details key elements for each type of learning technology that is surveyed. This paper also identifies key areas for future research. This survey differs from others like it by having a broader scope of learning technology applications (artificial intelligence, game-based learning, gamification, and simulation-based learning) and its focus on literature specifically related to information warfare education.

3. Background

In this section, the topics of information warfare and learning technology are discussed to provide context for this survey. A discussion of how learning technologies are appropriate for use in information warfare education also follows in this section.

3.1 Information warfare

Information warfare is the utilization of ICTs with the intention of either launching offensive or defensive actions to swiftly infiltrate, disrupt, or exert control over an adversary's assets and resources or defend against such attacks (Taddeo, 2012). Figure 1 models this behaviour. Both offensive and defensive intentions have the aim of securing a competitive advantage by leveraging the power of information. This kind of warfare spans multiple professions including cyber and intelligence operations (Williams, 2010). Information warfare has continually grown in importance over the years as nations around the world become increasingly dependent on ICTs (Frater & Ryan, 2001). In today’s ICT-dependent world, it is critical for nations to properly organize, train, and equip information warfare professionals.

The four characteristics that differentiate information warfare from traditional warfare are variance, non-lethality, ambiguity, and persistence (Libicki, 2020). Variance refers to the unpredictability of effects when conducting information warfare. This makes relying on these effects as key parts of operations as unrealistic, but information warfare can be used as supporting effects or multiple information warfare efforts can be executed for a potentially cumulative effect. Non-lethality and ambiguity are massive advantages of information warfare. Effects can be generated in both physical and non-physical domains (Taddeo, 2012), and these effects can be non-lethal and hard to determine who actually caused the effects due to the relative anonymity of ICTs (Libicki, 2020). The last differentiating characteristic of information warfare is persistence, and this refers to the constant connection ICTs provide to nations. A nation is able to constantly generate effects on another nation, no matter where in the world those two nations are, due to their constant connection through ICTs.

3.2 Learning technology

Learning technology, also known as educational technology, is the use of technology to deliver educational experiences to learners (An & Oliver, 2021). This broad field covers a wide range of technologies, which enhance and support the learning process. Technology in this context can be defined as hardware, rules, or systems (Dusek, 2006). This includes, but is not limited to, physical tools and resources, computers, mobile devices, online platforms, and other digital resources. Table 1 provides the different types of learning technology this survey acknowledges (Baek, 2009; College, 2024). While the use of learning technologies does not inherently make education better, it can change how individuals approach it (An & Oliver, 2021). Direct instruction does not allow full comprehension of a topic for everyone, so education can be made interactive and dynamic through learning technologies. This is a step toward integrating knowledge directly into the learner’s world rather than the learner and knowledge remaining independent of one another.

Table 1: A partial list of learning technologies present in education

Learning Technologies	Description
Adaptive Learning Systems	Systems that can provide personalized learning plans and feedback.
Artificial Intelligence and Machine Learning	Intelligent agents that can be used to enhance systems such as e-learning platforms, tutoring systems, and personalized learning experiences.
E-Learning Platforms	Online platforms that host self-paced, interactive e-learning courses.
Game-Based Learning	The use of games to teach educational content through gameplay.
Gamification	The use of game elements, such as points, badges, and leaderboards, to engage and motivate learners.

Learning Technologies	Description
Learning Management Systems	Software that allows for the creation and online delivery of educational content.
Mobile Learning	The use of mobile devices to deliver and access educational content.
Simulation-Based Learning	Virtual learning simulations allow learners to gain experience in scenarios similar to the real world.
Social Learning	The use of platforms such as discussion boards and blogs to support and enhance learning.
Virtual and Augmented Reality	Technologies that simulate the real world or overlay new information onto it to deliver immersive educational content.

