NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

CAPSTONE

INTERACTIVE WARGAMING CYBERWAR: 2025

by

David Tyler Long
Christopher M. Mulch

December 2017

Thesis Advisor: Michael Freeman
Second Reader: Robert Burks

Approved for public release. Distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE	*Form Approved OMB No. 0704–0188*

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC 20503.

1. AGENCY USE ONLY	**2. REPORT DATE** December 2017	**3. REPORT TYPE AND DATES COVERED** Capstone

4. TITLE AND SUBTITLE INTERACTIVE WARGAMING CYBERWAR: 2025	**5. FUNDING NUMBERS**
6. AUTHOR(S) David Tyler Long and Christopher M. Mulch	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB number NPS.2017.0054.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release. Distribution is unlimited.	**12b. DISTRIBUTION CODE**

13. ABSTRACT (maximum 200 words)

Cyberspace operations are an increasingly important mission focus and warfighting domain within the Department of Defense (DOD). There are a number of educational courses and training exercises that have been developed to prepare leaders to plan and execute cyberspace-based effects to support operations; however, there are currently no virtual simulations used by the military to train and educate servicemembers in the basic concepts of cyberspace operations. Because of this training gap, we have designed and developed *CyberWar: 2025*, a simultaneous turn-based multiplatform computer-based educational wargame that is intended to be used as a support tool for education and training of basic cyberspace operations concepts to military professionals and other DOD personnel. The objective of *CyberWar: 2025* is to stimulate, build, and increase the players' knowledge base and experience in planning and practical application of cyberspace operations in the areas of defensive cyberspace operations, offensive cyberspace operations, and computer network exploitation. *CyberWar: 2025* focuses on doctrine and doctrinal training as a serious game by reinforcing key learning objectives set by the DOD; however, this wargame also encourages player engagement and motivation through unique and balanced multiplayer interactions within a virtual environment.

14. SUBJECT TERMS cyber education, cyber training, cyber wargaming, computer-based simulation, virtual simulation, educational courses, multiplayer, serious games, cyberwar, cyber domain, cyberspace operations, cyber doctrine, cyber policy, computer network exploitation	**15. NUMBER OF PAGES** 101
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

INTERACTIVE WARGAMING CYBERWAR: 2025

David Tyler Long
Sergeant First Class, United States Army
B.S., University of Maryland University College, 2013

Christopher M. Mulch
Captain, United States Army
B.A., Columbus State University, 2011

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION STRATEGY AND POLITICAL WARFARE

from the

NAVAL POSTGRADUATE SCHOOL
December 2017

Approved by: Dr. Michael Freeman
Thesis Advisor

Dr. Robert Burks
Second Reader

Dr. John Arquilla
Chair, Department of Defense Analysis

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Cyberspace operations are an increasingly important mission focus and warfighting domain within the Department of Defense (DOD). There are a number of educational courses and training exercises that have been developed to prepare leaders to plan and execute cyberspace-based effects to support operations; however, there are currently no virtual simulations used by the military to train and educate servicemembers in the basic concepts of cyberspace operations. Because of this training gap, we have designed and developed *CyberWar: 2025*, a simultaneous turn-based multiplatform computer-based educational wargame that is intended to be used as a support tool for education and training of basic cyberspace operations concepts to military professionals and other DOD personnel. The objective of *CyberWar: 2025* is to stimulate, build, and increase the players' knowledge base and experience in planning and practical application of cyberspace operations in the areas of defensive cyberspace operations, offensive cyberspace operations, and computer network exploitation. *CyberWar: 2025* focuses on doctrine and doctrinal training as a serious game by reinforcing key learning objectives set by the DOD; however, this wargame also encourages player engagement and motivation through unique and balanced multiplayer interactions within a virtual environment.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

ACOPC	Army Cyber Operator Planners Course
ALCOC	Army Leader Cyberspace Operations Course
ARCYBER	United States Army Cyber Command (ARCYBER)
APT	advanced persistent threat
CEMA	cyber electromagnetic activities
CNE	computer network exploitation
COPS	Cyberspace Operations Planners Seminar
CTC	Combat Training Centers
DCO	defensive cyberspace operations
DDOS	distributed denial of service
DICE	Design, Innovate, Communicate, Entertain
DOD	Department of Defense
DSTS	Dismounted Soldier Training System
ECOS	Executive Cyberspace Operations Seminar
ELO	enabling learning objectives
EST	Engagement Skills Trainer
G4C	Games for Change
GFT	Games for Training
HPTL	high payoff target list
HVTL	high value target list
IA	information assurance
IO	information operations
IOT	Internet of Things
JP	Joint Publication
JSON	JavaScript Object Notation
KIPS	Kaspersky Interactive Protection Simulation
MDA	mechanics, dynamics, and aesthetics
MEAN	MongoDB, ExpressJS, AngularJS, and NodeJS
MOOC	massive open online course
MVC	model-view controller

NGG	Next Generation Game
NPC	non-playable character
OCO	offensive cyberspace operations
OPE	operational preparation of the environment
PKI	Public Key Infrastructure
PvP	player versus player
SGI	Serious Games Initiative
SOC	Squadron Officer College
SVG	scalable vector graphics
TLO	terminal learning objectives

ACKNOWLEDGMENTS

First and foremost, I would like to graciously thank my wife, Courtney, for the love, patience, and encouragement she has given me during my time here at NPS. Thank you for being the rock-solid foundation throughout my Army career. For that, I am forever in your debt.

I sincerely want to thank my advisors, Dr. Michael Freeman and Dr. Robert Burks, for their wisdom, patience, and guidance. I also want to thank Dr. John Arquilla for planting the seed for this project; Kate Egerton for the amazing thesis assistance from start to finish; Eric Heine and the rest of the MOVES developers for all their coding help and development support; and Greg, Ian, Anders, Niels, Bo, and Scott for their hard work and feedback in the early design stages of *CyberWar: 2025*.

—SFC David "Ty" Long

I am grateful for the amazing support of the faculty and staff of Naval Postgraduate School. I appreciate the courses and instruction provided by the Defense Analysis Department. I am thankful for the hours Kate Egerton of the Graduate Writing Center spent working on this project. She provided valuable feedback and guidance, helping turn random thoughts and independent clauses into the completed work of this thesis.

I am especially grateful for the instruction provided by Professors Appleget, Burks, and Freeman on the topic of wargaming. Without this instruction, this project would not have been possible. Their leadership and mentorship laid the foundation and provided direction for this project.

Finally, a special thanks to my wife, Julie, and my daughter, Isabella, who gave so much encouragement and support during the many hours I spent away working on this project.

—CPT Chris M. Mulch

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

Cyberspace operations are an increasingly important mission focus and a warfighting domain within the Department of Defense (DOD).[1] But despite the fast-paced and consistently changing cyberspace domain, there are no DOD-developed virtual simulations used by the military that cover basic cyberspace operations training. The purpose of this project is to fill that gap.

During the course of several months, we, the authors, developed a computer-based educational wargame designed to prepare decision makers and service members to succeed in cyberspace operations. This multiplatform computer-based educational wargame, designed and adapted for multiple players in a rapidly changing virtual environment, simulates real-world operations. The simulation, dubbed *CyberWar: 2025*, offers a level of randomization that provides players a different outcome each time the simulation is played. We expect the simulation of cyberspace operations in this serious game, or games that support an education purpose and are not entirely for entertainment format, to reinforce existing instructional programs and provide an engaging and practical application of cyberspace concepts for cyberspace planning, theory, and doctrine.[2]

The DOD has used several virtual simulations to train and educate servicemembers for many years. Virtual simulations such as America's Army, Virtual Battlespace 2, the Engagement Skills Trainer (EST), and the Dismounted Soldier Training System (DSTS) have been actively used by the military to train, educate, and prepare soldiers for specific tasks, mainly dealing with land combat operations.[3] The tasks include squad-based infantry tactics, react-to-contact, and

[1] Jim Garamone, "Cyber Command Deputy Details Formation of Cyber Mission Force," U.S. Department of Defense, June 22, 2016, https://www.defense.gov/News/Article/Article/809904/cyber-command-deputy-details-formation-of-cyber-mission-force/.

[2] Fedwa Laamarti, Mohamad Eid, and AbdulmotalebFedwa Laamarti, Mohamad Eid, and Abdulmotaleb El Saddik, "An Overview of Serious Games," *International Journal of Computer Games Technology* 2014 (2014): 2, https://doi.org/10.1155/2014/358152. El Saddik, "An Overview of Serious Games," Research article, International Journal of Computer Games Technology, 2014, https://doi.org/10.1155/2014/358152.

[3] United States Army, *America's Army*, Windows (United States Army, 2002), https://www.americasarmy.com/; Bohemia Interactive, "Bohemia Interactive Simulations," 1999, https://bisimulations.com; United States Army, "Engagement Skills Trainer (EST)," USAASC, December 21, 2015, http://asc.army.mil/web/portfolio-item/engagement-skills-trainer-est/; *Dismounted Soldier Training System* (Intelligent Decisions, 2017), http://www.intelligent.net/news/dismounted-soldier-training-system-0812.

calling for artillery fire. However, there are a couple of DOD-developed cyber related simulations that are extremely technical or present a highly abstracted view of cyber actions. The Naval Postgraduate School has developed CyberCIEGE and CyberStrike, the two most prominent examples we will address in this paper.[4]

CyberCIEGE is a single-player and highly technical cybersecurity serious game that teaches the player how to configure and maintain a network, security management and configuration of that network, protection of network assets, and defense of end users from attacks.[5] CyberStrike is a multiplayer serious game in which several players take on specific cyber actor roles and conduct either offensive or defensive attacks against other players in a turn-based setting. We will discuss these two games in depth in chapter two.

A. WHY WE USE GAMES

Serious games combine both educational and entertainment game elements.[6] The industry standard and purpose of serious games is to provide players with educational experience and challenges that reinforce set core tasks that the player or players need to accomplish. The game rewards these players with some sort of experience or knowledge at the conclusion of the game. Gamification's, which is the practice of developing serious games, effectiveness is based on the increased long-term engagement with the program, which relies on leveraging the psychology of motivation to encourage players to play.[7] Maslow's hierarchy of needs provides a model that aids in the understanding of how motivation is used in serious games to create positive impacts. These levels include physiological, security, belonging, esteem, and self-actualization needs. Examples of these needs are experienced in everyday life in the form of shelter, stability, friendship, status, and achievement. Gamification provides a means for working toward self-actualization by allowing participants to fulfill the need for achievement, challenge,

[4] *CyberCIEGE*, Windows (Monterey, CA: Naval Postgraduate School and Rivermind, Inc., 2004), http://my.nps.edu/web/cisr/cyberciege; *CyberStrike - GlobalECCO*, Web (Monterey, CA: Naval Postgraduate School, 2011), https://globalecco.org/play.

[5] Michael Thompson and Cynthia Irvine, "CyberCIEGE: A Video Game for Constructive Cyber Security Education," *Call Signs* 6, no. 2 (2015).

[6] Talib S. Hussain and Susan L. Coleman, eds., *Design and Development of Training Games: Practical Guidelines from a Multidisciplinary Perspective* (New York, NY: Cambridge University Press, 2015), 1.

[7] Jemma Looyestyn et al., "Does Gamification Increase Engagement with Online Programs? A Systematic Review.," *PLOS ONE* 12, no. 3 (March 31, 2017): 2, https://doi.org/10.1371/journal.pone.0173403.

and inclusion in a group. Daniel Pink establishes that purpose, autonomy, and mastery must be achieved as motivational factors to work toward self-actualization.[8] Purpose, autonomy, and mastery are common factors of a well-developed gamification application. Purpose is experienced when players are engaged in a meaningful activity where their visible actions have an effect. Autonomy is achieved when players have the ability to choose their strategy within the rules of the game. The game must not be so restrictive that it causes players to be overly restrained in their actions. Finally, mastery is accomplished when players are able to see their skills and lessons learned being applied during the game, contributing to the achievement of an objective.[9] The combination of Maslow's and Pink's concepts is used as the basis for understanding how gamification motivates players to act in a way that fulfills their needs.

The entertainment element within serious games is what keeps players engaged, creating an internal learning cycle: understanding the challenge/concept, adapting and overcoming through learning, and then rewarding through self-accomplishment. Learning objectives are the key in design and development of serious games, and these objectives should be structured in a hierarchal manner starting from the most basic concepts and increasing in difficulty to the pinnacle of understanding.[10] This higher understanding is where the player has the "ability to synthesize new knowledge and make critical judgments," and building this understanding is the ultimate end goal of serious games.[11]

Wargames are very similar to serious games; they provide a level of educational experience to the players and may or may not have a level of entertainment involved. Wargames also are played with a set of rules within a well-established framework. The DOD uses wargames to stimulate creative thinking, decision making, and problem solving as applied to possible situations that the United States might encounter in the future. These elements are exactly what serious games work to accomplish.

[8] Nils Davis, "The 'Drive' To Gamification: Motivation 3.0 and Game Mechanics," *Hardcore Product Management* (blog), September 4, 2012, https://pmhardcore.com/the-drive-to-gamification-motivation-3-0-and-game-mechanics/.

[9] Andrzej Marczewski, "Understanding Intrinsic Motivation with RAMP," Gamification Co, May 1, 2013, http://www.gamification.co/2013/05/01/understanding-intrinsic-motivation-with-ramp/.

[10] Hussain and Coleman, *Design and Development of Training Games*, 126.

[11] Ibid., 57.

B. WHY DO GAMES WORK?

Game-based learning is a form of experienced-based learning. The goal is to encourage students to perform specific actions in support of the learning objectives.[12] The use of games has been successful in the instruction of many topics including math, electronics, economics, and military training. After conducting an extensive literature review, Robert T. Hays concluded that well designed games that tie to specific instructional objectives have instructional value when they are incorporated into a larger program.[13] Instructional games should never be stand-alone products; they should always be used in combination with other instructional methods.[14]

The use of a stand-alone instructional game would be largely ineffective because of the lack of debriefing during the instructional process. The idea of debriefing is common in education, sports, and life. Simply put, it is the time where a coach, instructor, or leader is able to discuss what was supposed to happen, what happened, and what could be done to improve.[15] Marc Prensky supports the importance of debriefing when he explains that simply "playing" the simulation can lead to learning, but for a game to be most effective as an educational aid, there must be reflection and processing of lessons learned in the game.[16] The role of the instructor is important because of the need for serious games to be incorporated with programs that provide debriefing and feedback during the instruction process. The instructor also plays a major role in ensuring that student/players are able to focus on the course content as opposed to being focused on the mechanics and requirements of the game.[17] Instructional games conducted online or with limited instructor involvement should incorporate similar "instructor functions" including evaluation, debriefing, and feedback to remain an effective contribution to the overall instructional objectives.[18] The process of debriefing is also possible in networked based games

[12] Frank Anders, "Gaming the Game: A Study of the Gamer Mode in Educational Wargaming," *Simulation & Gaming* 43, no. 1 (February 1, 2012): 2, https://doi.org/10.1177/1046878111408796.

[13] Robert T. Hays, "The Effectiveness of Instructional Games: A Literature Review and Discussion" (Orlando, FL: Naval Air Warfare Center Training Systems Division: DTIC Document, 2005), 41.

[14] Ibid.

[15] Marc Prensky, "'Simulations': Are They Games?," in *Digital Game Based Learning* (New York, NY: McGraw-Hill, 2001), 8.

[16] Ibid.

[17] Hays, "The Effectiveness of Instructional Games: A Literature Review and Discussion," 53.

[18] Ibid.

through the use a chat function to exchange information about the lessons gleaned from the experience.[19]

Frank Anders stresses the importance of instructor involvement in the wargaming process. He suggests that the number of instructors might need to be upwards of one per every three to four students. This is viewed as an unobtainable number of instructors for many educational organizations.[20] The instructor role will ensure that the wargame does not simply become a contest of wills and they will also support student/players through the process of understanding the rules and purpose of the activity in regards to the educational objectives.[21] The role of the instructors will include conducting the rigorous and extensive debrief after completion of the game.[22] Anders states that students should be provided a detailed debriefing that includes discussion of overall experience, analysis of moves, and examination of examples of gamer mode. The purpose of debriefing is to connect the game experience with learning objectives and address how the lessons could be applied to real-world situations.[23] Anders also suggests that allowing student/players to engage with the wargame multiple times could reduce the occurrence of gamer mode.

Prensky cites Elliot Masie who argues that, "in a game, what we're triggering is the competitive/cooperative spirit, what we're triggering is a playfulness, and what we're triggering is the achievement, greed and victory element."[24] Masie addresses the question of when a simulation becomes a game. Simply put, the difference between a simulation and game occurs in the mind of the student/player. Incorporating the elements of learning and competing can enhance a simulation. Prensky also stresses the importance making simulations more interesting and engaging by removing the boring elements and adding fun, the result being a game. He suggests the next step would be to add the other elements of a game, which, he suggests, are goals, rules, challenges, and narrative or scenario.[25]

[19] Prensky, "'Simulations': Are They Games?"

[20] Anders, "Gaming the Game," 129.

[21] Ibid.

[22] Ibid., 130.

[23] Ibid.

[24] Prensky, "'Simulations': Are They Games?," 3.

[25] Ibid.

Wargames are used to support learning objectives; they are able to teach and reinforce training of specific maneuvers or tasks.[26] However, they should be viewed as tools that will stimulate players to make decisions and better explore concepts in a dynamic environment.[27] Educational games should be treated only as a complement to the course, as opposed to being the principal method of teaching. An instructor who can assist with debriefing leads student-players to reflect on their experience with the game. This reflection will increase the effectiveness of educational wargaming and better prepare students for future educational games and real situations. Wargames enhance a learning objective by testing the skills of student players; in addition, wargaming has the ability help students learn to accept conditions that they cannot control within the game. There will be unforeseen scenarios in the wargame just as there are in actual warfare. Seeing the unthinkable in a wargame prior to experiencing it in real life benefits the student/player.[28]

Commercial games should not simply be added to an educational situation in hopes of their having a positive impact. There is minimal benefit to using commercial games in an educational situation without a great deal of modification. Educational games are best suited for instructional purposes when they are developed with the educational objectives in mind. Instructional games should be viewed as training aids to support existing learning objectives.[29]

C. PURPOSE AND TARGET AUDIENCE OF CYBERWAR: 2025

We have developed a computer-based educational wargame simulating this domain to educate and train users in the basic concepts of cyberspace operations; however, *CyberWar: 2025* is not designed and does not cover all topics in the broad field of cyber. The wargame was designed as an educational training aid for entry-level Army cyber training courses that are attended by U.S. Army leaders, ranging from members of a unit staff to cyber electromagnetic activities (CEMA) professionals and senior leaders. The target audience of the wargame is

[26] Frank Anders, “Unexpected Game Calculations in Educational Wargaming: Design Flaw or Beneficial to Learning?,” in *DiGRA ‘11 - Proceedings of the 2011 DiGRA International Conference: Think Design Play* (DiGRA/Utrecht School of the Arts, 2011), 3, http://www.digra.org/wp-content/uploads/digital-library/11310.31521.pdf.

[27] Ibid.

[28] Ibid., 15.

[29] Hays, “The Effectiveness of Instructional Games: A Literature Review and Discussion,” 53.

members of a unit staff with limited experience with cyberspace operations. The wargame was developed to be played by students with no prior education or training in cyberspace operations. Players with cyberspace operations experience can also use *CyberWar: 2025* as a refresher opportunity to increase understanding of strategic cyberspace concepts. The objective of the wargame is to stimulate, build, and increase the players' knowledge base while they gain experience in planning and practical application of cyberspace operations such as defensive cyberspace operations (DCO), offensive cyberspace operations (OCO), and computer network exploitation (CNE). *CyberWar: 2025* allows for use as a stand-alone education and training aid; however, it is intended for use as a practical exercise section of an educational course or refresher training prior to a major staff exercise.