A majority of studies in this survey utilized game-based learning. Game-based learning is the use of games to transfer knowledge to learners in an environment comparable to the real-world (Tobias, Fletcher & Wind, 2014). Studies suggest that knowledge learned in this manner can transfer to external tasks and can engage learners more than traditional instruction methods. That is not to say game-based learning should replace direct instruction, rather it should complement and enhance the overall learning experience. This is because game-based learning benefits from a learner already having baseline knowledge of the subject related to the game's learning objectives (Plass, Mayer & Homer, 2020). The other studies found in this survey employed artificial intelligence and simulation-based learning as well as one study for gamification.

3.3 Discussion of how Learning Technologies are Appropriate for use in Information Warfare Education

The four characteristics of information warfare previously discussed, variance, non-lethality, ambiguity, and persistence, present opportunities to utilize learning technologies. Variance is easily conveyed through game-based learning. Rules and systems can be implemented that create randomness in the form of percentage-based chances for actions to successfully take place (Henno, Jaakkola & Mäkelä, 2018). This can be implemented in a physical environment with dice or in a digital environment by generating random numbers. Persistence can be conveyed through game-based learning as well. Real-time strategy games, for example, create constant connectivity by putting players in a shared world in which any player can create effects on any other player and at any time they desire, given they have the means to carry out their plans (Metoyer et al., 2010).

Non-lethality can be conveyed in simulations. A learner could be guided to complete particular actions within a simulation, and then they can be shown the results of those actions (Barjis et al., 2012). Ambiguity can also be conveyed in simulations. A learner could be given a scenario in which a lot of information is unknown, yet a specified task must still be completed and the learner must use critical thinking skills. (Barjis et al., 2012). These examples show how learning technology can be applied to information warfare education in an appropriate and effective manner.

4. Survey of Learning Technologies Integrated Into Information Warfare Education

Table 2 lists the inclusion and exclusion criteria used for this survey. These criteria were chosen due to this paper's specific interest in information warfare and the desire to survey papers no older than the beginning of this century. The majority of papers that were excluded were on the basis of not pertaining to information warfare education.

Table 2: Inclusion and exclusion criteria used in this survey

Inclusion Criteria	Exclusion Criteria
1. Papers with a focus on information warfare education and the use of learning technologies	1. Papers with a focus on operational information warfare units, papers solely on classical methods of instruction, or papers with unrelated topics
2. Papers with the full text available	2. Papers that did not have the full text available
3. Papers written after the year 1999	3. Papers written before the year 2000
4. Papers written in English	4. Papers written in any language besides English

The methodology used to gather papers consisted of keyword searches using “learning technologies”, “educational technologies”, “information warfare”, and “information warfare education”. These keyword searches were conducted through the databases shown in Table 3. A total of 4,238 results were found, but only 14 of the results matched the inclusion criteria of this survey.

Table 3: The results of the database searches that used exclusion criteria 2, 3, and 4 to filter the databases and exclusion criterion 1 was used to exclude papers after reviewing each of them.

Database	Number of Results	Number Selected for Inclusion
Google Scholar	383	9
IEEE Xplore	54	2
JSTOR	1,434	1
Database	**Number of Results**	**Number Selected for Inclusion**
ACM Digital Library	1,623	1
Springer Link	744	1

Table 4 lists the surveyed learning technologies and which studies pertain to them.

Table 4: The information provided includes references of papers that contain pertinent discussion of a specific learning technology (two of the studies are discussed in both the artificial intelligence and game-based learning sections as indicated by *)

Learning Technology	References
Artificial Intelligence	Bowman et al., 2004 Cramer, Ramachandran & Viera, 2004* Ormrod et al., 2020*
Game-Based Learning	Cramer, Ramachandran & Viera, 2004* Doriot, Hutto & Smoak, 2011 Herr & Allen, 2015 Evgenia, Ekaterina & Gennady, 2019 Flack & Lin et al., 2020 Flack & Voltz et al., 2020 Ormrod et al., 2020* Yamin, Katt & Nowostawski, 2021
Gamification	Berisford et al., 2022
Simulation-Based Learning	Davey & Armstrong, 2001 Ragsdale, Lathrop & Dodge, 2003 Schweitzer & Fulton, 2010 Katsantonis et al., 2023