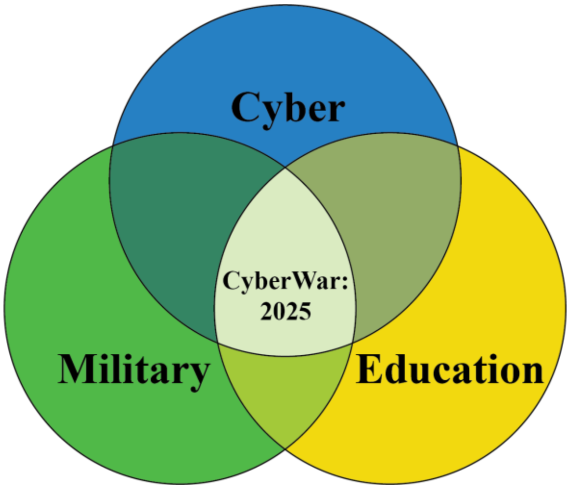


Figure 1. *CyberWar: 2025* Venn Diagram

D. CYBERWAR: 2025 SUPPORTING EDUCATION AND TRAINING

This game will focus on supporting the courses hosted by the United States Army Cyber Command (ARCYBER) and the training that occurs as part of the Cyber Support Corps and Below (CSCB). ARCYBER currently host several courses that provide training to specialists and senior leaders in the Cyber Electromagnetic Activities (CEMA) fields, including Army Cyber Operator Planners Course (ACOPC), Army Leader Cyberspace Operations Course (ALCOC), Executive Cyberspace Operations Seminar (ECOS), and Cyberspace Operations Planners Seminar (COPS).

CSCB is currently exploring, experimenting and evaluating with the integration of cyberspace operations into operational training exercises. A portion of this training occurs at the Combat Training Centers (CTC), where the rotational unit combines with members of ARCYBER, 780th Military Intelligence Brigade (Cyber), Cyber Protection Brigade, and 1st Information Operations (IO) Command to work toward CEMA objectives. During the training at the CTCs, cyber professionals are evaluated based on collective tasks published in the Army Universal Task List. The cyberspace-related collective tasks include Conduct Cyber Network Operations, Develop Cyber Situational Awareness, Integrate OCO, and Conduct Defensive DCO.[30]

[30] United States Army, *ART 5.9.1: Conduct Cyberspace Operations* (Department of Defense, February 27, 2013), https://rdl.train.army.mil/catalog-ws/view/100.ATSC/AFBAB9EB-8336-4798-961E-DF8009B23537-1361948176953/report.pdf.

II. GAMIFICATION OF CYBERSPACE OPERATIONS FOR EDUCATION

In an educational setting, gamification is synonymous with game-based learning, learning games, and fun ware. Gamification is a form of serious games, which are defined as "digital games used for purposes other than mere entertainment."[31] A serious game uses key elements of gamification including mechanics, components, and dynamics as part of education to solve a serious problem; gamification uses key elements to induce an engaging behavior.[32] Serious games provide entertainment value and reduce students' tension by providing a less intimidating environment in which to learn new concepts such as cybersecurity, while working toward specific educational objectives.[33] The use of game-based learning and serious games predates the use of gamification. The commonality among all of these terms is that they are used to support education and they are created for more than mere entertainment.[34] According to Kim and Lee, it is foreseeable that gamification could be applied to every aspect of life, resulting in gamification of business, education, finance, fitness, marketing, the medical field, and military.[35]

The first definition of gamification is "the process of game thinking and game mechanics to engage users and solve problems."[36] According to Kim and Lee, the concept of gamification, simply put, is the application of game-design into non-game situations.[37] They explain that the main goal of gamification is to increase engagement, create richer experiences, and increase enjoyment through the use of game mechanics in everyday life.[38] Typically, gamification involves the adoption of game design techniques and game mechanics in order to change behavior, develop skills, or drive innovation among a target audience—that being employees,

[31] Looyestyn et al., "Does Gamification Increase Engagement with Online Programs?," 2.

[32] Mehdi Khosrow-Pour, ed., *Encyclopedia of Information Science and Technology, Third Edition:* (IGI Global, 2015), 2, https://doi.org/10.4018/978-1-4666-5888-2.

[33] Saboor Zahir et al., "Protection and Deception: Discovering Game Theory and Cyber Literacy through a Novel Board Game Experience," *ArXiv:1505.05570 [Cs]*, May 20, 2015, 1, http://arxiv.org/abs/1505.05570.

[34] Looyestyn et al., "Does Gamification Increase Engagement with Online Programs?," 2.

[35] Jung Tae Kim and Won-Hyung Lee, "Dynamical Model for Gamification of Learning (DMGL)," *Multimedia Tools and Applications* 74, no. 19 (October 1, 2015): 2, https://doi.org/10.1007/s11042-013-1612-8.

[36] Looyestyn et al., "Does Gamification Increase Engagement with Online Programs?," 2.

[37] Kim and Lee, "Dynamical Model for Gamification of Learning (DMGL)," 2.

[38] Ibid.

customers, or a community.[39] The common components are points, badges, leaderboards, quests, competition/challenge, virtual goods, gifting/sharing, and levels.[40] There are a number of benefits to incorporating gamification. According to Asha Pandey of EI Design, the benefits of gamification include "better learning experience, better learning environment, instant feedback, prompting behavior change applicable to most learning needs, and impact on the bottom line."[41] The commonality of these factors contributes to increased learner engagement, resulting in the improved ability to recall. According to Asha Pandey, providing players with "fun" has been shown to increase retention of course material, and the environment used in gamification allows for players to "practice" real life situations in a safe, effective, and informal situation.[42] The use of instant feedback encourages learners to better understand what they know or should know from the lesson. The use of points, badges, and leaderboards allows for certain behaviors to be reinforced resulting in desired changes in behaviors. This is largely made possible using repeated retrieval, spaced repetition, and experimentation. Gamification adapts to a variety of different learning needs, styles, topics, and applications ranging from cyber security to compliance. The end goal of gamification is the increased contribution of participants based on engagement, which results in a positive impact on performance for the individual and organization.[43]

A. HISTORY OF WARGAMING AND GAMIFICATION

Wargaming has long been a method of role-playing to prepare, understand, anticipate, and even plan for war. Wargaming has grown from the early use of games such as chaturaṅga, otherwise known as chess, and Wei-Chi, most commonly known as Go, which have been used as abstract versions of war.[44] The use of maps and model ships advanced the use of wargaming as

[39] Eyvind Garder B. Gjertsen, "Use of Gamification in Security Awareness and Training Programs," *98*, 2016, 23, https://brage.bibsys.no/xmlui/handle/11250/2403232.

[40] Jung Tae Kim and Won-Hyung Lee, "Dynamical Model for Gamification of Learning (DMGL)," *Multimedia Tools and Applications* 74, no. 19 (October 1, 2015): 4, https://doi.org/10.1007/s11042-013-1612-8; Torsten Reiners and Lincoln C. Wood, eds., *Gamification in Education and Business* (Cham: Springer International Publishing, 2015), https://doi.org/10.1007/978-3-319-10208-5.

[41] Asha Pandey, "6 Killer Examples of Gamification in ELearning," eLearning Industry, October 6, 2015, 2, https://elearningindustry.com/6-killer-examples-gamification-in-elearning.

[42] Ibid., 3.

[43] Ibid.

[44] Matthew Caffery Jr., "Toward a History-Based Doctrine for Wargaming," *Air and Space Power Journal* 13, no. 3 (Fall 2000): 33.

early practitioners used these early methods to gain insights and understanding of their plans prior to execution, allowing players to forward think about the impacts of their decisions. Wargaming has been in practice since the early years of Kriegsspiel by the German and Prussian armies in 1824.[45] The beginning of modern wargaming is commonly associated with the methods used by a Prussian officer named Baron von Reisswitz. The earliest versions of his wargames date back to 1811.

The earliest use of wargaming in the United States dates back to 1883 when Major William R. Livermore adopted and developed a version Prussian Kriegsspiel to practice the art of war on topographic maps.[46] The early forms of wargames shaped the methods of waging war that are still in use today.[47] The earliest versions of wargames in the United States were simply German games translated into English, combined with attribution tables from the Civil War. Modern wargames are still conducted using simple maps; however, increasingly complex wargames require computers to operate the algorithm and provide an interface with the players. Today, large-scale wargames are in the form of Title Ten wargames such as “Global Engagement” and “Army after Next.”[48] Wargaming and gamification continue to grow as methods of gaining insight about the impacts of future decisions in the military and other professions. This thesis does not cover the history of wargaming in depth; however, for more information on the history of wargaming please refer to these aforementioned sources.[49]

The use of gamification concepts and techniques date back to the early 1900s, significantly predating the term itself. The earliest examples highlight the use of gamification in business and education. The Boy Scouts provide an early example of gamification in education by using badges and a rank system to denote success as Boy Scouts progress through the program. The learning of new tasks is associated with the achievement of a new badge or rank.

[45] Michael E. Freeman, “Pushing the Envelope of Pedagogical Gaming: Dark Networks,” *PS: Political Science & Politics* 50, no. 04 (October 2017): 1, https://doi.org/10.1017/S1049096517001251.

[46] Caffery Jr., “Toward a History-Based Doctrine for Wargaming,” 36.

[47] Ibid.

[48] Ibid., 52.

[49] Ibid.; Peter P. Perla, *The Art of Wargaming: A Guide for Professionals and Hobbyists* (Annapolis, MD: Naval Institute Press, 1990); Neil Thomas, *Wargaming: An Introduction* (Stroud: Sutton Publishing, 2005).

This practice dates back to 1910.[50] The first commonly accepted use in business marketing interaction came in 1912 with the appearance of the free prize in every bag of Cracker Jacks.[51]

A significant increase of gamification was seen during the next seven decades, as many businesses begin using customer loyalty cards, promotional items in products, and games such as McDonald's Monopoly™ game. The next high point of gamification occurred in the 1980s when academic articles started referencing the use of games for learning in both education and business contexts, although the term gamification was still not used.[52] As computers entered the classroom, the ability to utilize gamification became increasingly more accessible. In the 1990s, students were introduced to games in the classroom such as Math Blaster and The Incredible Machine. These games were highly criticized, but have shown positive effects on student's learning of basic skills using repetition.[53]

The term gamification is credited to Nick Pelling, based on his work as a consultant working on Serious Games Initiative (SGI).[54] He first used the term in 2002 as part of the development of SGI.[55] The goal, simply put, was to use serious computer games as a way to make education and training more fun while "the goal of the initiative [was] to help usher in a new series of policy education, exploration, and management tools utilizing state of the art computer game designs, technologies, and development skills" and to "accelerate the adoption of computer games for a variety of challenges facing the world today."[56] SGI and the first gamification consulting firm, created in 2003, have both disbanded, but the accomplishment of their goals and many uses of gamification are visible in the military and other fields.

These early initiatives produced developments in the field and organizations that continue to have an impact today. Games for Change (G4C) grew out of these advancements. G4C was established in 2004, and their goal was to focus on the use of gamification for positive social

[50] Daniel Griffin, "Resources: Gamification in e-Learning," Ashridge Executive Education, 4, accessed August 14, 2017, https://www.ashridge.org.uk/virtual-ashridge/elearning-insights/resources-gamification-in-e-learning/.

[51] Ibid.

[52] Steve Dale, "Gamification: Making Work Fun, or Making Fun of Work?," *Business Information Review* 31, no. 2 (June 1, 2014): 4, https://doi.org/10.1177/0266382114538350.

[53] Griffin, "Resources," 4.

[54] Dale, "Gamification," June 1, 2014, 3.

[55] Ibid., 4.

[56] Griffin, "Resources," 4.

impacts. The prime example is their early development of Peacemaker, which is a serious game that allows players to gain a greater understanding of the Arab and Israeli conflict.[57]

Advances in software technology and the Internet helped the next two developments in gamification such as Bunchball. Examples of gamification are often hosted on the technologies we use on a daily basis. The shift from using personal computers to using smart phones and tablets for Internet access has contributed to the growth of gamified applications. The increased use of smart phones and tablets overall has increased the amount of gamification on these platforms.[58] Bunchball, which was created in 2007, is the first commercially developed and leading platform specifically designed for gamification. Bunchball allows companies and organizations to use game elements such as points, leaderboards, and badges to empower employee engagement and customer loyalty. According to the Bunchball website, their use of gamification has led to over 20 billion actions associated with customer loyalty and employee engagement. They have worked for a number of noteworthy companies ranging from Adobe to Universal Studios.[59]

With the increase in interest in gamification came the creation of summits to get likeminded people together to share ideas about advancements. A web conference hosted by DICE (Design, Innovate, Communicate, Entertain) contributed to the term as well as to the advances in gamification. The success of the web conference contributed to the creation of the first gamification summit in 2011 in San Francisco, which attracted more than 400 people. This is also the same year that the term gamification made it into the Oxford Dictionary, which included the term on their shortlist, defining it as "the application of concepts and techniques from games to other areas of activity."[60] According to research conducted by M2 Research in

[57] Daniel Griffin, "Resources: Gamification in e-Learning," Ashridge Executive Education, 5, accessed August 14, 2017, https://www.ashridge.org.uk/virtual-ashridge/elearning-insights/resources-gamification-in-e-learning/; Steve Dale, "Gamification: Making Work Fun, or Making Fun of Work?," *Business Information Review* 31, no. 2 (June 1, 2014): 3, https://doi.org/10.1177/0266382114538350.

[58] Kim and Lee, "Dynamical Model for Gamification of Learning (DMGL)," 9.

[59] Bunchball, "Bunchball," April 29, 2011, http://www.bunchball.com.

[60] Griffin, "Resources," 5.

2011, the revenue of gamification, then valued at nearly $100 million, was predicted to grow to 2.8 billion by 2016 and to as much as $7.3 billion by 2021.[61]

B. EXAMPLES OF USE IN EDUCATION

Gamification in education is a form of active learning, the role of which is to structure activities and processes within a module of instruction. The focus of this structure is designed to increase engagement and educational outcomes.[62] The use of learning games has been seen in all educational subjects including language, mathematics, science, and computers.[63] The use of games has been applied to learning skills in serious game sectors such as medical instruction, fire-fighting, military, and simulations of flight or driving.[64]

The most recent developments in educational gamification have been prompted by the growth in online education or e-learning. Coursera hosted a Massive Open Online Course (MOOC) on gamification in 2012. This initial offering of this course attracted 80,000 students.[65] Educational websites covering a variety of different topics use gamification. Khan Academy utilizes gamification to accomplish its mission "to provide a free world-class education for anyone anywhere."[66] Khan Academy hosts ten million students that view 300-million videos per month, and Khan Academy students have completed 1.6 billion activities.[67] Khan Academy combines YouTube videos for instruction and gamification features such as points and badges to encourage students to track their progress toward mastery of the subject matter.[68] According to Sal Khan, the use of game mechanics actually predates the use of the video instruction. This

[61] Sam S. Adkins, "The 2016–2021 Global Game-Based Learning Market —Serious Play Conference" (Ambient Insight, July 26, 2016), 7, http://seriousplayconf.com/downloads/the-2016-2021-global-game-based-learning-market/.

[62] Khosrow-Pour, *Encyclopedia of Information Science and Technology, 3rd Ed.*, 3039–47; Reiners and Wood, *Gamification in Education and Business*, 5.

[63] Kim and Lee, "Dynamical Model for Gamification of Learning (DMGL)," 2.

[64] Ibid.

[65] Dale, "Gamification," June 1, 2014, 4.

[66] Brian Burke, *Gamify: How Gamification Motivates People to Do Extraordinary Things* (Brookline, MA: Bibliomotion, 2014), 10.

[67] Ibid.

[68] Ibid.

highlights the significance of gamification to the overall structure of the Khan Academy instructional model.[69]

C. EXAMPLES OF USES IN THE MILITARY

There are numerous examples of the use of gamification in the military, ranging from using gamification in the recruiting process to the training and education of service members. The U.S. Army uses gamification in the recruiting process with America's Army. The game, which is free to play, exists in multiple editions dating back to 2002 and is designed to provide potential recruits with an introduction to Army career opportunities.[70] According to a report that was prepared by MIT and presented to the U.S. Congress, "30 percent of all Americans age 16 to 24 had a more positive impression of the Army because of the game and, even more amazingly, the game had more impact on recruits than all other forms of Army advertising combined."[71]

The U.S. Air Force's Air University's Squadron Officer College (SOC) uses gamification during their course to educate company-grade officers (Lieutenants and Captains). The commander and president of Air University explained how they use "technology innovations to transform learning environments in an effort to keep them efficient, effective, relevant, and adaptable to tomorrow's challenges."[72] The SOC has developed and uses over 30 vignettes in their programs to engage officers with an "immersive learning experience."[73]

The use of games has moved the Air Force's course structure from a traditional learning model to a more constructive learning approach. This approach focuses on student involvement and engagement with the course material while encouraging students to incorporate past knowledge and experiences into the learning environment. The military students are allowed the

[69] Ibid.

[70] United States Army, *America's Army*.

[71] Luke Plunkett, "America's Army: Super-Effective," Kotaku, accessed November 9, 2017, https://kotaku.com/5407142/americas-army-super-effective.

[72] Fil Arenas and Andrew Stricker, "Gamification Strategies for Developing Air Force Officers," *Learning Solutions Magazine*, June 17, 2013, https://www.learningsolutionsmag.com/articles/1190/gamification-strategies-for-developing-air-force-officers.

[73] Ibid.

opportunity to “process information to knowledge” and incorporate that knowledge into action as agile and adaptive leaders.[74]

The U.S. Army Program Executive Office for Simulation, Training, and Instrumentation displayed its desire for an increase in gamification in military education and training by seeking interested vendors in a paper titled “Games for Training (GFT) Next Generation Game (NGG).” The priority is to find companies able to provide games to be used in training programs. The Army seeks to use gamification for individual and small unit training, and they are looking for games available to support training on various platforms ranging from web-based to personal computers to augmented reality gaming machines. The use of gamification allows for immersion in a shared environment, similar to wargaming, and is used for a much larger group. The use of games in training is beneficial because it provides a cleaner, faster, and more cost-effective way to train Soldiers.[75]

D. EXAMPLES OF USES FOCUSING ON CYBER

Mackenzie Adams and Maged Makramalla conducted a review of the gamified training solutions capable of developing cybersecurity skills in employees, focusing on the level of awareness, defensive strategies, offensive strategies, and attacker centricity.[76] For each game, they determined whether the game included elements of each of the four categories. The most common awareness provided focused on basic knowledge. The analysis of defensive strategies determined that the focus was penetration. There was not a common offensive strategy, but topics addressed included passwords, capture the flag, and system penetration. The last category considered was attacker centricity with the majority of games not addressing it; however, two games displayed limited attacker centricity. The gamified examples considered include CyberCIEGE, CyberNEXS, Cyber Protect, NetWars, and Micro Games.[77]

[74] Ibid.

[75] Heong Weng Mak, “U.S. Army Begins Search for Next-Gen Game Based Training,” Gamification Co, September 30, 2015, http://www.gamification.co/2015/09/30/u-s-army-begins-search-for-next-gen-game-based-training/.

[76] Mackenzie Adams and Maged Makramalla, “Cybersecurity Skills Training: An Attacker-Centric Gamified Approach,” *Technology Innovation Management Review* 5, no. 1 (2015): 7.

[77] Ibid.

Gamification has been used in the training of a number of different types of cybersecurity. The development of Kaspersky Interactive Protection Simulation (KIPS) is a prime example of how gamification supports cyber related education or training. KIPS is developed to increase the enthusiasm of employees during cyber security awareness. The use of KIPS has been viewed as a shortcut to learning. The user feedback supports the continued use of gamification during cyber education. The feedback from users shows that over 90 percent use the knowledge and would recommend the use of KIPS to their colleagues. The success of the program is contributed to factors common to gamification such as interactivity, learning-by-doing, customized games that foster fun and competitive interaction between employees.[78]

Customization is an important factor in the gamification of cyber education because not all employees require the same skill level or the same topical knowledge based on their role in the organization. A similar use of customization would be required in gamified versions of cyber training in the military. According to Slava Borilin, the host of the game, “KIPS is a tool that we use to teach the decision makers about the role of cyber security and to convince them that they need to allocate money and time for management and employees learning about cybersecurity.”[79] KIPS could be used differently when educating top management, information technology specialists, and middle/line managers. The use of gamification in the military would require a similar level of customization based on the different levels of experience with the topic and military specialty.

The gamification of cyber allows players to have an opportunity to learn and experiment in a safe environment, because “it is better to fail in the simulated environment than face the same attacks in real-life and be unprepared for them.”[80] In a serious cyber game, there must be a balance between the game being too easy and too difficult. There must be enough difficulty that the player is able to experiment and learn during multiple iterations of the game. This balance will ensure that players remain interested in the game. If it is too easy and the player is able to win in a single round, they may become bored. The other scenario would be if it were too difficult, causing the player to fail repeatedly and resulting in players becoming disengaged. As

[78] Zeljka Zorz, “Cybersecurity Gamification: A Shortcut to Learning,” Help Net Security, December 8, 2016, https://www.helpnetsecurity.com/2016/12/08/cybersecurity-gamification-shortcut-learning/.

[79] Ibid.

[80] Ibid.

noted by Borilin, “During the training, people must have several opportunities to make mistakes, try out different actions, and elaborate a successful solution before the training ends.”[81]

1. CyberCIEGE

In 2004, the Naval Postgraduate School designed and developed a single-player-only 3D simulation game called CyberCIEGE, where the player has to make choices between their office’s cyber policy and operability to maintain or increase the company’s overall profit.[82] This serious game requires the user to find a balance between protecting the user and network from internal and external threats while maintaining high productivity and operability. In CyberCIEGE, the players decide what computer or network assets—such as firewalls, virtual private networks, servers, operating systems, physical security measures, biometrics, and software applications—to use and the best ways to implement these assets to accomplish the mission in each given scenario. Players learn through opportunity, either success or failure, by interacting with non-playable characters (NPC) to work through a cybersecurity issue and implement an idea of what constitutes as a solid cyber security posture using the financial resources they have on hand. If the player fails to obtain a balance in the security and operability requirements for their office before going into debt, such as in one case where a malicious actor infiltrates the network and steals valuable company secrets because of poorly implemented security and network controls, then the player is prompted to play the mission again.

The level of detail in each scenario of CyberCIEGE—ranging from configuring simple security settings in routers, firewalls, and personal computers to designing and managing multiple network enclaves which use advanced security access controls such as authentication using Public Key Infrastructure (PKI) cryptograph and device and network logging—can be overwhelming to players of a non-technical background. However, the campaigns of CyberCIEGE do allow the player to progress from the “basic” or starter levels to the more advanced “expert professional” scenarios.[83] CyberCIEGE also has the ability to create custom scenarios to teach specific topics in cybersecurity. CyberCIEGE, as an educational tool, is geared

[81] Ibid.

[82] *CyberCIEGE*; Thompson and Irvine, “CyberCIEGE: A Video Game for Constructive Cyber Security Education,” 2.

[83] Christopher Herr and Dennis M. Allen, “Video Games as a Training Tool to Prepare the Next Generation of Cyber Warriors,” *Software Engineering Institute*, July 2015, 13, https://doi.org/10.1145/2751957.2751958.

more toward the experienced network technician, information assurance (IA), security professional, or students in these career fields with prior background knowledge in network systems. Besides being granular in its educational scope, CyberCIEGE is also very linear in design. When a player is presented with an objective or problem, the game will only display mission success if and only if the player solves the IA problem with a specific set of actions; otherwise, the player will fail the mission. This linearity is a limiting factor in the simulation environment of CyberCIEGE because alternate methods to solving an IA issue, if not programmed in the scenario, are not allowed as acceptable milestones to progress the player to the next objective. Finally, CyberCIEGE is only available for the Windows operating system with Microsoft DirectX and is played entirely on a standalone PC system.

2. CyberStrike

CyberStrike and CyberStrike Advanced are on opposite sides of the spectrum when compared to CyberCIEGE.[84] These games were also developed at the Naval Postgraduate School and their purpose is to teach a highly-abstracted view of cyber operations and strategy in an interactive and socially engaging manner. CyberStrike is a turn-based multiplayer game in which six players take on the various roles of state and non-state cyber actors and use a basic cyber strategy—by increasing their attack, defense, and attribution points each round—to acquire the victory points. Each role has a different objective and incentive structure to win the game. Each role also has differing strengths and weakness to start the game; this is intended to represent the group strengths of different roles such as the nation state, terrorist, criminal, and hacker groups. The first player that hits the maximum amount of victory points wins the game. The only modifiers in the game are in the form of stability points, which represent the infrastructure of the three nation state actors, and of which the players have to keep these stability points as high as possible throughout the game. CyberStrike is an excellent icebreaker for students in laboratory sessions and cyber introduction courses because of its ability to bring students together in a low-pressure environment and help them gain a basic understanding of what to expect in the cyber course. CyberStrike allows for flexible game play, meaning games are played as fast or as slow as the players allow, and each player can act on their own play strategy within their chosen role. Another benefit of CyberStrike is that the game is played using a web browser (e.g. Chrome,

[84] *CyberStrike - GlobalECCO*.

Safari, Firefox, and Internet Explorer/Edge), which allows for players to play the game regardless of what operating system or device they use.

III. DESIGN AND DEVELOPMENT OF CYBERWAR: 2025

A. HOW CYBERWAR: 2025 IS DIFFERENT

Our major goal throughout the development process of *CyberWar: 2025* was to make an interactive wargame that balances both the serious games style of CyberCIEGE and the engagement and entertainment value of CyberStrike. *CyberWar: 2025* is intended to be used as a tool to support education and training of cyberspace operations to entry-level military professionals and other DOD personnel. What distinguishes this wargame from CyberCIEGE and CyberStrike is its reinforcement of key learning objectives, concepts, and vocabulary addressed in DOD training and doctrine. The relationship of how these learning objectives and doctrine are tied to the actions in CyberWar:2025 is described in Appendix C. The focus on doctrine and doctrinal training is what makes this wargame a serious game; however, to maintain player engagement and motivation, we decided that *CyberWar: 2025* needed to have real multiplayer interaction. By introducing a live player element in this wargame, we gave players the ability to learn from their mistakes as well as each other, through the means of unique player-on-player interactions.

We designed *CyberWar: 2025* to be an even playing field by not enabling the element of player roles, strengths, and weaknesses as in CyberStrike. However, we also designed *CyberWar: 2025* to allow for two levels of randomization, which means that no two games will ever be the same and that each game will have its own internal challenges based on the skill level and actions made by the players. From an external view, player interaction, gamer play styles, and the unique player strategies are true random elements of the wargame. The dice roll function, which is the main probability function and orders the adjudication system, constitutes the internal mechanics of *CyberWar: 2025*. It is completely invisible to the player, randomize the wargame in ways we can directly observe. We can set or modify these mechanical elements to improve or shape the wargame to meet specific requirements or learning objectives.

We argue that by not assigning player roles in the game like in CyberStrike, each player is freely able to make their own choices to support their cyber strategy. This enables players to experiment with different strategies in each new round of the game and find out what cyber strategy works best with for them. We believe the educational value behind balanced and "roleless" mechanics will allow instructors to engage with students directly on what player strategies worked or did not work after the conclusion of a game; enabling players to directly associate and discuss both the actions of the cyber effects they used and the timing of those effects during each round of the play session.

B. CYBERWAR: 2025 LEARNING OBJECTIVES

The learning objectives of *CyberWar: 2025* are based on our desire to support an educational course currently in use to train and educate staff members on cyberspace operations. We conducted an assessment of the Terminal Learning Objectives (TLOs) of ALCOC to determine and prioritize which ones would be best suited for inclusion into our wargame. The result of the prioritization allowed us to focus on the TLO most suitable for *CyberWar: 2025*. These learning objectives and their relationship within CyberWar:2025 are covered deeper in Appendix C.

Those Terminal Learning Objectives and Enabling Learning Objectives (ELOs) are

- Understanding the fundamentals of cyberspace operations,
- Understanding cyberspace threats,
- Targeting in cyberspace,
- Providing intelligence support to cyberspace operations, and
- Understanding defensive and offensive cyberspace operations.[85]
- Understanding cyberspace as a domain,
- Understanding cyber threat actors,
- Understanding High Value Target List (HVTL) and High Payoff Target List (HPTL),
- Understanding cyberspace infrastructure and key terrain, and

[85] "Terminal Learning Objectives" May 2017.

- Describing OCO/DCO actions and effects.[86]

C. SCOPING AND GAMIFYING THE CYBER PROBLEM

Cyberspace is large, vastly indeterminate, rapidly changing, and exponentially growing, with the mass influx of Internet connected devices coming online each day. In 2015, there were approximately three Internet-connected devices per person; however, in 2017, that number is nearing five including devices such as cars, televisions, and even household lights. Even though these devices are broken down into smaller, more manageable networks, they can still easily talk to each other with little or no delay in the network connectivity. According to the Department of Defense Joint Publication (JP) 3–12(R), cyberspace

> consists of many different and often overlapping networks, as well as the nodes (any device or logical location with an Internet protocol address or other analogous identifier) on those networks, and the system data (such as routing tables) that support them. Cyberspace is described in terms of three layers—physical network, logical network, and cyber-persona.[87]

These layered and overlapping networks create a convoluted sense of how we understand cyber and cyberspace. Network connected devices in cyber present a huge challenge because the data generated from these is tracked, analyzed, and stored, but the shortfall is that there is no one to one relationship between a device in cyberspace and its location in the physical domain. The major drawback with this missing link between the digital and the physical is that entities in cyber are not tactile and thus cannot be observed easily. On top of that, cyberspace has its own set of terminology and definitions, which describe the several different types of cyber functions, effects, and operating environment. This jargon such as the cloud, distributed denial of service (DDoS), hacking, dark net, botnet, worms, malicious code, and advanced persistent threat (APT) are a combination of the effects that cyber can inflict and that of current trends and buzzwords. The problem with cyber is it is unequivocally confusing considering the combination of network complexity, verbiage, its intangibility, and the growing rate of change of the domain and how it is perceived by the general populace.

[86] "Enabling Learning Objectives" May 2017.

[87] Department of Defense, *Joint Publication 3–12 (R) Cyberspace Operations* (Department of Defense, February 5, 2013), I-3, http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf.

When creating simulations, the majority of game designers and developers use what they observe in the real-life execution of the tasks through tactile means, structure those observations into learning objectives, and then recreate that environment within a virtual world. Game developers reengineer their experiences from what they feel and transform that feeling to something more tangible, so that a player can grasp or understand those same experiences.[88] Since cyberspace is so vast, complex, and cumbersome to observe, the ability to gather these observations and structure them into experiences becomes rather difficult. One method of approaching cyber gamification is to break cyber down into specific subsets to build and simulate certain learning objectives. These learning objectives are what make up the mechanics, otherwise known as the ruleset, and dynamics, the run-time behavior based on player input, of a game.[89] It is a common business practice for game designer and developer studios to tailor their games and gaming experience to a specific target audience, because it is absolutely impossible to build one simulation that encompasses everything. These studios research, design, develop, and test to find the equilibrium that meets the preset requirements for their product. In the case of cyberspace operations, should the software be more technical and simulation based—focusing on specific tasks such as command line execution of tools, policy planning and implementation, or building system components and networks—or should the software be more abstract and high level, focusing on the big picture, such as strategy? The balance in gamification of any simulation should be focused on the methods in delivery of learning objectives: technical and rigid or fun and entertaining. One may argue that a fun and entertaining method of delivery has a high level of replay; however, the apparent downside with this could be reduced retention of the learning objectives. Bear in mind that the scope of a cyber simulation should be constrained to a specific subset of themes or key areas of all that currently encompasses cyber, because it is from those keys areas that the learning objectives originate and limiting the amount of these learning objectives allows the player to focus on the dynamics and mechanics of the game without becoming inundated and frustrated with too much information.[90]

[88] Jesse Schell, *The Art of Game Design: A Book of Lenses*, Second edition (Boca Raton: CRC Press, 2015), 11.

[89] Robin Hunicke, Marc Leblanc, and Robert Zubek, “MDA: A Formal Approach to Game Design and Game Research,” *Press*, In Proceedings of the Challenges in Games AI Workshop, Nineteenth National Conference of Artificial Intelligence, 2004, 5.

[90] Ibid.

When gamifying cyberspace operations, designers must balance between the constructive learning objectives and players' cognitive learning ability and motivations.[91] Considering that the motivations of the each of the players will be different, it is imperative to stimulate the players' motivations in such a way that increases the replay value of the game, as well as the retention of the learning objectives. Abstraction and realism are the most important aspects when designing and developing a game for cyber education. Since cyberspace is complex, it is paramount that the designers extract the most important elements of cyber to reinforce in the development of the game and present those concepts in a simplistic way that the player will understand. Policy, doctrine, best practices, historical case studies, and credible scenarios provide the realism aspects of a serious game and this realism reinforces the learning objectives with which the player can identify.

To urge the player further into the simulation, the designers and developers need to easily present the learning objectives and information in a way that is aesthetically engaging to the player. Aesthetics tie the player to the learning objectives of the game by evoking a level of emotional response in the player.[92] This emotional response is evoked through something as simple as a player avatar or recognizable board designs like chess or checkers. It is through aesthetics that players become familiarized to the game mechanics and dynamics, which, in turn, keep the player invested during play. How a cyber simulation should look and feel aesthetically are the purely the responsibility of the development team, although feedback from players, game testers, and subject matter experts are highly encouraged when solidifying the user interface, as well as reinforcing the validity of the game. Finally, developers should also focus on what type of platform, such as web-based HTML5 model view controllers or standalone 3D game processing engines, best meets the end requirements of the software product.

D. METHODS USED IN DEVELOPMENT

The process of designing a serious game is more of an art than a science. That said, there are fundamental steps that we used in the development of *CyberWar: 2025* that are commonly used by experts in the field of wargaming. Designers of wargames bring different talents to

[91] Hussain and Coleman, *Design and Development of Training Games*, 128.

[92] Hunicke, Leblanc, and Zubek, "MDA: A Formal Approach to Game Design and Game Research," 2.

develop a quality wargame.[93] We blended the frameworks and principles published by the widely known and respected Peter Perla and James Dunnigan as well as HG Wells' book *Little Wars*.[94]

James Dunnigan published a ten-step process in his book titled *The Complete Wargames Handbook*. The steps are as follows: concept development, research, integration of ideas into a prototype, fleshing out the prototype, first draft of rules, game development, blind-testing, final rules edit, production, and feedback.[95] Dunnigan used this iterative process to produce a number of games. His process focused on incremental processes in an attempt to not get trapped working on the details for too long by trying to produce the elusive "perfect game."[96] Peter Perla's steps for creating a wargame were published in *Wargame-Creation Skills* and the *Wargame Construction Kit***.** The steps are as follows: specify objectives; identify players, roles, and decisions; collect information the players will need to make decisions; devise tools to make the game work; document the result of the effort; validate model data and scenario, playtesting, and blind testing; prepare the final rules, execution of the game, and feedback and analysis.[97]

In addition, serious games also need to work around the mechanics, dynamics, and aesthetics (MDA) framework.[98] The MDA framework is what builds the bridge between the designer/developer and the player. Strong core mechanics provide the driving force of the game.[99] Dynamics focus on the challenge of the game, such as levels of random events or unpredictability, which assist in creating replay value and provide feedback to the player.[100] Finally, aesthetics are the visual aspects within the game that connect the design value of the game to human emotion and player experiences.[101] The MDA framework is easily tied to its lay

[93] Perla, *The Art of Wargaming*.

[94] H. G. Wells, *Little Wars* (Dodo Press, 2009).

[95] James F. Dunnigan, *The Complete Wargames Handbook: How to Play, Design, and Find Them*, Revised, Subsequent edition (New York, N.Y: Quill, 1992), 111.

[96] Perla, *The Art of Wargaming*.

[97] Ibid.

[98] Hunicke, Leblanc, and Zubek, "MDA: A Formal Approach to Game Design and Game Research," 1.

[99] Schell, *The Art of Game Design*.

[100] Hunicke, Leblanc, and Zubek, "MDA: A Formal Approach to Game Design and Game Research," 1.

[101] Ibid.

counterparts in the form of rules, game, and, ultimately, fun.[102] Game mechanics create the rules and form the boundaries of the game. These rules set the scope and challenges that the player must understand, and these challenges are the objectives from which the player learns to gain further experience or knowledge on a subject.

E. DESIGN OF CYBERWAR: 2025

The progression of designing and developing serious or educational games is a methodical and sometimes chaotic process. For this project, we, as the authors, had a nine-month time window to design, develop, and produce a rough beta version of the wargame in software. We designed this game to be an influencer for all branches of the DOD and their subordinate cyber fields, as well as an educational tool for decision makers and leaders on cyber policy. *CyberWar: 2025* went through four separate phases during the design and development. In each of these phases, we encountered different challenges, which in the end resulted in the final software product of the wargame. Although these challenges, such as reducing the wargame complexity and how we can improve upon reinforcing the learning objectives during gameplay, were temporary roadblocks in the complete design and development process of the wargame, they were necessary in order to prove the validity and educational value of *CyberWar: 2025*. We argue that this interactive wargame has not yet been fully developed to its complete potential, and that this beta version of *CyberWar: 2025* can be a stepping stone to future versions. In this regard, it should be used as a platform to advance the education of cyberspace operations and cyber conflict in the future.

During the initial design stages of *CyberWar: 2025*, the topics of player learning objectives, game framework and structure, player interaction and motivation, possible strategies and outcomes, and game mechanics were constantly in flux. As a team of two for this project, our initial process was to lay the foundation of the cyber wargame with as much detail about the development plan of *CyberWar: 2025* as we could at that time and then modify, add, or remove items as needed later. Using the ADDIE system—analysis, design, development, implementation, and evaluation—during the thesis proposal stage, we set an initial mechanics, dynamics, and aesthetics framework for *CyberWar: 2025* knowing that some of these elements

[102] Ibid.

within this framework might change during the research and initial design phase of the wargame.,[103]

F. INITIAL DESIGN PHASE

Player interaction and motivation, their background knowledge about cyber, the overall learning objective guidelines we wanted the player to understand, and how an organization could use this interactive wargame as a teaching tool were top priorities in the early design phase of *CyberWar: 2025*. The purpose of *CyberWar: 2025* was to create an educational training aid for entry-level Army Cyber training courses. Our preliminary efforts were spent on focusing on which cyber-specific learning objectives and guidelines we wanted the students of these courses to understand, since the majority of personnel attending these courses most likely will come from non-technical backgrounds with no prior knowledge of cyberspace operations. Our main goal, in support of the overall learning objectives, was to keep the player motivated and engaged in the wargame by maintaining a high level of user interaction and stimulation. In short, we envisioned that *CyberWar: 2025* should not be like the Cyber Awareness Challenge or any annual online mandatory training module.[104] With this in mind, our initial design of *CyberWar: 2025* was to be a two-dimensional top-down rectangular board, and inside that board were hexagonal points from which the player would be able to maneuver a full 360 degrees from point to point. These hexagonal points represented the open cyberspace domain. On top of that, the player domains were a small subset area on this board, and each player's position, or domain, on the board was randomized.

[103] Hussain and Coleman, *Design and Development of Training Games*, 9; Hunicke, Leblanc, and Zubek, "MDA: A Formal Approach to Game Design and Game Research," 1.

[104] United States Army Cyber Center of Excellence, "Information Assurance Training Center," 2017, https://ia.signal.army.mil/dodiaa/.