4.1 Artificial Intelligence

Artificial intelligence (AI) is a fast growing field in the modern world. It has the potential to do many things, including enhance education. An example of this is an AI agent used at the United States Army War College (Bowman et al., 2004). An AI agent called “Disciple-RKF” was created to aid in rapid knowledge formation and reasoning in the Information Age. The main use case of the agent was to help military officers identify centres of gravity, but evidence was provided that subject matter experts could teach “Disciple-RKF” agents about any complex military domain, including information warfare. The agents could then be used in a classroom environment to assist the learner in creating a knowledge base while performing educational activities (Bowman et al., 2004). This learning technology allows for the instructor's knowledge to be freely available to learners and allows for more individualised training.

Although not actually implemented, one of the game-based learning studies highlighted the use of AI agents to act as evaluators that can provide immediate feedback as a desired feature that would enrich the overall experience (Cramer, Ramachandran, & Viera, 2004). This could be an effective use of AI as it allows the learner to receive feedback at any time including when an instructor is not present. Another example of AI in one of the game-based learning studies was the utilization of AI agents to create massive amounts of posts on a privately hosted social media site in attempt to realistically generate massive amounts of data (Ormrod et al., 2020). This is an effective use of AI to support information warfare education as it enables instructors to add game elements that would otherwise take large amounts of time to implement into a game.

The effect of artificial intelligence on information warfare education is still fairly unknown. Its ability to act as a virtual tutor and evaluator or to create large amounts of data have potential to ease burdens on educators. A key element of successful integration of artificial intelligence into information warfare education may include teaching AI agents within the proper context of the learning content to avoid the agents providing irrelevant information to the learner.

4.2 Game-Based Learning

Many of the studies found in this survey utilize game-based learning to teach information warfare. This is most likely due to the flexibility that is allowed when designing a game and how effective games are at engaging learners (Plass, Mayer & Homer, 2020). For example, one study created a pre-test for an information warfare education course in the form of a game. This proof of concept computer-based game allowed incoming students to participate in a simulated scenario, and their success or failure would indicated their understanding of the game's learning objectives. This use of game-based learning was decided upon due to its distance learning capabilities as well as the immersion it can provide to learners (Cramer, Ramachandran, & Viera, 2004).

One such study that also sought to be immersive was the design of CyberWar RTS, a cyber real-time strategy training game (Doriot, Hutto, & Smoak, 2011). Real-time strategy games allow learners to think strategically at a high level while still having tactical control over the simulated environment. The game itself consists of a dynamic network diagram that the learner must complete tasks within such as defending ally networks or attacking adversary assets. The goal behind CyberWar RTS was to provide an entertaining educational experience for information warfare education that could be stand-alone or used within the context of a training course (Doriot, Hutto, & Smoak, 2011). A serious real-time strategy game like this is a great example of conveying the persistence of information warfare. The learner must balance both offence and defence due to the constant connectivity with adversaries.

It is important to understand certain elements are necessary for game-based learning to be effective within an information warfare education environment (Herr & Allen, 2015). Realism needs to be maintained, but must be balanced with the learners' engagement level. This applies to complexity as well. The game should be complex enough to relate to its real-world counterpart, but must also be simple enough for learner to understand what they must accomplish. Clear learning objectives are also key for learners to comprehend what they are supposed to master through the game. Recommendations to achieve these elements include achievements, enabling collaboration, and ensuring relevance of the game in relation to its target audience (Herr & Allen, 2015).

One such game that implemented these ideas is Information Security Quest (Evgenia, Ekaterina & Gennady, 2019). In this game, participants were tasked with investigating the theft of a flash drive that contained the usernames and passwords of a fictional bank's clientele. The participants had to work together to complete multiple objectives that included cracking passwords to get information on laptops, using a stenography tool to uncover hidden data, and discovering an encryption key to decrypt a file. The game only covered high-level information security concepts, but it implemented active education methods that future information warfare games could seek to implement as well. The participants were all very engaged during the game with the exception of instructions they were given at the beginning of the game. The instructions were deemed too lengthy by the participants, so this is something other information warfare games should be cognizant not to repeat (Evgenia, Ekaterina & Gennady, 2019).

Two studies that used card games to teach information warfare are Multi-Domain Command and Control Trading Card Game (MDC2 Game) and Battlespace Next™ (Flack et al., 2020). Both of these serious games teach multi-domain operations (MDO), with an emphasis on information warfare. The original game, MDC2 Game, contained a deck building element that allowed for custom strategies, while its successor, Battlespace Next™, removed that element for simpler entry into the game. While Battlespace Next™ added features as well, the core concepts of both games remain the same. The learners utilize cards representing assets from various military domains to defeat their opponent. The data from the studies show that through playing these card games, a majority of the learners felt like their knowledge of MDO increased and that the game was enjoyable (Flack et al., 2020). These two serious games are great examples of the ambiguity that is present in information warfare. A player does not know what cards their opponent has in their hand, but they are expected to complete their objective regardless.

Another study in which learners encountered much ambiguity was a large-scale wargame, referred to as The Persuasion Game, in which information warfare played an extensive part (Ormrod et al., 2020). A fictional world was constructed that contained six nations, five of which consisted of teams of learners. A large part of the world-building included the use of privately hosted social media platforms and online news platforms. Within this environment, the teams of learners had to create multiple concepts of operation to produce strategic, operational, and tactical actions that advanced the goals of their nation. These actions encompassed multiple domains, including information warfare. The findings from this study concluded while there were many improvements to be made, the wargame was successful at achieving its learning objectives (Ormrod et al., 2020). It stands as an effective example of utilizing learning technologies to aid information warfare education.

Some serious games can be customizable such as a study that created a proof of concept cyber attack and defence game (Yamin, Katt, & Nowostawski, 2021). The game allowed for scenarios, either attack or defence, to be built by instructors which could then be played by learners. These scenarios sought to offer both a strategic simulation and a low-level cybersecurity infrastructure experience (Yamin, Katt, & Nowostawski, 2021). Customizable serious game frameworks can be beneficial because then specific scenarios can be produced without having to design a whole new game.

The effect of game-based learning on information warfare education is largely positive from the studies above. Learners were widely reported to be engaged and gaining the intended knowledge. Key elements of successful integration of game-base learning into information warfare education include finding the right balance of gameplay and learning objectives, not overburdening learners with instructions, and providing the appropriate level of complexity as to relate to the real world but be simple enough to learn the mechanics of the game.

4.3 Gamification

Gamification is the use of game elements to increase engagement and motivation in learners. This can be seen in a study that created a gamified learning system that taught three ICT vulnerabilities: broken access control, cryptographic failures, and injection (Berisford et al., 2022). This system was built in the Unity game engine, and consisted of gamified elements such as storylines, experience points, levels, and badges. Learners were asked to analyse code and answer whether or not the code was safe or it if contained a vulnerability. Experience points would be gained for correct answers and lost for incorrect answers. Once enough experience points were gained, learners would increase in level, or promote, which allowed them to access new content. Learners could also be "fired" though if they lost too much experience points. Badges were also earned as positive and negative achievements. The results of this study revealed that the promotion/firing mechanic was the most motivating to learners, and the storylines were the least interesting, although they were still seen as beneficial (Berisford et al., 2022).

The effect of gamification on information warfare education could be increased motivation and engagement. Key elements of successful integration of gamification into information warfare education include experience points and levels as well as negative consequences for consecutive failures.