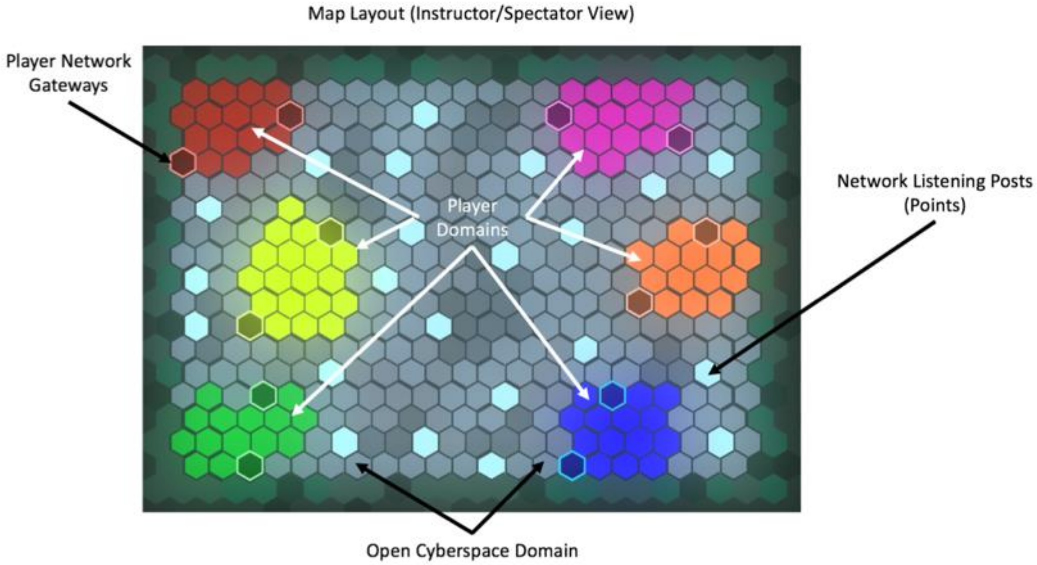

Map Layout (Instructor/Spectator View)
Player Network Gateways
Player Domains
Network Listening Posts (Points)
Open Cyberspace Domain

Figure 2. Initial Board Design

Inside each player domain was a small network infrastructure that modified the player’s cyber effects and attributes, much like buildings and structures modify resource acquisition and usage in a manner similar to the popular strategy game, Age of Empires.[105] Players would have to maneuver around cyberspace from their local domain to nearby players’ domain via network listening posts, or capture points in this case, and ultimately gain territory or intelligence to improve the player’s overall cyber posture. To envelop the player further into the game, the player is also assigned a background story, assuming the role of a commanding officer on a cyberspace operations watch floor whose mission is to seek out unknown actors in cyberspace—the other players—and assess their threat potential and vulnerabilities while protecting their own cyber related assets such as access points, research servers, and intelligence databases. This version used a budgetary and resources management element, which was gained through intelligence collection from opposing players, as the driving motivation for players to advance their cyber tools and effects to improve their chances of success against opposing players in this simulated version of cyberspace operations. Time was also a limiting factor in cyber tool/effect research and development. This was an important element because we wanted decision makers and cyber planners to understand that development and research of cyber effects do not happen

[105] Microsoft Studios, *Age of Empires* (Redmond, WA: Microsoft Studios, 1997), https://www.ageofempires.com/.

overnight. Therefore, players would have to balance their strategy with their resource management and timing carefully, because if they used all their resources, lost too much intelligence, or did not implement proper cybersecurity measures, they would be overtaken by other players and removed from the game. Unfortunately, considering the massive amount of complexity in both design and mechanics for the initial version of *CyberWar: 2025*, we decided it was best to restructure and simplify the wargame to a more practical level.

1. Redesigning and Refining

Taking the lessons learned from the draft version of *CyberWar: 2025*, as well as researching and evaluating the MDA framework of other successful games such as CyberStrike, Diplomacy, and chess, we realized that a reduction in the wargame's complexity was absolutely necessary. We wanted to mimic and incorporate into *CyberWar: 2025* the ease of play and overall game flow of CyberStrike, the turn-based mechanics and communication structure of Diplomacy, and the "easy to play but difficult to master" impression that chess delivers. Gamifying cyber meant taking specific elements from the overall problem of cyberspace training and understanding and presenting that problem in a manner that induces an engaging behavior with the players while educating them at the same time: this meant redesigning a large part of the MDA framework of *CyberWar: 2025*. Our initial version of the wargame had too many design elements at the macro and micro level that convoluted the overall mechanics, which ultimately obfuscated the learning objectives. We realized that in order to make a successful product that reflected our stated learning objectives to our target audiences, we had to drastically reduce the sophistication of *CyberWar: 2025* in the MDA framework areas such as user interaction and movement complexity, while at the same time reinforcing the learning objectives and maintaining a level of player enjoyment and excitement.

2. Reduction in Game Complexity

In simplifying the game, we redesigned the board mechanics to mimic that of the games of Othello and Wei-chi, where players have a restricted number of spaces to which they can move and occupy on a predefined game board based on the ruleset in order to implement their strategy. However, there are multiple paths available to the player that they can control to gain territory, meaning the players have to capture points adjacent to their own points to occupy territory in order implement their own player strategy and achieve their goal. With Othello and Wei-chi, the play area of these games is a limited square board that can only accommodate two players. We wanted *CyberWar: 2025* to support this style of adjacent point control while at the same time becoming a multiplayer game of six players. Therefore, the board took the shape of a hexagon, which allowed us to implement a set amount of points on the board as major sources of contention while restricting the players' movement to a limited number of spaces available. This restricted amount of playable space reduced movement complexity by eliminating neutral space from the initial design, as well as denying players the ability to isolate themselves from territorial conflict. At the macro level, the redesigned board is a simplified model of cyberspace, because of the network is made up of 48 inter-connectable server nodes and the six additional player bases. These server nodes and player bases were static on the board, and the only randomization in the wargame was the player's physical location, which is determined by the player avatar they selected at the start of every game.

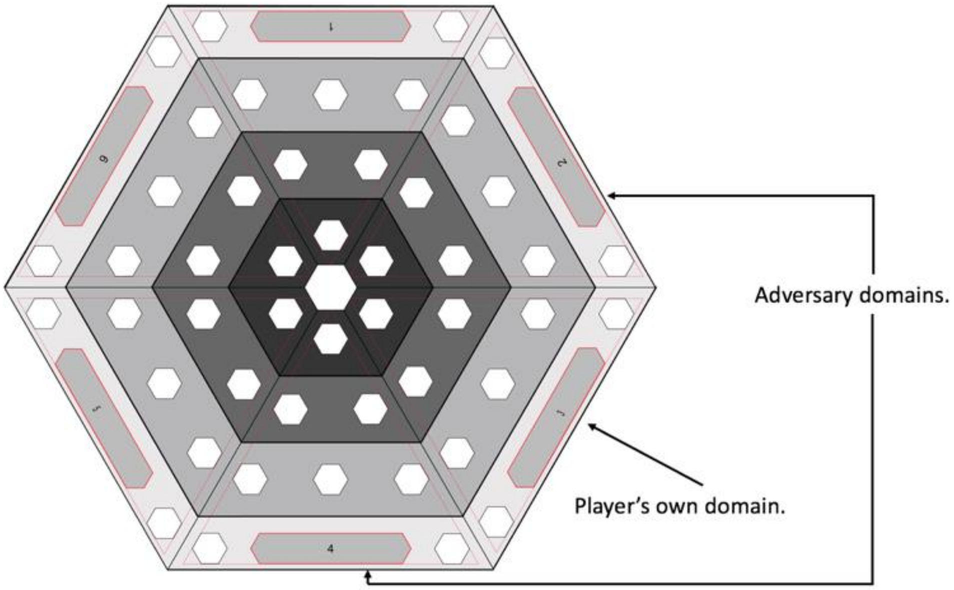


Figure 3. Redesigned *CyberWar: 2025* Board

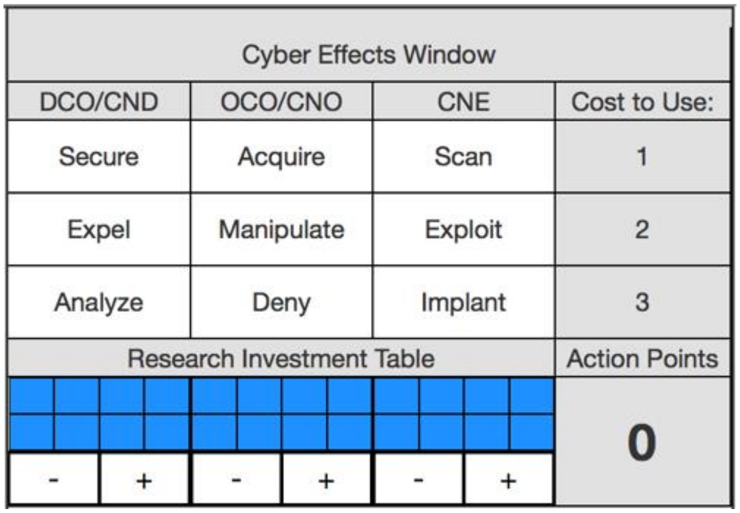
Out of the six total triangles in the hexagon, a single triangle represents a single network, otherwise known as the local domain, of server nodes, or the eight smaller hexagonal points that belong to one player. The remaining five triangles, or foreign domains, belong to the opposing players. We wanted to demonstrate the idea of local cyber threats to the player, through the close proximity of the two foreign domains on their left and right sides. These close proximity players could impact the player's domain and immediate cyber strategy. This designed allowed adjacent players the ability to cross over horizontally to an opposing player's territory via the inter-domain lines on the board; however, all players can access each other's domains easily through the server nodes in the center of the board.

Internally on the board, there are tiered levels going from Tier 1 at the center to Tier 4 at the outer edge. The player's own base resides in Tier 4 along with the only two directly connectable server nodes. At the Tier 1 level, players can jump to any other Tier 1 server point with a cost of one action/research point and the cost of the cyber effect, whereas at the Tier 4 level, players can only control their nearby opponents' servers with a cost of four action/research points on top of the cost of the cyber effect. The reason behind this increased cost at the Tier 4 level is to discourage players from attacking opponents' bases in the initial rounds of the game—reducing the effect of "base camping," which is a common and disreputable tactic in most real-time strategy and first-person shooter multiplayer games—and to keep the players focused on the servers, or the main points of contention, in the center of the board.

3. Cyber Effects Window and Research Investment Table

In *CyberWar: 2025*, our goal was to adhere our cyber effects closely to DOD naming conventions and definitions as stated in the DOD JP 3–12(R) and DOD Dictionary of Military and Associated Terms.[106] However, a few of our cyber effect names were not documented in either publication; therefore, we had to develop explanations for these undocumented effects based on best practices from professional experience and common usage terminology. In the initial design stages of *CyberWar: 2025*, the research tree consisted of approximately 20 cyber effects broken down in to the three major categories of attack, defend, and exploit. Many of these effects had overlapping attributes; therefore, a consensus to reduce the 20 tools down to nine specific cyber effects, three per each effect category of DCO, OCO, and CNE, was necessary in the development phase of the game to reinforce the learning objectives with *CyberWar: 2025*.

[106] Department of Defense, *Joint Publication 3–12 (R) Cyberspace Operations* (Department of Defense, February 5, 2013), http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf; Department of Defense, "DOD Terminology Program," 2017, http://www.dtic.mil/doctrine/dod_dictionary/.



Cyber Effects Window			
DCO/CND	OCO/CNO	CNE	Cost to Use:
Secure	Acquire	Scan	1
Expel	Manipulate	Exploit	2
Analyze	Deny	Implant	3
Research Investment Table			Action Points
- +	- +	- +	0

Figure 4. *CyberWar: 2025* Cyber Effects and Research Investment Table

By capturing a server node in the game, either overtly or covertly, one action/research point is gained which allow players to either launch a cyber effect or invest into the research table to produce more powerful cyber effects. However, action/research points earned at the start of each round do not carry over to the next round. We designed the action/research points system in this manner to encourage players spend their points before the ending each round and to prevent the hoarding of action/research points for later use in the wargame. At the start of the game, the base level of cyber effects (secure, acquire, and scan) is immediately unlocked and ready for use by the player. To unlock additional effects, the player has to invest four action/research points per cyber effect level. To completely unlock one category of effects, a total of eight points is needed. By implementing the research table from row levels one to three, the player has to invest their acquired action/research points in the research table area that corresponds with their cyber strategy, to compete effectively against the other players.

Our idea of the research table closely mirrors that of the research card meter system used in CyberStrike Advanced. In CyberStrike Advanced, a player may invest a number of points into various research items such as an attack, defend, detect, sabotage, and investment card before that card is placed in their arsenal to play as an action in the next round. These cards are the foundation of a player’s strategy along with the player’s chosen role in the CyberStrike. With the cards and depending on how or when they are played, a player can either launch offensive cyber-attacks or defend against incoming ones.

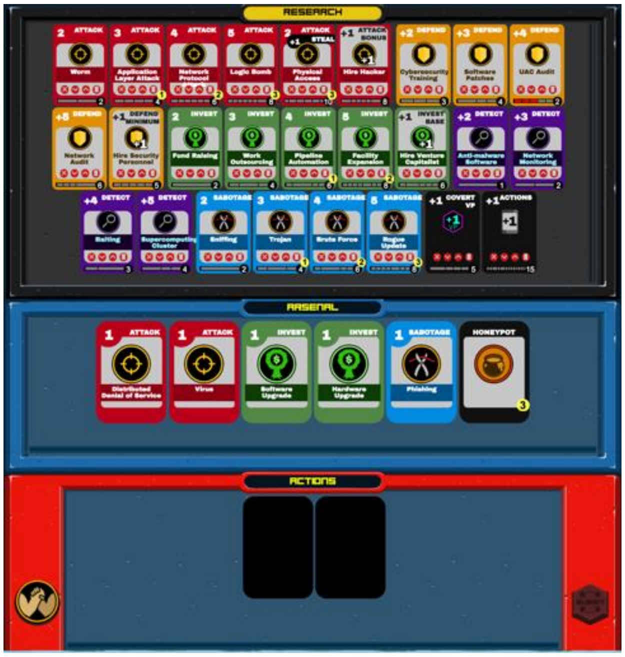

RESEARCH
2 ATTACK Worm
3 ATTACK Application Layer Attack
4 ATTACK Network Protocol
5 ATTACK Logic Bomb
2 ATTACK +1 STEAL Physical Access
+1 ATTACK BONUS Hire Hacker
+2 DEFEND Cybersecurity Training
+3 DEFEND Software Patches
+4 DEFEND UAC Audit
+5 DEFEND Network Audit
+1 DEFEND MINIMUM Hire Security Personnel
2 INVEST Fund Raising
3 INVEST Work Outsourcing
4 INVEST Pipeline Automation
5 INVEST Facility Expansion
+1 INVEST BASE Hire Venture Capitalist
+2 DETECT Anti-malware Software
+3 DETECT Network Monitoring
+4 DETECT Baiting
+5 DETECT Supercomputing Cluster
2 SABOTAGE Sniffing
3 SABOTAGE Trojan
4 SABOTAGE Brute Force
5 SABOTAGE Rogue Update
+1 COVERT VP
+1 ACTIONS
ARSENAL
1 ATTACK Distributed Denial of Service
1 ATTACK Virus
1 INVEST Software Upgrade
1 INVEST Hardware Upgrade
1 SABOTAGE Phishing
HONEYPOT
ACTIONS

Figure 5. CyberStrike Advanced Play Area[107]

As the player increases in investment points, they can also increase the number of points they can place into research for better cyber effects or personal card actions. By implementing a minimalistic version of research and resource management from the initial design of *CyberWar: 2025*, we were able to still support the idea of how important research and development of cyber effects are to a player's success when executing their cyber strategy.

4. Employment of Exploitation Effects and Strategy

The JP 3–12(R) focuses on OCO and DCO as the primary methods of cyberspace operations; however, computer network exploitation is an "intelligence collection and Information Operations related activity" and is "not viewed as an integral pillar of DOD Information Operations doctrine."[108] In the design phase of *CyberWar: 2025*, we believe it is important to include CNE because of the several cyber related events that have taken place since 2007. Our incorporation of CNE as a primary method of executing cyber effects, next to OCO

[107] *CyberStrike Advanced - GlobalECCO*, Web (Monterey, CA: Naval Postgraduate School, 2011), https://globalecco.org/play.

[108] Central Intelligence Agency, *Information Operations and Intelligence Community Related Activities*, Director of Central Intelligence Directive 7/3. (Central Intelligence Agency, July 1, 1999), 4, https://fas.org/irp/offdocs/dcid7-3.pdf.

and DCO, was a means to present an argument that cyberspace operations should not be solely restricted to attack and defend methodologies. Even though OCO and CNE are closely related, the separation of the two is clearly defined by the end result of their employment. Reconnaissance (scanning) and intelligence gathering are defined end results of exploitation, whereas disrupting, degrading, denying, and destroying fall directly under the purview of OCO. We argue that CNE should not be a subset of OCO, but a modifier to OCO as a viable means to effectively deliver cyber effects. Therefore, we recommend that CNE be included into the DOD doctrine because of the emerging threat of "hider/finder" actors in cyberspace.

To demonstrate this in *CyberWar: 2025*, the dominant strategy to win is to efficiently employ CNE cyber effects against opposing players. There are three main reasons why CNE is the dominant strategy. First, opposing players have to use action/research points to scan or analyze their server nodes to reveal hidden players on their network. Second, OCO and CNE effects can be launched to any adjacent server node that is covertly occupied. Lastly, any server point that is covertly occupied by one or more players is an action point gained by those players, even if an opposing player overtly controls that server point. In *CyberWar: 2025*, the CNE cyber effects we developed and defined are scan, exploit, and implant. Both scan and exploit fall into the actual classification of CNE. However, the implant effect is a hybrid between OCO and CNE because its closer relationship to that of both degrade and deny effects than that of probing and reconnaissance effects. We chose to keep implant as a CNE cyber effect because of its force multiplier ability that enables other cyber effects in the wargame such as exploit, acquire, manipulate, and deny.

G. DEVELOPMENT PHASE

1. Working Group

For the entire spring 2017 quarter, a Defense Analysis program working group met twice a week to develop, implement, test, improve, and finally solidify the ruleset and mechanics of *CyberWar: 2025*. This group mainly consisted of non-cyber background students who provided valuable feedback on our design and development of the wargame. This allowed us to tailor the mechanics, dynamics, and aesthetics of our wargame to our targeted audience and their level of understanding of cyber. The working group conducted a number of playtesting integrations to determine orders adjudication, balance, and fairness as well as designing the randomization equation depicted in chapter three (see Niels' Method in Appendix B).

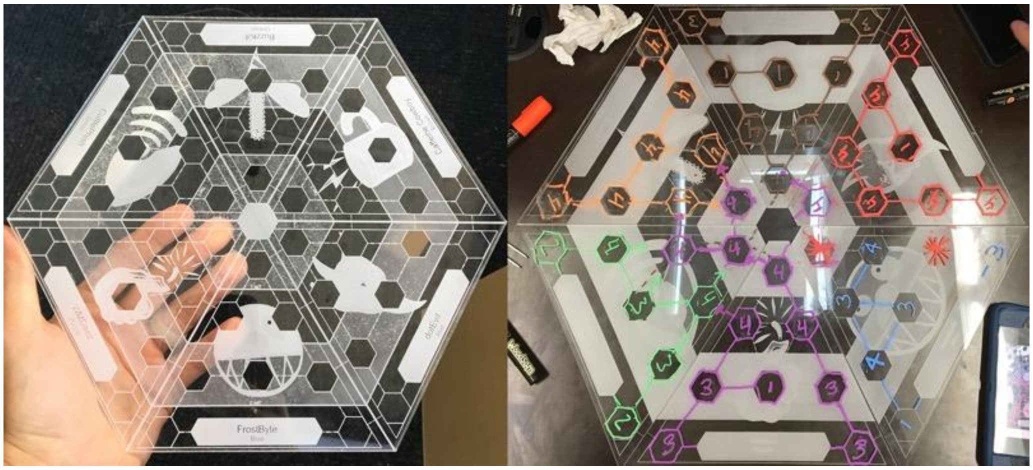


Figure 6. Acrylic Table-Top Boards

During this development process, the table-top version of *CyberWar: 2025* was physically created, cut from customized laser cut acrylic sheets at the NPS RoboDojo lab. We cut a total of six small boards and one large one out of six smaller pieces. The small boards were given to the players used as a means write their orders and maintain their view of the game state similar to that of the game Battleship. The one larger board was the observer view of the entire game state of *CyberWar: 2025*, its main use was to organize and adjudicate all of the players' orders at the end of each round. The major benefit of using acrylic boards as opposed to pen and paper was the ability update the game state on the fly and visualize it using colorful and erasable chalk ink markers. This allowed us to conduct several playtest sessions with the same hardware without having to waste time and resources.

These acrylic boards were also used at the end of the quarter in a live wargame demo where we asked students and faculty to playtest the wargame to demonstrate the effectiveness of the *CyberWar: 2025* rules and game mechanics.