4.4 Simulation-Based Learning

Simulation-based learning focuses on the creation of real-world scenarios in an educational environment. This can be seen in a study that discusses the creation of custom-designed computer networks, isolated from all outside networks, for the purpose of simulation-based learning (Davey & Armstrong, 2001). A five stage process was introduced in which a learner would start by familiarizing themselves with this custom network and the provided tools. Then, elements would start getting added on such as traffic from another human, two networks divided by routers and firewalls, and pseudo network traffic generated to mimic network activity as if it was connected to the internet. Finally, learners would participate in scenarios that pitted them against other learners and each team was tasked with specific objectives they must complete to win. The benefits of this approach include required planning of how objectives would be achieved, hands-on experience, reflection of actions taken, and collaboration with teammates (Davey & Armstrong, 2001).

A similar approach was taken in a study that created a cyber security laboratory that would allow learners to study offensive and defensive cyber operations (Ragsdale, Lathrop & Dodge, 2003). This laboratory consisted of two main parts: a cyber "firing range" and a network of computers that contained the software VMware on them. The "firing range" was a completely isolated network that allowed for learners to practice with both offensive and defensive tools without risking the release of malicious code outside of the network. The network of computer with VMware on them allowed students to practice being network and server administrators. VMware allowed them to create virtual machines that gave them full configuration control. This network resulted in a laboratory for students to learn about cyber operations that would give them skills they could use in the real world (Ragsdale, Lathrop & Dodge, 2003).

Another study incorporated simulation-based learning into the information warfare program at the United States Air Force Academy (Schweitzer & Fulton, 2010). The motivation for integrating simulation-based learning into this program was based on two challenges that arose from only using a lecture-based approach: the large amount of material to cover and the lack of hands-on training that allows for active engagement with the material. A mix of lecture and simulation-based learning allowed for the students to first develop a common understanding of the subject and then apply their knowledge to interactive exercises. The incorporated simulation-based learning included web labs and a capture the flag (CTF) competition. These labs and CTF competition both used custom networks that allowed students to attack and defend ICTs that were specifically designed for them. The data collected showed that the combined lecture and learning technology approach was far more effective in teaching students the desired material than a solely lecture-based approach (Schweitzer & Fulton, 2010).

The final simulation-based learning paper in this survey discusses how a modern cyber range should be designed. (Katsantonis et al., 2023) The COFELET framework is highlighted as the foundation of this proposed modern cyber range. At a high-level, this framework seeks to combine teaching content, learning objectives, learner profiles, learning strategy, and educational context to fine-tune simulation scenarios and environments. Many range architectural specifications are provided, but the important part is that this new cyber range was designed to correct perceived weaknesses in current cyber ranges. This includes high costs, high testing requirements, learning strategy neglection, fixed workspace, ineffective assessment, and lack of participant profiles. The expected results of implementing this new cyber range design is the strengthening of cyber education by simulating real networks with a high degree of realism (Katsantonis et al., 2023).

The effect of simulation-based training on information warfare education are very positive. Simulation-based learning allows learners to gain hands-on experience in an educational environment that they can transfer directly into the real world. Key elements of successful integration of simulation-based learning into information warfare education include realistic custom networks and providing learners with scenarios that make them plan, act, and reflect.

5. Future Research

Future research should include further analysis of how AI can support information warfare education. Through research for this survey, it was discovered that there is much literature discussing how AI can support operational information warfare units, but very little on how it could benefit training. Promising uses of how AI could support information warfare education include AI agents to be used as opponents in digital information warfare serious games and educational assistants such as "Disciple-RKF". Future research should also include more holistic studies that compare traditional information warfare education to hybrid approaches that include the use of learning technologies such as game-based learning and simulation-based learning. Case studies showing the successful use of learning technologies within the information warfare education environment could encourage larger scale adoption of hybrid instruction approaches, and it can enable further research to be conducted on the use of specific learning technologies in this context. Finally, the learning technologies that were not found in this survey such as adaptive learning systems, e-learning platforms, learning management systems, mobile learning, social learning, and virtual/augmented reality should be explored to further this research area.