2. Software Improved Gameplay

One of the major issues when playing the table-top version of *CyberWar: 2025* was the lengthy amount of time wasted per each round. In one round, we had to collect all the players' orders, note them on the observer/master board, adjudicate each order in a simulated simultaneous fashion, produce the final results of that round, and distribute those results to each of the players for the next round of orders. The approximate time for one round of play in the table-top version was upwards of five to ten minutes. This severely limited the number of rounds we could play within a one to two-hour time window. Another issue with the table-top version was with human error in adjudicating the orders. Most errors occurred when more than one player attacked a single server node with various cyber effects. Just as many software based multiplayer games such as Diplomacy Online and Frozen Synapse have managed complex and simultaneous orders, we believe that a software version of *CyberWar: 2025* would vastly reduce the amount of time between each round and increase the overall accuracy of complex orders adjudication.[109] At the beginning of each round in CyberStrike, players analyze, decide, and execute their orders independently of each other by submitting their choices to the server that is hosting game to the players. When every player has submitted their orders, the server sorts all the player inputs, calculates each of their actions, collects the results of those actions, and then broadcasts them back to the players within a split second. This allows the game flow to move as fast as the slowest player. With CyberStrike as a model, we understood that a software based version of *CyberWar: 2025* would improve the gameplay speed, replay value, and increase player engagement with the wargame as well as other players.

3. Initial Software Development Pitfalls

After the successful live demo test of the table-top version, we started development on the software version of *CyberWar: 2025*. The initial plan for development of this wargame was to build the entire game in the C# programming language using the Unity3D game development suite.[110] However, there were a several of restrictions that dissuaded us from using Unity3D—efficient cross-compatibility and installers on various types of hardware, server/client networking, development and testing time, and final integration into GlobalECCO. Even though Unity3D supports various operating systems, the issue of installing and running the wargame on old or outdated laptops could pose potential problems in playing the wargame effectively, and

[109] Volo Media Ltd, “Web Version of the Classic Diplomacy Board Game,” Play Diplomacy Online, 2017, http://www.playdiplomacy.com/; Ian Hardingham, *Frozen Synapse: A Simultaneous Turn-Based Strategy Game / Turn-Based Tactical Game!* (Mode 7 Games, 2011), http://www.frozensynapse.com/.

[110] John Riccitiello, “Unity Technologies,” Unity3D, June 8, 2005, https://unity3d.com.

we did not want to have to develop and incorporate every end user case in to the game binary. Networking the clients, or players, to the wargame server was another major issue. We understood that for networking to happen, players would have to connect to the server's game lobby via TCP/IP addressing. This posed another problem since we would have implement the ability for the server to know its own IP address during the setup phase of the game, and then broadcast that for the remaining clients to connect to that IP address and specified port. On top of that, if there were any connection issues, the wargame would become inoperable. The issue of development and testing time has to do with Unity3D development suite's compilation times, live editing, and error checking cycle since the C# interpreter has to compile all the code and assets into a software binary, which can take anywhere from two minutes to an unknown amount. Lastly, the final release version of this software is intended to be placed on the NPS GlobalECCO servers for easy access. The majority of the games on GlobalECCO are developed using JavaScript with the AngularJS framework which allows the players to create game lobbies and play these games from anywhere in the world with only their web browser. Currently Unity3D supports a WebGL (graphics library) as an emulator in JavaScript, but because this game was designed as a 2D wargame, we had no need to use WebGL. Therefore, we shifted from using Unity3D to the already established and tested coding framework of AngularJS and JavaScript, through the previous projects from the GlobalECCO developers.

4. Web-Browser-Based Development and Implementation

The choice to use AngularJS and JavaScript was greatly influenced by the effective cross-compatibility between all types of hardware, since web browsers are widely supported on all devices, as well as the vastly improved development cycle and testing time. Raw JavaScript is not "compiled" but instead implemented as an interpretive language, which means JavaScript is interpreted "on the fly" by the web browser, along with HTML, XML, and CSS, with the exception to specific libraries like BabelJS.[111] By using strictly JavaScript and with its supported frameworks such as the MEAN web stack, it was now possible to test code changes instantly by simply refreshing the page within any standard web browser without having to recompile and run the code on every change.

[111] Babel, "The Compiler for Writing Next Generation JavaScript," 2017, https://babeljs.io/.

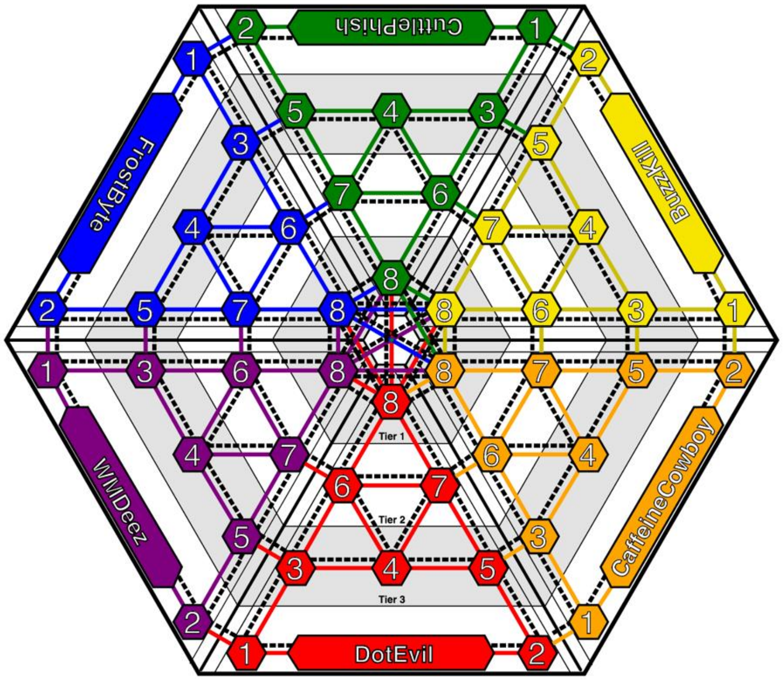


Figure 7. Final "Development" view of *CyberWar: 2025* board

The MEAN (MongoDB, ExpressJS, AngularJS, and NodeJS) is a collection of JavaScript-based technologies that, at the very minimum, can create a basic HTML web application that goes from client to server to database. From the client side to the server, AngularJS is the frontend portion of the web application that provides two-way data binding and model-view controlling (MVC) of data from the client to the server. ExpressJS and NodeJS are the lightweight frameworks that encompass the sever side execution of the web application and are completely scalable. MongoDB is a "schemaless" NoSQL database architecture that saves customizable data in JavaScript Object Notation (JSON) format, which is passed between the server and client quickly and efficiently. Along with the MEAN web stack, we also implemented a 2D HTML canvas layer from a third-party JavaScript library called KonvaJS.[112] Konva allowed us to rapidly draw on, position, and prototype the board with several interactive and callable library elements such as polygons, lines, and rectangles. This cut down development time drastically, since we did not have to manually input values and positions with the XML-based scalable vector graphics (SVG) image format. With Konva, we were able to assign our

[112] Anton Lavrenov, "Konva.Js - JavaScript 2d Canvas Library," Konva.js - JavaScript 2d canvas library, accessed October 14, 2017, https://konvajs.github.io/index.html.

board elements to variables that we could call directly in the AngularJS framework, which allowed us to easily manipulate the game and board state per client. Another library we implemented is SockJS, which is a web network socket controller library that allowed us to have multiple client instances, six in the case of this wargame, to connect to the server and be able to have low-latency and seamless network communications. Final development code and all documentation are located on the NPS GitLab repository.[113]

[113] David T. Long, "CyberWar:2025," Repository, GitLab, 2017, https://gitlab.nps.edu/dtlong/cyberwar.

IV. CYBERWAR: 2025 OVERVIEW AND WALKTHROUGH

CyberWar: 2025 is a cyber themed two-dimensional, top-down, turn-based strategy wargame simulation in which a maximum of six players will be forced to scan the cyberspace domain, hold key locations on a flat hexagonal map, defend their network from adversaries, and attack other players to gain action/research points. *CyberWar: 2025* implements a level of chance via a randomized dice roll in which the odds are calculated by the attacking and the defending server nodes' security level. The software version wargame is designed to be played with exactly six players; however, if fewer than six players are involved, the only viable and balanced options for play would be to use two or three players. Involving two, three, or six players will maintain the balance of fairness that the wargame is developed to accomplish between player interactions.

A. OBJECTIVES AND STRATEGY

CyberWar: 2025 is a game of stealth, alliances, long term strategy, and chance probability. All players in *CyberWar: 2025* are created equal in regards to their starting position and objective in the wargame. Players are not assigned specific objectives. The players must decide how they will allocate their very limited action/research points per round. Players must navigate, analyze, and maintain control of server nodes in cyberspace by overt or covert means. They are encouraged to implement their own cyber tactics and strategy within the *CyberWar: 2025*. The outcome of the wargame is determined by the decisions each individual player takes based on their own developed strategy. The overall objective of *CyberWar: 2025* is to educate or train personnel from a range of non-technical to technical backgrounds involving cyberspace operations and the cyber effect complex relationship of OCO, DCO, and CNE, as stated in the DOD JP 3–12(R).[114]

OCO intends to project power by the application of force in and through cyberspace. Similar to other offensive operations, OCO must be approved via an execute order. DCO is the implied defense of DOD and allied networks within cyberspace. These operations are either passive or active measures to protect capabilities, data, networks, and related systems.[115] CNE is

[114] Department of Defense, J*oint Publication 3–12 (R) Cyberspace Operations*, II-2.

[115] Ibid.

the enabling operations and intelligence collection capabilities that are conducted on computer networks to support other operations on a potential adversaries automated information systems or network. Intelligence capabilities are used to gain information about the target and the systems being used by potential adversaries. CNE is utilized as an enabling operation of both OCO and DCO.[116] CNE is the scanning of systems and reconnaissance that allows for future OCO and supports ongoing ODO.

B. CYBER EFFECT ACTIONS IN CYBERWAR: 2025

1. Defensive Cyberspace Operations Effects (DCO)

The *secure cyber effect* is the base action for all defensive operations. The *secure cyber effect* hardens the player's server node by increasing its defensive value against attacks. This defensive value is also used as the attack value when launching OCO and CNE cyber effects on other players. The *expel cyber effect* is a level-two cyber effect that removes any covertly hidden or exploiting players who reside on your overtly controlled server nodes. The *expel cyber effect* can also be used by exploiting players to remove other players, but not the player overtly controlling that server node; however, successful adjudication using the *expel cyber effect* from a player who is covertly on that server node will reduce the defensive level of that server node to the base value of one. The *analyze cyber effect* is the highest level cyber effect in the DCO table. The *analyze cyber effect* is a similar but more effective version of the CNE *scan cyber effect* because it can scan the player's entire network of linked server nodes to reveal any exploited players residing on the player's network. The *analyze cyber effect* also can attribute *manipulate cyber effects* to the launching attacker.

2. Offensive Cyberspace Operations Effects (OCO)

The *acquire cyber effect* cyber effect is the base action for all offensive operations. The *acquire cyber effect* captures adjacent server nodes on the map. If the nearby server node is unoccupied, acquire automatically captures that server node for the player. However, if the adjacent server node is occupied by another player, then the defensive value from the player's launching server node and the defending player's server node are factored together, along with

[116] The Vice Chairman of the Joint Chiefs of Staff, *Joint Terminology for Cyberspace Operations* (The Vice Chairman of the Joint Chiefs of Staff, November 2010), http://www.nsci-va.org/CyberReferenceLib/2010-11-joint%20Terminology%20for%20Cyberspace%20Operations.pdf.

the dice roll (see Niels' Method in Appendix B), to adjudicate who controls the contested server node. Players who lost in defending against an *acquire cyber effect* attack in their own local domain can see which player attacked them; however, if a defending player's server node is lost outside their local domain then that server node is displayed as neutral server node. Attacking players cannot acquire opposing player bases. The *manipulate cyber effect* is a level-two cyber effect that is similar to the level-one *acquire cyber effect*. The only difference with the *manipulate cyber effect* is that, if successful in adjudication and in the defending player's local domain, the attacking player can misattribute the acquire action launched and deceive the defending player as another player on the board. The *deny cyber effect* is the highest level cyber effect in the OCO table and is a permanent cyber effect which renders the attacked server node as unusable for all players for the remainder of the game. The *deny cyber effect* essentially destroys that server node on the map and further restricts player movement on the board.

3. Computer Network Exploitation Effects (CNE)

The *scan cyber effect* is the base action for all exploitation operations. The *scan cyber effect* is a reconnaissance effect that identifies adjacent server nodes' defensive value as well as any overt and covert links that are established to and from that server node. The *scan cyber effect*, when used internally of the player's domain, identifies localized threats as well as those external to the player's domain when strategizing consecutive moves. The *exploit cyber effect* is a level-two cyber effect that is similar to the level-one *acquire cyber effect* in the OCO table except that *exploit cyber effect* is a covert *acquire cyber effect*, therefore the action is not revealed to the defending player. Several exploiting players can "stack" on one server node; however, the identities of these exploiting players are not revealed until either a *scan or analyze cyber effect* has been launched by a player. Players on exploited server nodes can also launch overt cyber effects, but the attacking value is either the overt value of that server node or one, if not overtly controlled. Attacking players cannot exploit opposing player bases. The *implant cyber effect* is the highest level cyber effect in the CNE table. The *implant cyber effect* has two separate effects depending on if it is launched on a regular server node or an opposing player's base. If launched on a regular server node, then the defensive value of that server node is reduced to one, and then the attacking player can stack, or conjunctively launch, another OCO or CNE effect to gain access to that server node. If the *implant cyber effect* is launched on a base, then the effect resembles that of a ransomware attack on the defending player. When the base is implanted with the ransomware, the defending player is effectively locked out of their network and can only attempt to remove the ransomware by expelling it from their base, if the *expel cyber effect* has been researched and if the player has enough action/research points to launch the cyber effects. The ransomware effect only lasts five rounds and after those five rounds have passed, the defending player will be free of the ransomware attack and can continue play. Otherwise, the defending player either has to pay out their total amount of action/research points from server nodes they own to be free of the ransomware. Also, attacking players cannot acquire opposing player bases.

C. CYBERWAR: 2025 INITIAL SETUP AND PLAY

CyberWar: 2025 is a simultaneous turn-based wargame in which players start from their base and branch out on the game board to gain control of the cyberspace domain. One round in *CyberWar: 2025* is made up of four phases. In the first, all players submit their orders, by either executing their three cyber effects or investing in research to unlock the remaining six cyber effects; this is the only visible phase that the players see and control. The second phase is orders adjudication where the game sorts and prioritizes each of the players' submitted moves from a defender's point of view and calculates the success or failure of each order. The third phase is orders resolution, and the final phase is action/research points allocation, which counts all the positively linked server nodes that each player controls. These last two phases make up the calculated and resolved information that when displayed back to the player, starts the next round.

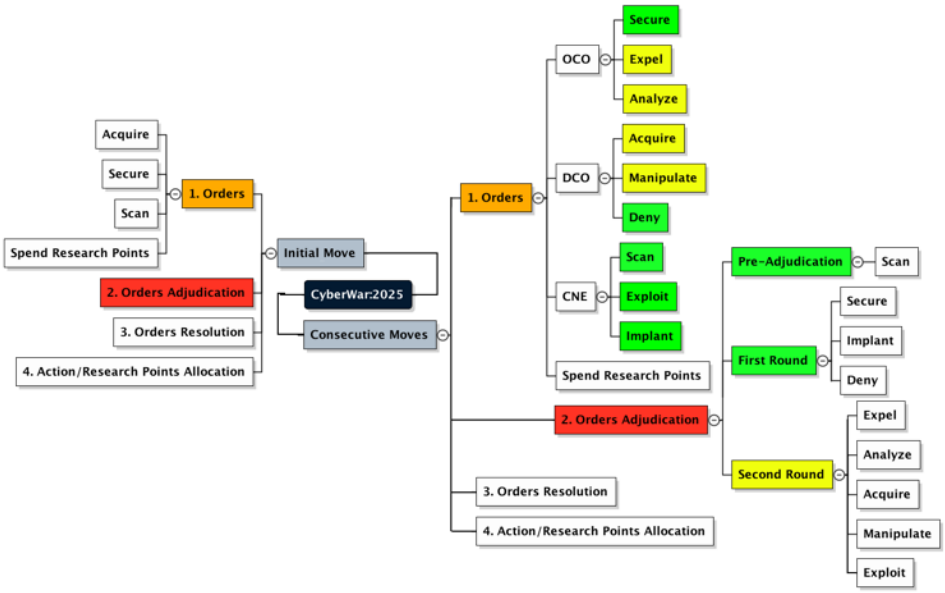
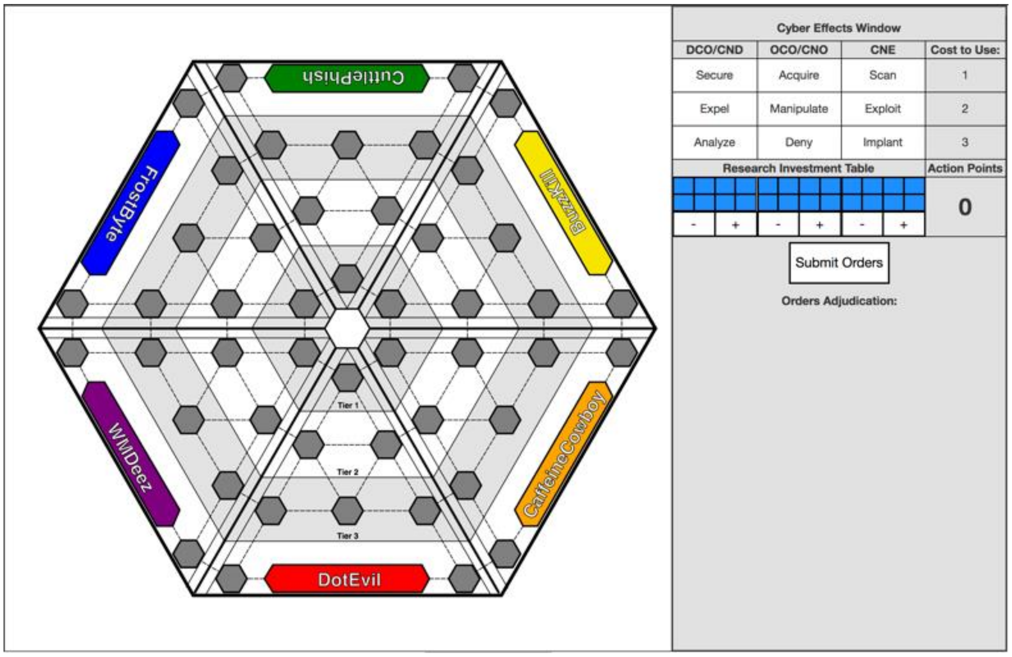


Figure 8. CyberWar: 2025 Game Flow

The players' domain is in the shape of a triangle and is comprised of a base and three tiers. The tier nearest to the base, Tier 3, contains three server nodes. The players navigate within their domain in a tiered fashion to locate and assess other players as potential adversaries or allies. Players open the game at their bases without owning any server nodes. For the opening round only, all players are provided with three points. They can use two of those points to expand to the base-level servers and can add the remaining research point to their Research Investment Table. All actions in the game cost action/research points. Players gain one action/research point from each server they have acquired or exploited that is positively linked back to their base. During the wargame, players will have to decide which effects to use based on their available resources, as well as choose what specific effects to develop in their research Investment Table.



Cyber Effects Window

DCO/CND	OCO/CNO	CNE	Cost to Use:
Secure	Acquire	Scan	1
Expel	Manipulate	Exploit	2
Analyze	Deny	Implant	3

Research Investment Table						Action Points
-	+	-	+	-	+	0

Orders Adjudication:

Figure 9. CyberWar: 2025 Main View

D. DEVELOPMENT OF ADVANCED CYBER EFFECTS CAPABILITIES

Since the structure of *CyberWar: 2025* is turn-based, the development of new technologies will require predefined resources and action/resource points, as well as a specific number of rounds for these technologies to be fully developed and deployable. The players are required to use their action/research points to unlock of the remaining six cyber effects that they are available to players during the wargame. The use of action/research points is intended to represent the resources of time and money required in the real world to develop advanced capabilities to conduct cyberspace operations. Players will have to focus on a small segment of the effects in the domains of OCO, DCO, and CNE.[117] This will force players to think ahead and manage their resources effectively based on their current view of the cyberspace domain.

Players will have to navigate toward and locate adjacent server nodes within the cyber domain, and use them to assist in their OCO, DCO, and CNE operations against their adversaries. These server nodes will become a key factor in the wargame simulation because they provide an unmasked and clear view of the active cyberspace domain, as well as increase overall situational awareness to the player. From there, players can acquire information on their

[117] Department of Defense, *Joint Publication 3–12 (R) Cyberspace Operations*.

adversaries' server nodes, launch OCO and CNE effects towards their adversaries' networks, create an early warning net from opposing attacks, or completely deny all cyber operations by destroying the server node. However, in order to maintain effective operations, the server nodes need to be active. If a server node is destroyed, a player cannot reactivate it. A major aspect this wargame takes into account is cyber attribution, in which a player who conducts an OCO attack on their adversary might end up being retaliated against, but only if the victim has the ability to investigate the attack. However, player retaliation is not incentivized or penalized by the game, like it is in CyberStrike.

E. WINNING/ENDING CYBERWAR: 2025

The purpose of the wargame is to provide an educational training aid for entry-level Army Cyber training courses. For this, we have provided a number of ways that *CyberWar: 2025* could be won/concluded and the learning objectives that support those outcomes. The ability to end a game based on time, number of rounds, or total domination should be viewed as a few of the different options available to conclude the game of *CyberWar: 2025*.

In a time-based endgame of *CyberWar: 2025*, the player with the most server nodes at the end of the time allotted wins. The time allowed could be determined by the class schedule or the training time available. The time-based method allows the facilitators to have control of the timeline of the wargame, but will not allow the player to know specifically when or how many more rounds will occur. We tested *CyberWar: 2025* with this style of endgame during the nine-month development process.

The second option would be to play a determined number of rounds after which the player with the most server nodes wins. This is similar to the time based, but the pace of play would increase or decrease the amount of time used to complete. This method would allow planners to develop their tactics and strategy based on the number of rounds to be played.

The final option to winning/ending the wargame would be to allow players to compete until one player has achieved total domination the board. This could allow a player to ally with other players—or to ally against an aggressor—in acquiring every server node on the board. Generally, this version of winning/ending the wargame would require the most amount of time to complete. However, it allows for the largest number of rounds between the players and would encourage players to plan for an extended strategic conflict.

F. WALKTHROUGH OF INITIAL ROUNDS FROM THE RED PLAYER PERSPECTIVE OF "DOTEVIL"

CyberWar: 2025 is a wargame based on the individual decisions made by the player. The player must decide how they will allocate their very limited action/research points per round. The players are faced with two decisions to start the game. They must decide which server node or nodes to acquire first and then secure using both the *acquire and secure cyber effects*. Each player will begin the wargame with three action/research points to start the first round. All future action/research points will be based on the number of server nodes that are controlled and positively linked to the player's base. Starting off, a player may use their initial three action/research points to secure one adjacent server node from their base, harden their only acquired server node to a level of two, and spend a minimum of one action/research point in the Research Investment Table. The only categories available to spend action/research points in the Research Investment Table are Defensive Cyberspace Operations Effects (DCO), Offensive Cyberspace Operations Effects (OCO), and Computer Network Exploitation Effects (CNE).

In the initial round, the player has only five possible moves they can make as seen in the figure below. From these five potential moves in the first round, there are only two actions a player can choose that will allow them to have one more action/research point in the next round.

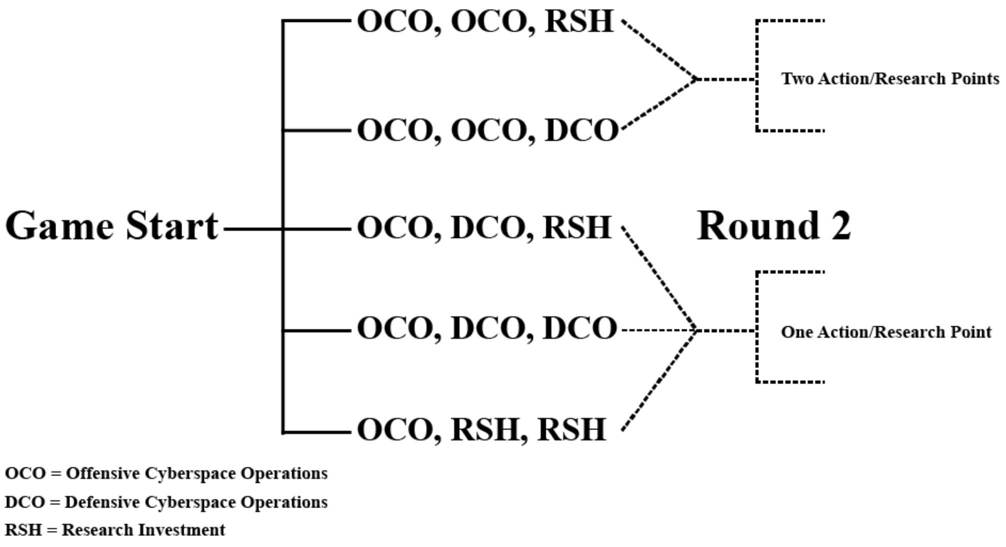
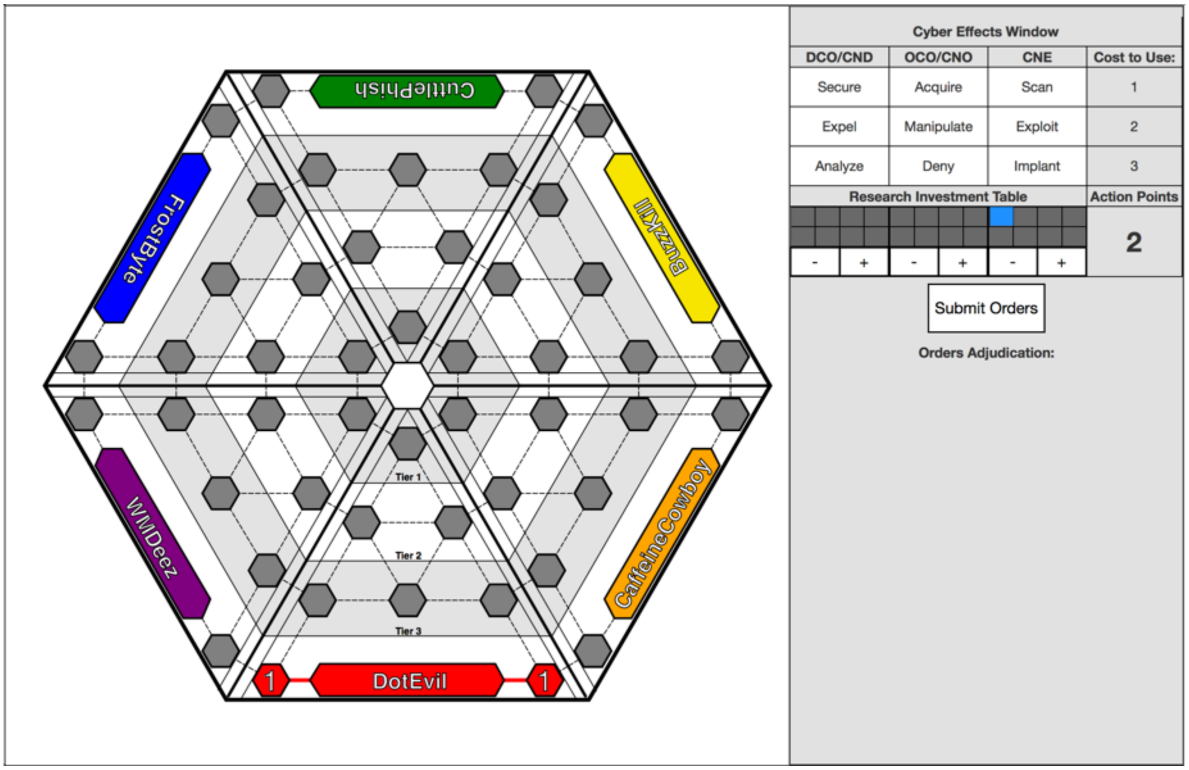

Game Start
OCO, OCO, RSH
OCO, OCO, DCO
OCO, DCO, RSH
OCO, DCO, DCO
OCO, RSH, RSH
Two Action/Research Points
Round 2
One Action/Research Point
OCO = Offensive Cyberspace Operations
DCO = Defensive Cyberspace Operations
RSH = Research Investment

Figure 10. Round 1 Actions Game Theory Tree

As an example, DotEvil will decide to use two action/research points on the two outer server nodes to the outside of the base and invest action point into the CNE category of the Research Investment Table.



Cyber Effects Window

DCO/CND	OCO/CNO	CNE	Cost to Use:
Secure	Acquire	Scan	1
Expel	Manipulate	Exploit	2
Analyze	Deny	Implant	3

Research Investment Table

-	+	-	+	-	+

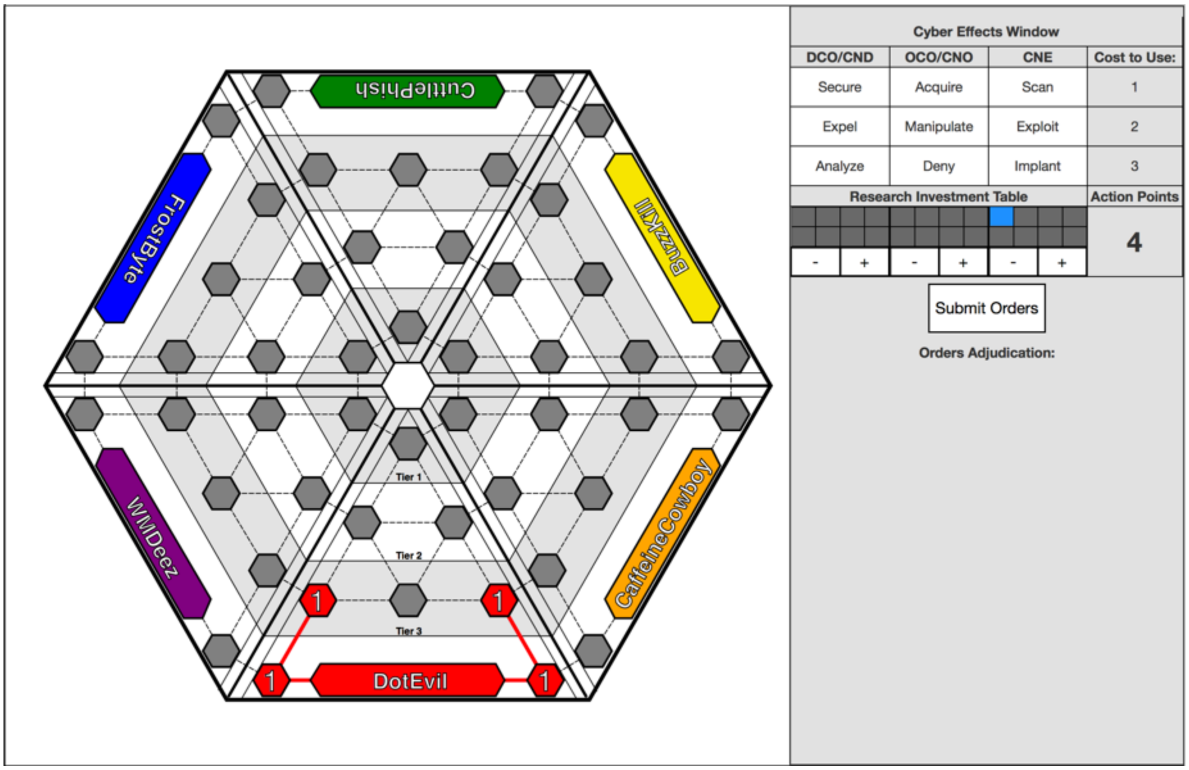
Action Points

2

Orders Adjudication:

Figure 11. Board View: Start of Round 2

DotEvil will begin the second iteration with two action/research points available to the player. DotEvil controls and is connected to the two server nodes that were acquired in the prior iteration. As an example, DotEvil will decide to use two action/research points to acquire the two outer server nodes to the outside of the Tier 3. DotEvil will not be able to invest in the Research Investment Table during this iteration. DotEvil is aiming to maximize the number of server nodes controlled. This decision will maximize the number of action/research points available in the following iteration. At the conclusion of this round, the DotEvil player will control four server nodes and have one investment point in CNE on the Research Investment Table.



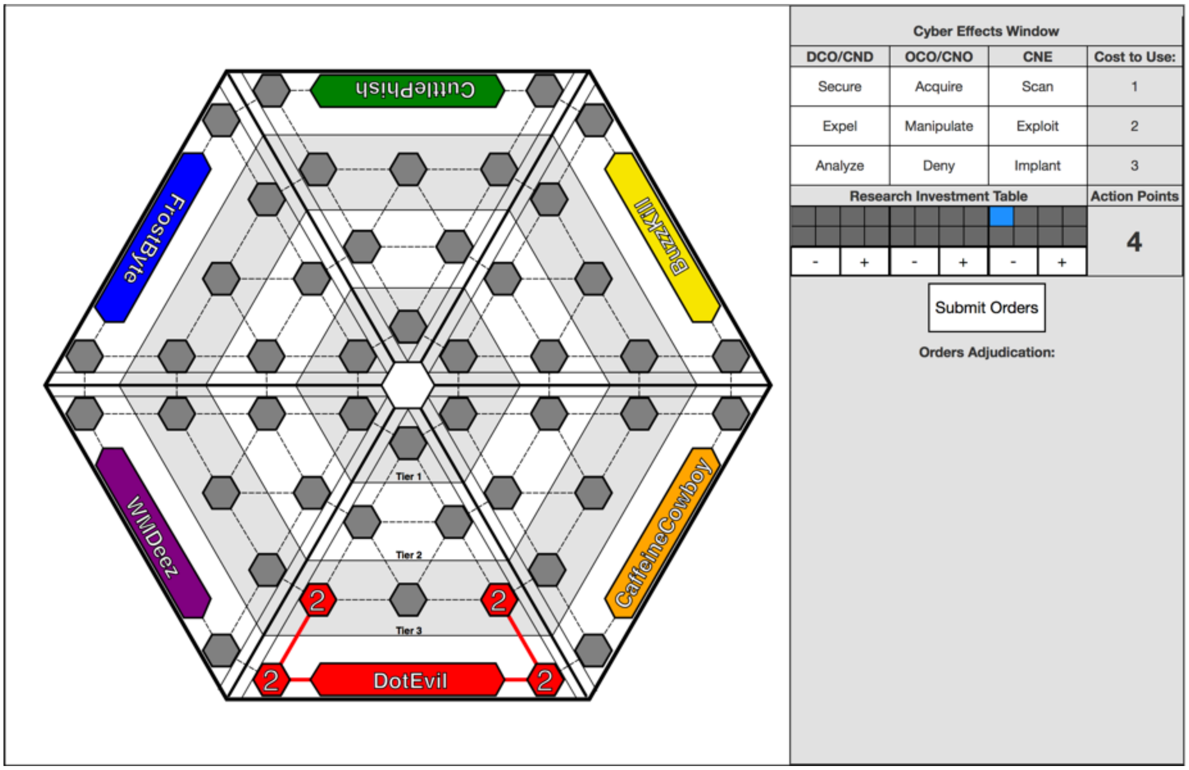
Cyber Effects Window

DCO/CND	OCO/CNO	CNE	Cost to Use:
Secure	Acquire	Scan	1
Expel	Manipulate	Exploit	2
Analyze	Deny	Implant	3

Figure 12. Board View: Start of Round 3

DotEvil will begin the third iteration with four action/research points to be used. As an example, DotEvil will decide to use all four action/investment points to secure all four acquired points to a level of two. To increase a server node hardening by one level for all controlled server nodes using the secure effect, DotEvil can only spend one action/research point per server node and then end the round.

In the fourth and final iteration of this walkthrough, DotEvil will use all four action/research points to scan CaffeineCowboy's Tier 3 server node to the right of DotEvil, because it costs one action/research point to use the Scan Effect and three action/research points to cross Tier 3 domain boundary. At the end of round four, DotEvil will have four server nodes acquired, positively linked to his base, and secured to a level of two. He also has one investment point in the CNE category of the Research Investment Table and has seen if CaffeineCowboy's Tier 3 server is controlled or not.



Cyber Effects Window

DCO/CND	OCO/CNO	CNE	Cost to Use:
Secure	Acquire	Scan	1
Expel	Manipulate	Exploit	2
Analyze	Deny	Implant	3

Research Investment Table	Action Points
- + - + - +	4

Orders Adjudication:

Figure 13. Board View: Start of Round 4

This initial strategy is simply intended to provide an overview of one possible way that a player could decide to take actions in *CyberWar: 2025*. Players are encouraged to freely make decisions in the wargame based on the tactics and strategy they seek to accomplish. Players will only be provided action/research points once at the beginning of the game. This is also the only time that their decision to use action/research points is prescribed.

V. FUTURE RESEARCH AND CONCLUSION

We designed *CyberWar: 2025* to keep players engaged with each other as well as with the instructor during consecutive rounds. The drastically limited play space and the fluid game mechanics, particularly in the center of the board, push players to either vie for overt control or work covertly through exploitation. We realized in our initial playtests that most players would fall into two separate strategy categories—either push to the center of the board to gain control or hang back and build up defenses against opposing players. Only a few players worked their way around the board using CNE cyber effects instead of using overt actions. We did not document and archive these playtests for future analysis; however, when we concluded these playtests, those players who used CNE as a primary means to dominate the board were largely successful against the other players who attacked or defended overtly. This supported our argument on how useful CNE cyber effects are in cyber strategy. We also realized that, after the first five rounds of a playtest, players became comfortable with the mechanics and dynamics of *CyberWar: 2025* and were able to execute and revise their cyber strategy at the start of each new round.

After each playthrough, we asked players to fill out a survey about their experiences with *CyberWar: 2025* and about how to improve the game. From these player comments, as well as our own comments during the design and development phases, we recognized a few key elements such as attribution, additional cyber effects in the game, game balancing, and alliances which we were either not able to implement or support with valid research that would effectively increase the educational and training effect of *CyberWar: 2025* in future revisions.

A. ATTRIBUTION AND POSSIBLE RETRIBUTION

During the action phase, players select their cyber effects to support their strategy. When the adjudication phase is completed, the board is updated with the new state of the simulated cyberspace domain. This version of *CyberWar: 2025* does not take into account the recognition and possibly identification of opposing player actions to one player's domain or server nodes. A player only knows when they have lost territory when a point they own has been disconnected, or otherwise gone dark, from their network. To improve *CyberWar: 2025*, we argue that this wargame should incorporate some sort of notification, either through a popup message on the board or in a generic status window, that lets the player know of a failed OCO or CNE attempt on their domain. To further advance the gameplay, we suggest creating another cyber effect or user interaction ability that enables the player to further investigate the notification to identify the origin of the attack and the attacker who launched the cyber effect.

B. ADDITIONAL OCO, DCO, AND CNE EFFECTS AND TIES TO OPE AND MANEUVER ELEMENTS

Currently, a total of nine cyber effects make up a playable version of *CyberWar: 2025*. This wargame should be able to expand an additional level or two of cyber effects, effectively increasing the number of effects to 15. At this time, we do not have any suggestions on what those cyber effects should be. However, we argue that an increase in cyber effects beyond 15 would severely disrupt the MDA flow of the wargame by creating too many choices for players to implement their cyber strategy and therefore increasing the overall complexity of *CyberWar: 2025*. This increase in choices could potentially put the player at risk of not fully understanding the learning objectives of the wargame because that player might shift attention and focus on trying to obtain the maximum level in research rather than actually playing the wargame.

To increase the validity of these cyber effects, this wargame should implement an element of operational preparation of the environment (OPE) to support physical maneuver elements. At this time, we do not have any suggestions on how both *CyberWar: 2025* and OPE to the physical domain might function cooperatively and still be playable. However, that in order to support this type of cohesion, the framework of this wargame should be incorporated into a separate and possibly larger project or wargame.