6. Conclusion

Information warfare is a critical warfighting domain in the modern world, and it is important to keep the training of these forces relevant and to utilize the best methods of instruction available. The use of learning technologies in this context can enhance information warfare education for both learners and instructors. Whether it be through artificial intelligence, game-based learning, gamification, or simulation-based learning, learning technologies provide additional support to the direct instruction of information warfare. This is a topic that should continue to be researched to further both national security and education.

NOTE: The views expressed are those of the author and do not reflect the official policy or position of the U.S. Air Force, Department of Defense, or the U.S. Government. Any reference to a commercial product is for informational purposes only and does not constitute an endorsement from the Department of the Air Force, the Department of Defense, or the U.S. Government.

References

An, T., & Oliver, M. (2021). What in the world is educational technology? Rethinking the field from the perspective of the philosophy of technology. Learning, Media and Technology, 46(1), 6–19. https://doi.org/10.1080/17439884.2020.1810066

Baek, Y. (2009). Digital Simulation in Teaching and Learning. In D. Gibson & Y. Baek (Eds.), Digital Simulations for Improving Education: Learning Through Artificial Teaching Environments (pp. 25-51). IGI Global. https://doi.org/10.4018/978-1-60566-322-7.ch002

Barjis, J., Sharda, R., Lee, P. D., Gupta, A., Bouzdine-Chameeva, T., & Verbraeck, A. (2012). Innovative teaching using simulation and virtual environments. Interdisciplinary Journal of Information, Knowledge & Management, 7. https://www.researchgate.net/profile/Tatiana-Bouzdine-Chameeva/publication/235246024_Innovative_Teaching_Using_Simulation_and_Virtual_Environments/links/0fcfd51098d1e6becd000000/Innovative-Teaching-Using-Simulation-and-Virtual-Environments.pdf

Berisford, C. J., Blackburn, L., Ollett, J. M., Tonner, T. B., Yuen, C. S. H., Walton, R., & Olayinka, O. (2022). Can gamification help to teach Cybersecurity? 2022 20th International Conference on Information Technology Based Higher Education and Training (ITHET), 1–9. https://doi.org/10.1109/ITHET56107.2022.10031716

Bowman, M., Tecuci, G., Boicu, M., & Comello, J. (2004). Information Age Warfare-Intelligent Agents in the Classroom and the Strategic Analysis Center. https://apps.dtic.mil/sti/citations/ADA431997

College, A. M. (2024). What is Instructional Design & Learning Technology?. Albertus Magnus College in New Haven, Connecticut. We have faith in your future. https://www.albertus.edu/instructional-design- and-learning-technology/ms/what-is-instructional-design-and-learning-technology.php

Cramer, M. J., Ramachandran, S., & Viera, J. K. (2004). Using computer games to train information warfare teams. Proceedings of The Interservice/Industry Training, Simulation & Education Conference (I/ITSEC). https://apps.dtic.mil/sti/citations/ADA459676

Davey, J., & Armstrong, H. L. (2001). An Approach to Teaching Cyber Warfare Tools and Techniques. Journal of Information Warfare, 1(2), 87–94.

Doriot, C., Hutto, C. J., & Smoak, C. (2011). Applying Training Analysis and Game-Based Learning toward the Design of a Cyber Warfare Real-Time Strategy Training Game.

Dusek, V. (2006). The Philosophy of Technology: An Introduction. Oxford: Blackwell.