C. BALANCING OF CYBER EFFECTS AND SERVER POINT REBUILDING

During milestone testing of *CyberWar: 2025*, we came to the conclusion that third-tier cyber effects such as Deny can be extremely powerful if the attacking player is extremely lucky. Since Deny is a permanent effect that alters the game board in a physical manner by ultimately removing that server point as a controllable element in cyberspace, we argue that it should either be harder to launch, or possibly to obtain, third-tier effects in *CyberWar: 2025*. Currently, the cyber effects in this wargame are directly tied to a software-implemented pseudo-random number generator, which means that all adjudication events are not truly random, and therefore, a player has a greater chance to succeed or lose when submitting orders. This could lead to a potential unbalanced feel during play, which could disrupt the wargame's MDA flow and hinder the player's understanding of the learning objectives. Also, this wargame should notify the player of "chance of success" or "calculated odds" before submitting for adjudication. This notification would consist of either the true calculated odds of success, in which the attacking player has been shown the opposing player's server point value through scanning, or an "educated/unknown" odds of success if the opposing player's server point value is not known. A modification like this would influence players to use Scan or Analyze more often since they might not want to launch a cyber effect "in the blind."

Another way to offset the imbalance of Deny would be to allow players to rebuild server nodes that have been rendered disabled on the game board. Since the cost to use Deny is currently set at three action/research points, we argue that the cost to rebuild server nodes should be that of equal or greater value, and that server nodes can only be rebuilt within that player's own domain. Because it is physically possible to fix or repair a server within a specified geographical location after an incident, we feel that this game should be able to simulate the rebuilding a server network that the player has the ability to physically travel to.

D. ALLIANCES, TEAM COMMUNICATION, AND SUPPORTED MOVES

When the table-top version of *CyberWar: 2025* was developed and tested, we implemented a simple protocol of team communication through means of note passing before the orders adjudication phase. To support this, we collected the notes from each player at the end of each adjudication round and hand delivered these notes to their intended receiver with a level of secrecy. There were a few times where we had to pass several communiques within a round. Ultimately, this level of communication allowed players to cooperatively work together and build alliances during play that is similar to Diplomacy, in which players could coordinate moves and player strategies with other players to obtain their most favorable outcome. One unforeseen element of communication with other players is that we were forced to rethink the rule on how to do supported moves. During the working group phase of *CyberWar: 2025*, the idea of supported moves was suggested and roughly implemented, but it was nowhere near perfect because of the amount of complexity involved. In our rough application of supported moves, players had to decide amongst themselves who was in the supporting role and who was attacking, but if both the attacker and the supporter failed, then the defender would see the actions of both the attacking players.

We restricted the use of supported moves in the table-top version of the wargame. As for the software version of *CyberWar: 2025*, we were not able to implement supported moves because the software version does not support an in-game chat function for player communication. Therefore, we recommend that any follow-on additions or improvements to *CyberWar: 2025* should implement an element of player communication, alliances, and the ability to conduct supported moves.

E. CONCLUSION

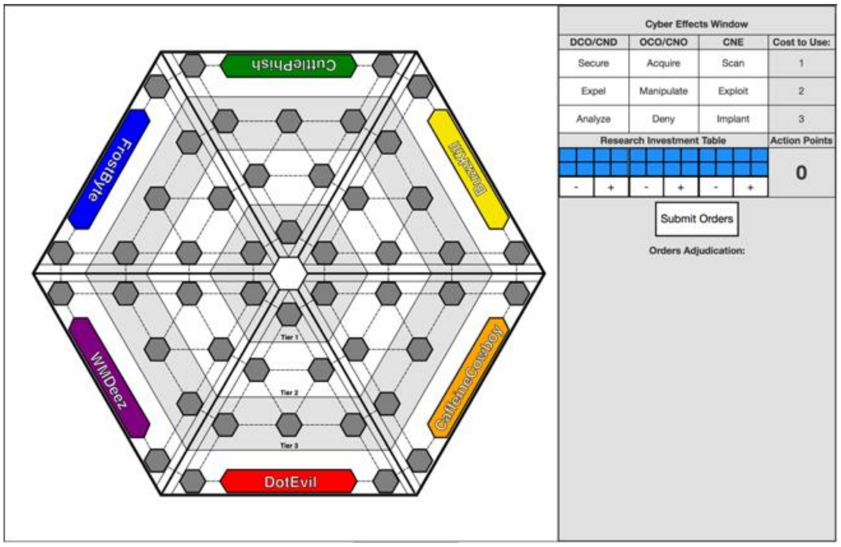
We designed and developed *CyberWar: 2025* as a tool to educate and train DOD personnel on cyberspace operations, and within our nine-month time window, we created both a table-top and an in-development beta version of the game. We argue that *CyberWar: 2025*, at its current state, will help DOD cyber education and training students and their instructors by demonstrating the core basics of cyberspace operations as stated by our researched learning objectives. However, *CyberWar: 2025* needs further testing and development to make it an effective final product. We recommend that future research should be conducted to assess *CyberWar: 2025*’s value is, from a pedagogical standpoint, in teaching or reinforcing the learning objectives of cyberspace operations. Cyberspace is a constantly growing, dynamic, and a largely uncharted domain, and we recommend that the best way to understand cyber is to simulate it and gamify.

APPENDIX A. RULESET

A. HOW TO PLAY

CyberWar: 2025 is a game of stealth, alliances, long term strategy, and chance. Players must map, navigate, and maintain control of servers in cyberspace. Players initially start from their base, which players branch out from in a tiered fashion to locate and assess other players for potential adversaries or allies. The game is won by either running out of time (player with the most server nodes wins), or by a player or alliance of two players acquiring every server node on the board.

The game is turn-based and conducted in a series of phases per turn. All actions or investments in the game use the same action/research points. Players gain one action/research point from each server node they have acquired or exploited. These action/research points can then be used for executing or investing cyber effects.



Cyber Effects Window

DCO/CND	OCO/CNO	CNE	Cost to Use:
Secure	Acquire	Scan	1
Expel	Manipulate	Exploit	2
Analyze	Deny	Implant	3

Research Investment Table

Action Points

0

Orders Adjudication:

Figure 14. Initial View of *CyberWar:* 2025 Board

Since players open the game without owning any servers (just their base), for the opening round only, all players have three free action/research points. They can use those action/research points to expand to the base-level servers, and can add the remaining point to their choice of any of the three fields in the Research Investment Table.

Initial turn:

1. Orders Phase:
    a. Spend Action/Research Points
    b. Acquire
2. Orders Resolution
3. Action/Research Points Allocation

Consecutive turns:

1. Orders Phase (in this order):
    a. Secure and Investing in the Research Tree
    b. Execute Offensive Cyberspace Operations (OCO), Computer Network Exploitation (CNE), or Expel or Analyze from the Defensive Cyberspace Operations (DCO) cyber effects.
2. Spend Action/Research Points
3. Orders Adjudication
    a. Pre-Adjudication (Scan Only)
    b. First Round Adjudication (Secure, Implant, and Deny)
    c. Second Round Adjudication (Expel, Analyze, Acquire, Manipulate, and Exploit)
4. Orders Resolution
5. Action/Research Points Allocation

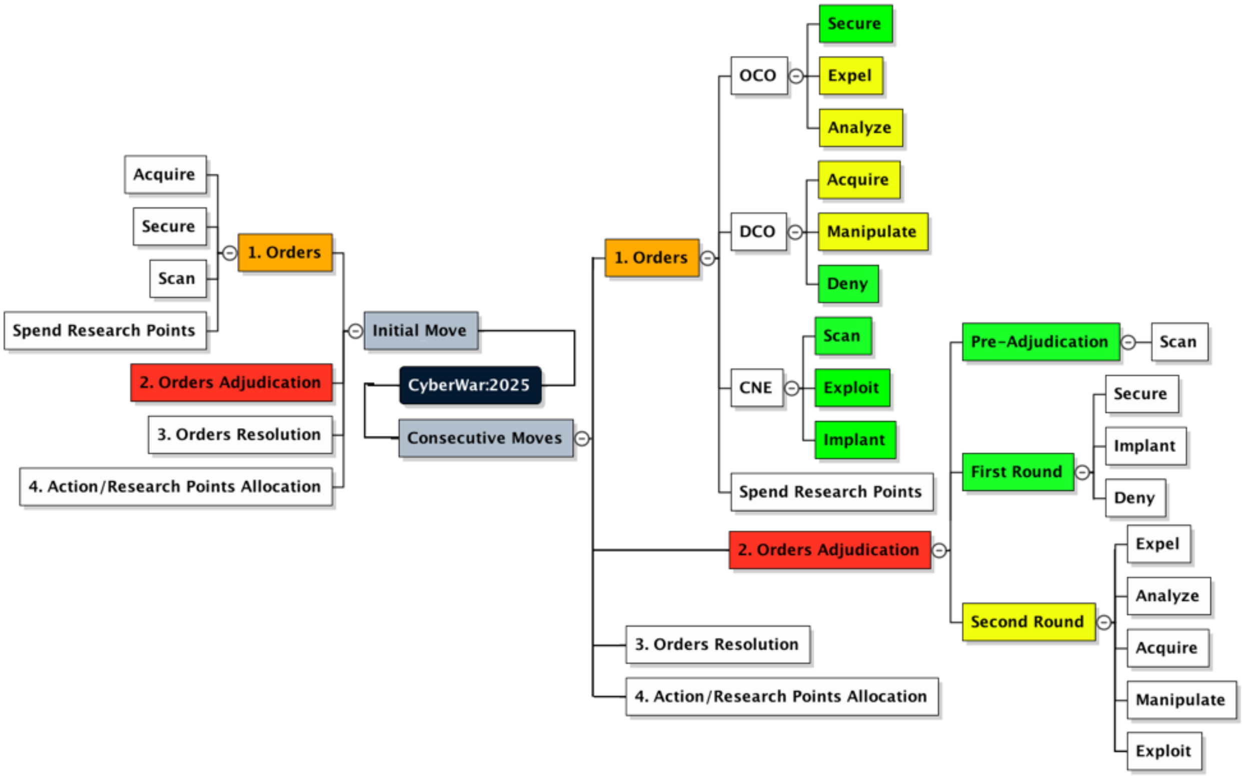


Figure 15. *CyberWar: 2025* Game Flow

B. ORDERS/EFFECTS:

On each turn, players can use the action/research points they gain from owning server nodes (one action/research point per node) to execute or invest in locked cyber effects. Action/research points invested in the research table accumulate over turns; however, any action/research points that are not used are discarded after the player’s orders have been submitted. For example, a player can invest one action/research point toward CNE field in round three, then add three more points in round four. This would unlock the Exploit Effect for use in round five and consecutive rounds. Adding four more points to CNE field afterwards, would unlock the Implant Effect. Most cyber effects are used individually or “unstacked” with other effects; however, the only stackable cyber effect is Implant because of its ability to join with Acquire, Exploit, Manipulate, and Deny cyber effects.

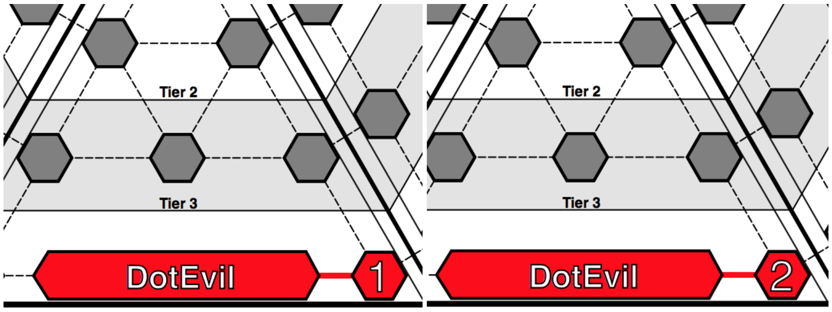
Table 1. Cyber Effects and Their Investment Research and Usage Cost

Cyber Effects			Costs	
DCO	**OCO**	**CNE**	**Research Investment**	**Cost to Use**
Secure	Acquire	Scan	0	1
Expel	Manipulate	Exploit	4	2
Analyze	Deny	Implant	8	3

C. CYBER EFFECT DESCRIPTIONS

1. Defensive Cyber Operations (DCO)

Secure Effect: This cyber effect increases the value of a server node by one point value. Players may increase their server node's maximum point value of four; this would cost the player a total of three action/research points. All server nodes have an initial value of one point when acquired regardless if they are unoccupied or taken from another player. The higher value on a server node, the stronger the attack and defense odds against opposing cyber effects.



Orders **Adjudication**

Figure 16. Secure Effect

Expel Effect: This effect removes any players running exploitation effects from the server node it is executed on. Players may only use this effect on servers they have already acquired and directly linked to. Players can execute this effect in the blind, or without prior knowledge of someone exploiting their server nodes.

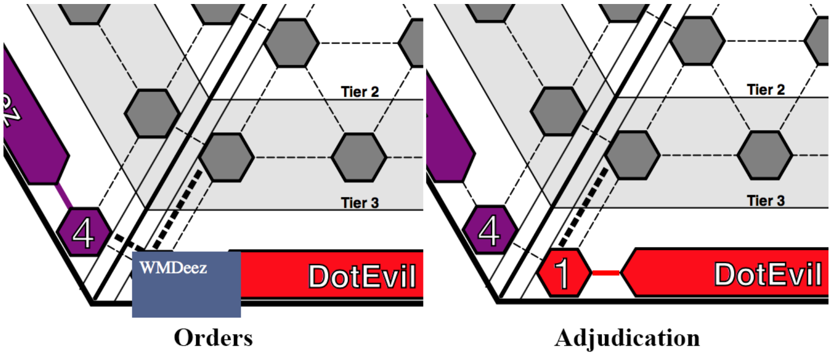


Figure 17. Expel Effect

Analyze Effect: This effect scans all of the player's acquired server nodes and reveals any exploit effects. It also exposes any players using the Manipulate Effect for that server node.

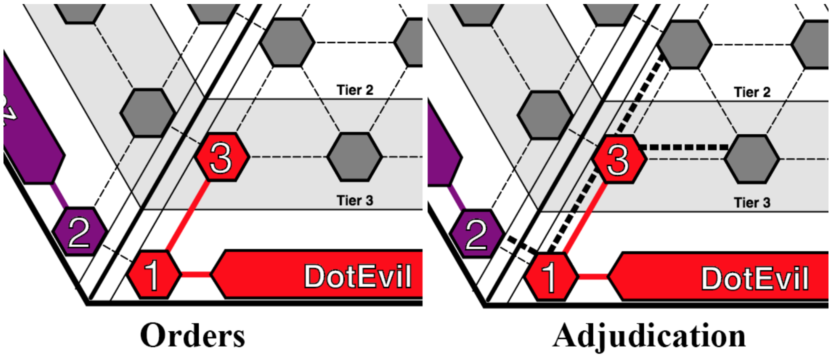


Figure 18. Analyze Effect

2. Offensive Cyber Operations (OCO)

Acquire Effect: This effect overtly seizes control over targeted server nodes. The Acquire Effect cannot be used against bases. The odds of success for an Acquire Effect attempt are determined by comparing the value of the attacking server node with the value of the defending server node (see Neil's Method in Appendix B). Thus, using Secure Effects increases the likelihood of a successful acquisition using the secured server. Players also can execute this effect in the blind, or without prior knowledge of someone controlling that server node using the Scan Effect.

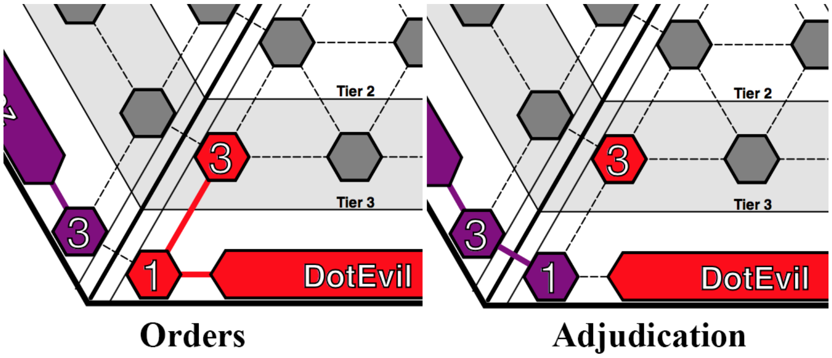


Figure 19. Acquire Effect

Manipulate Effect: This effect misattributes the source of and Acquire or Exploit Effects attempts. The attacking player chooses which player they want to impersonate. Acquisitions and exploitations conducted using this cyber effect maintain their misattribution until the server is lost. If either of the Acquire or Exploit Effects attempt fails, the manipulation will still be successful. Players also can execute this effect in the blind, or without prior knowledge of someone controlling that server node using the Scan Effect.

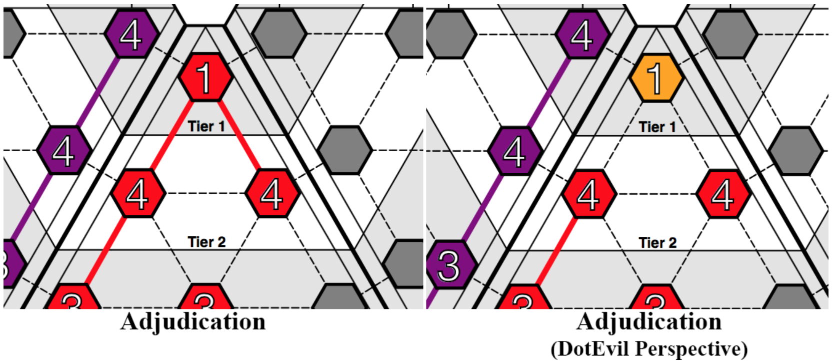


Figure 20. Manipulate Effect

Deny Effect: This effect destroys a targeted server node on the board, rendering it unusable by any player. In this example Purple, or WMDeez, launches a Deny Effect from its Tier 1 server node to Red's, or DotEvil's, Tier 1 server node and successfully removes Red's server node as a playable point from the board. Players also can execute this effect in the blind, or without prior knowledge of someone controlling that server node using the Scan Effect.

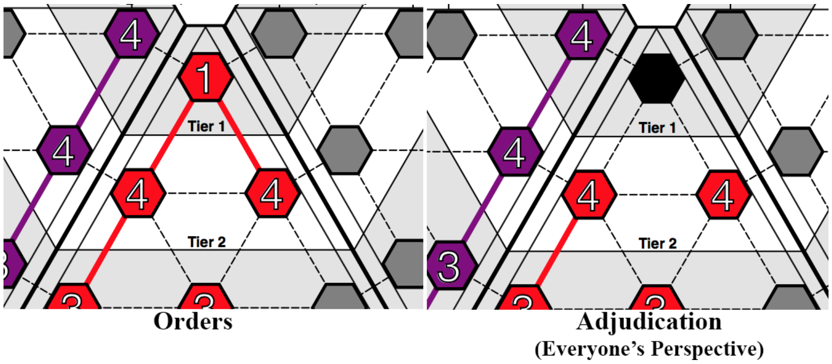


Figure 21. Deny Effect

3. Computer Network Exploitation (CNE)

Scan Effect: This effect determines the status of a targeted server. It reveals all overt and covert links running to and from the server but cannot correctly attribute acquisitions or exploitations that were masked using the Manipulate Effect.

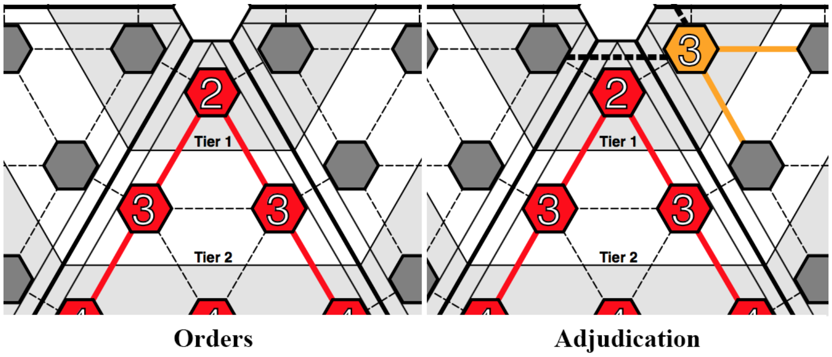


Figure 22. Scan Effect

Exploit Effect: This effect builds a covert link to an opponent's server, allowing the exploiting player to gain a point from that server and to see all overt links to that server, as well as all neighboring servers within the same domain. The targeted player will be unaware of the Exploit Effect unless he runs the Scan Effect on the effected server node, or runs the Analyze Effect on his entire network. Players may continue building covert links using the Exploit Effect from servers, which they have previously exploited. They may also use the Implant Effect from any exploited server. If used against an opponent's base, the Exploit Effect reveals the opponent's entire network, it also gives any cyber effects developed by the defender to the attacker.