Evgenia, I., Ekaterina, M., & Gennady, V. (2019). Development of information security quest based on use of information and communication technologies. Proceedings of the 12th International Conference on Security of Information and Networks, 1–5. https://doi.org/10.1145/3357613.3357632

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), 49–70. https://doi.org/10.17083/ijsg.v7i2.349

Flack, N., Voltz, C., Dill, R., Lin, A., & Reith, M. (2020). Leveraging Serious Games in Air Force Multi-Domain Operations Education: A Pilot Study. International Conference on Cyber Warfare and Security, 155-164,XVIII. https://doi.org/10.34190/ICCWS.20.097

Frater, M., & Ryan, M. (2001). Electronic warfare for the digitized battlefield. Artech House, Inc. https://scholar.google.com/scholar?hl=en&as_sdt=0%2C36&q=Frater%2C+M.+R.%2C+%26+Ryan%2C+M.+%282001%29.+Electronic+warfare+for+the+digitized+battlefield.+Boston%3A+Artech+House.&btnG=

Henno, J., Jaakkola, H., & Mäkelä, J. H. A. (2018). Using games to understand and create randomness. Workshop on Software Quality Analysis, Monitoring, Improvement, and Applications, 1–9. https://research.ulapland.fi/fi/publications/using-games-to-understand-and-create-randomness

Herr, C., & Allen, D. (2015). Video Games as a Training Tool to Prepare the Next Generation of Cyber Warriors. Proceedings of the 2015 ACM SIGMIS Conference on Computers and People Research, 23– 29. https://doi.org/10.1145/2751957.2751958

Katsantonis, M. N., Manikas, A., Mavridis, I., & Gritzalis, D. (2023). Cyber range design framework for cyber security education and training. International Journal of Information Security, 22(4), 1005–1027. https://doi.org/10.1007/s10207-023-00680-4

Libicki, M. C. (2020). The convergence of information warfare. In Information warfare in the age of cyber conflict (pp. 15–26). Routledge. https://www.taylorfrancis.com/chapters/edit/10.4324/9780429470509-2/convergence-information- warfare-martin-libicki

Metoyer, R., Stumpf, S., Neumann, C., Dodge, J., Cao, J., & Schnabel, A. (2010). Explaining How to Play Real- Time Strategy Games. In M. Bramer, R. Ellis, & M. Petridis (Eds.), Research and Development in Intelligent Systems XXVI (pp. 249–262). Springer London. https://doi.org/10.1007/978-1-84882-983- 1_18

Ormrod, D., Scott, K., Scheinman, L., Kodalle, T., Sample, C., Turnbull, B., & Ormrod, A. (2020). The Persuasion Game: Serious Gaming Information Warfare and Influence. Journal of Information Warfare, 19(2), 27– 45.

Plass, J. L., Mayer, R. E., & Homer, B. D. (2020). Handbook of game-based learning. Mit Press. https://books.google.com/books?hl=en&lr=&id=_2fKDwAAQBAJ&oi=fnd&pg=PR5&dq=handbook+of+game+based+learning&ots=AhkVTh--H2&sig=XQsvVXONk696N0p95lj6l8IvJdo

Ragsdale, D. J., Lathrop, S. D., & Dodge, R. C. (2003). Enhancing Information Warfare Education Through the Use of Virtual and Isolated Networks. Journal of Information Warfare, 2(3), 47–59.

Schweitzer, D., & Fulton, S. (2010). A Hybrid Approach to Teaching Information Warfare. International Conference on Information Warfare and Security, 299–X. https://www.proquest.com/docview/869617317/abstract/50C47F9FE5441F2PQ/1

Taddeo, M. (2012). Information Warfare: A Philosophical Perspective. Philosophy & Technology, 25(1), 105– 120. https://doi.org/10.1007/s13347-011-0040-9

Tobias, S., Fletcher, J. D., & Wind, A. P. (2014). Game-Based Learning. In Handbook of Research on Educational Communications and Technology (pp. 485–503). https://doi.org/10.1007/978-1-4614-3185-5_38

Williams, P. A. (2010). Information Warfare: Time for a redefinition. https://ro.ecu.edu.au/isw/37/

Yamin, M. M., Katt, B., & Nowostawski, M. (2021). Serious games as a tool to model attack and defense scenarios for cyber-security exercises. Computers & Security, 110, 102450.