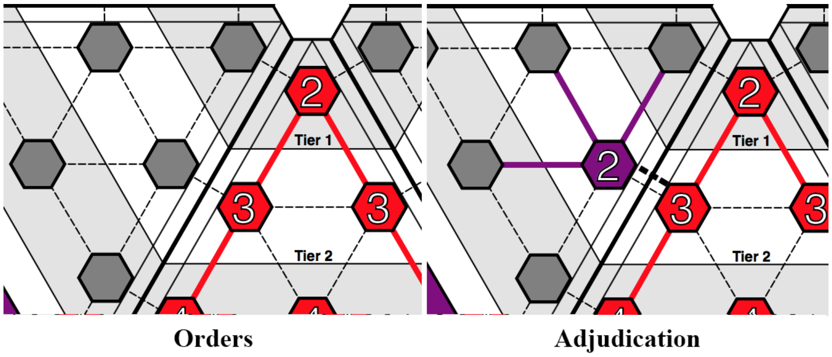


Figure 23. Exploit Effect

Implant Effect: This effect covertly weakens the targeted server node to one point during the turn in which it is used, making any Acquire or Exploit Effects used against the targeted server more likely to succeed, and making attacks launched from the server node more likely to fail. If the executing player is successful against an opponent's base then this cyber effect acts as ransomware, in which all points that would normally go to the base owner will be held ransom by the attacking player. If the base owner decides to pay the ransom, he will have no action/research points, but will be free of the ransomware. Otherwise, if base-owners have developed the Expel Effects prior to the implant attack on their base and have enough action/research points, they may use the Expel Effect once per turn until they successfully remove ransomware or until five rounds have passed since the initial ransomware attack took effect. Implant Effect may only be run against any base once every two turns, if the first attempt from the attacker is unsuccessful.

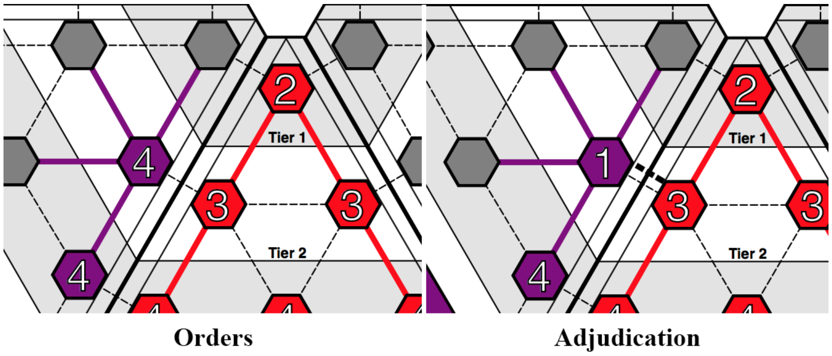


Figure 24. Implant Effect

Support: [Not implemented in the software version] Supporting effects come in the form of joined orders from multiple servers. Players can support their own use of effects or that of allied players. Players may not support defense. Players may support their own manipulated attacks, but if unsuccessful, the targeted player will see the overt support. If successful, the attacker may build an overt link on the support line (which are visible if scanned), or may choose not to build the link.

D. INTER-DOMAIN ACTIONS

Crossing Domains: Players can use the Acquire or Exploit Effects to gain access server nodes that are outside the player's own network domain. When inside an opposing player's domain, the cost to gain access is not modified by the tier level; however, crossing into an opposing player's domain initially has a tiered level, or modified cost, associated with it. Executing cyber effects against any servers in the center of the board, or Tier 1, only cost the player the base cyber effect cost and plus the tier amount. In this case, for a player to use the Acquire Effect at an adjacent server node on the Tier 1 level, the total cost would be two action/research points (one for the Scan Effect and one for the Tier level). At the Tier 2 level, it would be three action/research points and so on to Tier 4, which would cost four action/research points. The stacked cyber effect of Implant during cross-domain execution of cyber effects does not cost the player any additional action/research points to when used with another cyber effect.

For example, a cross-domain using the Acquire Effect attempt in Tier 1 costs two action/research points.

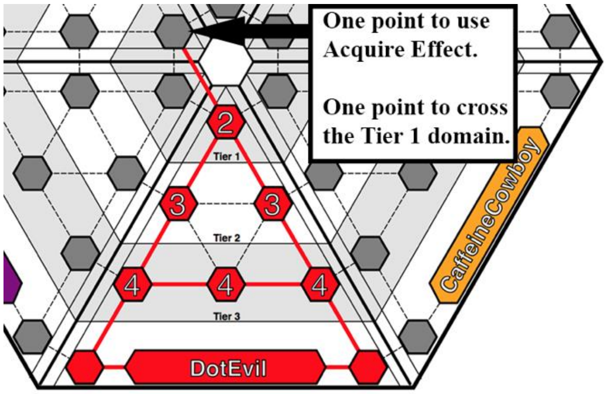

One point to use Acquire Effect.
One point to cross the Tier 1 domain.
2
Tier 1
3
3
Tier 2
4
4
4
Tier 3
DotEvil
CaffeineCowboy

Figure 25. Acquire Effect Crossing Tier 1 Domain

A cross-domain using the Exploit Effect attempt in Tier 2 costs four action/research points.

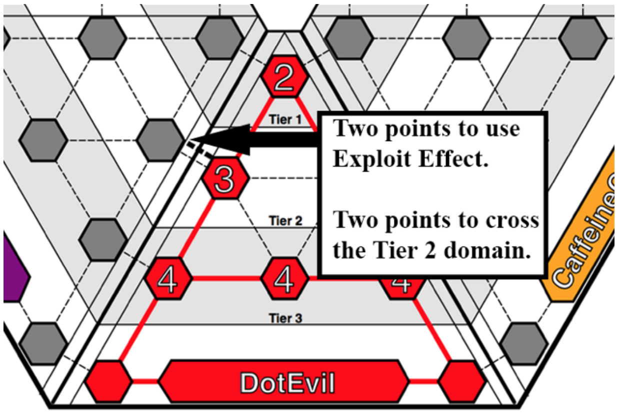

Two points to use Exploit Effect.
Two points to cross the Tier 2 domain.
2
Tier 1
3
Tier 2
4
4
Tier 3
DotEvil

Figure 26. Exploit Effect Crossing Tier 2 Domain

E. LINKS AND VISIBILITY

Link-Building Rules: Players can use Acquire or Exploit Effects to build links between server nodes. The base can build links to the nodes on the base-tier but not to nodes in other tiers. Players can only acquire one server node adjacent to a server node that the player controls, they cannot "double hop" to acquire a server node beyond any server node that they do not have control of.

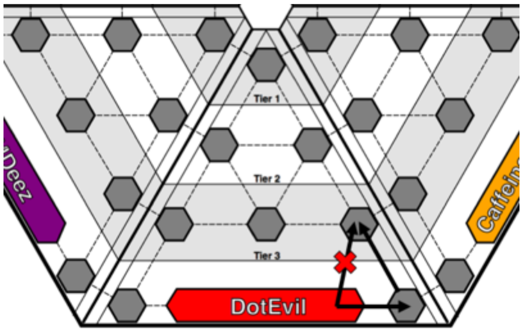


Figure 27. Link Building Example

Players can use Acquire or Exploit Effects to build a link from a Tier 1 server to any other Tier 1 server. However, players may only go to one other node at a time—no starburst attacks.

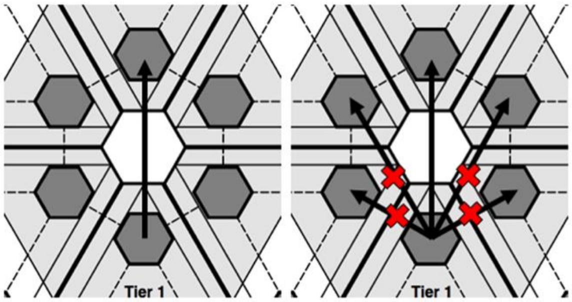


Figure 28. Starburst Cyber Effect Example

Visibility: Players can see any overt activity in their own domain. However, they cannot see across domain boundaries without first successfully acquiring or exploiting a server on the other side of the boundary or executing a scan on a server in another domain.

Covert activities (Exploit and Implant Effects) are invisible to the effected player unless the Analyze or Scan Effects are executed within the player’s network.

Failed access to a server node (whether overt using the Manipulate and Acquire Effects, or covert using the Manipulate and Exploit Effects), can only be properly attributed by using the Analyze Effect.

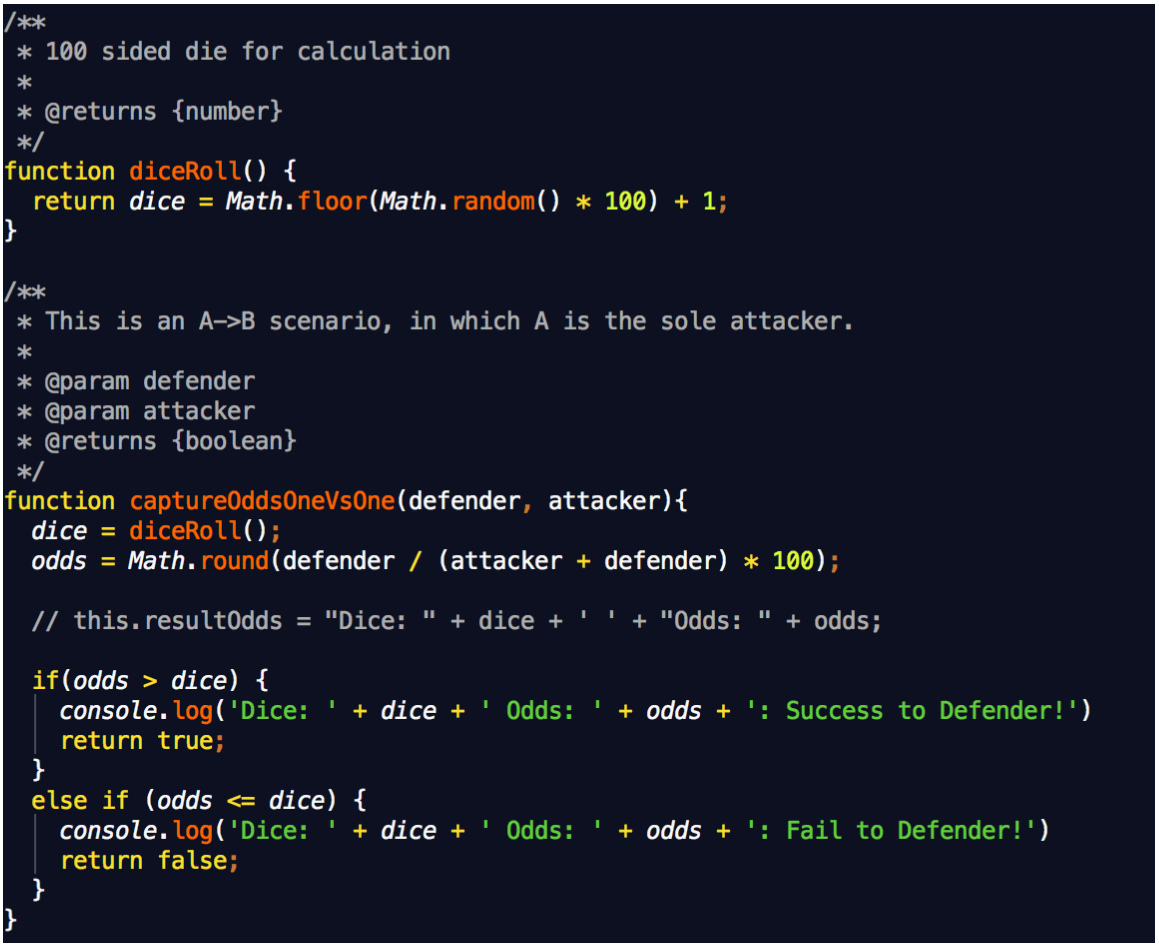
APPENDIX B. RANDOMIZATION AND ADJUDICATION MATH

During the orders adjudication process, all actions are collected and simultaneously calculated based on a simple mathematical equation. All cyber effects, minus Secure, Scan, and Analyze, use this equation called the "Niels's Method" to resolve all player actions. This equation was named after its creator during the working group phase of *CyberWar: 2025* and uses the server node values of both the defending and attacking players as well as a 100-sided dice roll (d100). This dice roll is the randomization factor in the success or failure of each player action, which roughly simulates the uncertainty in launching cyber effects in cyberspace.

$$\boldsymbol{d100 > Defense\ Odds \Rightarrow d100 > \frac{100 \text{ x } Defender\ Level}{Defender\ Level + Attacker\ Level}}$$

Figure 29. Niels' Method Equation

In the software implementation of *CyberWar: 2025*, we use a pseudo-random number generator as the 100-sided die incorporate that into each available player versus player (PvP) interaction in the game. During the game, if two or more players have the same dice roll result then the software will automatically re-roll until a single player is determined the winner. In figure two below, the Math.floor() function, or lowest value possible in a random dice roll, is set to the minimum of one because the smallest value on a 100-sided die is one.



```
/**
 * 100 sided die for calculation
 *
 * @returns {number}
 */
function diceRoll() {
  return dice = Math.floor(Math.random() * 100) + 1;
}

/**
 * This is an A->B scenario, in which A is the sole attacker.
 *
 * @param defender
 * @param attacker
 * @returns {boolean}
 */
function captureOddsOneVsOne(defender, attacker){
  dice = diceRoll();
  odds = Math.round(defender / (attacker + defender) * 100);

  // this.resultOdds = "Dice: " + dice + ' ' + "Odds: " + odds;

  if(odds > dice) {
    console.log('Dice: ' + dice + ' Odds: ' + odds + ': Success to Defender!')
    return true;
  }
  else if (odds <= dice) {
    console.log('Dice: ' + dice + ' Odds: ' + odds + ': Fail to Defender!')
    return false;
  }
}
```

Figure 30. JavaScript Code of Dice Roll and PvP Action

When a player decides to attack an opponent, the odds of the attack depends on the defender’s level versus the attacker’s level. These odds are then interpolated to a 100-sided die. In below example, the defending server node is secured to level three and the attacking server node is secured to level four. Therefore, the attacking server node will be successful in adjudication if the 100-sided dice roll is equal to or greater than 43 (the software rounds up to the nearest whole number), otherwise the defender will win by default.

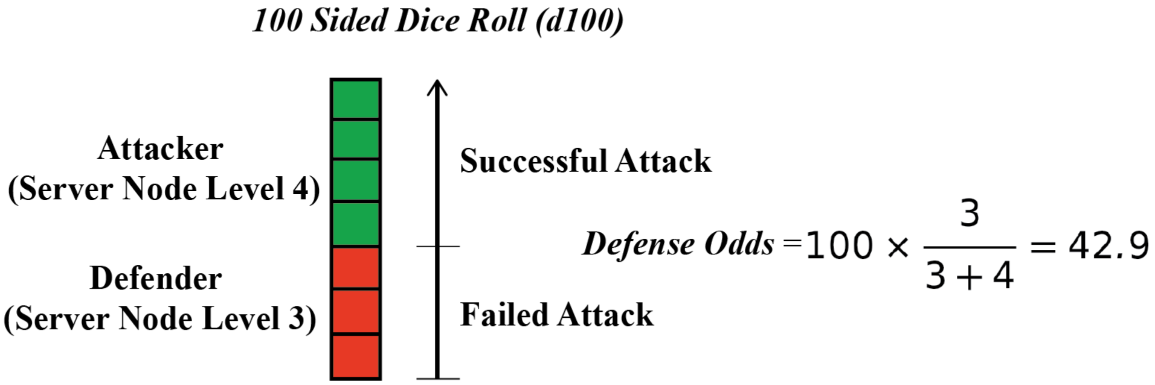


Figure 31. Player versus Player Action Adjudication

In a multiple-player attack, each player's defense odds are calculated the same way as a player versus player attack. However, since all moves are adjudicated simultaneously, a success margin is used which is based on the same defense odds of a player versus player action. The player with the highest positive margin of success to their specific defense odds wins the adjudication. If neither attacker has a margin of success higher than their specific defense odds, then the defender wins. If two or more attackers have the same margin of success to their defense odds, it is labeled as a draw and then those attackers who were in the draw roll again.

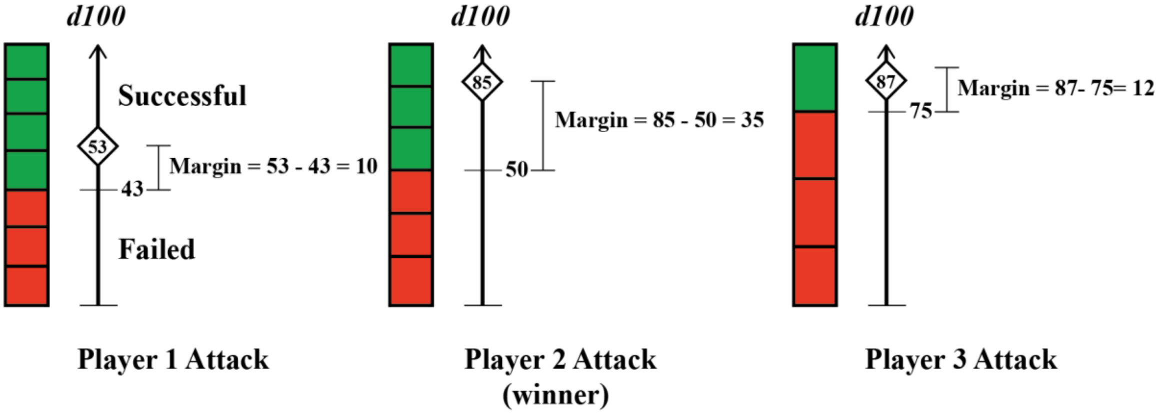
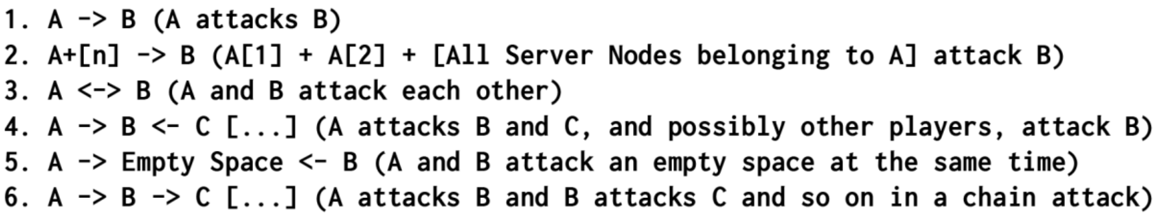


Figure 32. Multiplayer Action Adjudication

In *CyberWar: 2025* we have six possible move scenarios for each playable action. In the figure below, we have identified the six scenarios that the game recognizes and adjudicates. Any moves other than these six are identified as invalid at this time. The two adjudication actions mentioned above cover all six of these move scenarios.



```
1. A -> B (A attacks B)
2. A+[n] -> B (A[1] + A[2] + [All Server Nodes belonging to A] attack B)
3. A <-> B (A and B attack each other)
4. A -> B <- C [...] (A attacks B and C, and possibly other players, attack B)
5. A -> Empty Space <- B (A and B attack an empty space at the same time)
6. A -> B -> C [...] (A attacks B and B attacks C and so on in a chain attack)
```

Figure 33. The Six Possible Player Moves for Adjudication

APPENDIX C. RELATIONSHIP OF LEARNING OBJECTIVES TO ACTIONS IN CYBERWAR:2025

Authenticity and realism are the core concepts that were consistently interwoven throughout the entire research and development of *CyberWar: 2025*. We understood that *CyberWar: 2025* needed to have a proper mix of both entertainment and training methodologies to be effective tool for education as a serious game. To support this realism, we reached out to several Army cyber training course coordinators to obtain a consolidated list of learning objectives from which to build the foundation of *CyberWar: 2025* upon. These learning objectives remained persistent throughout the development process and were the validation for each decision, cyber effect, or mechanic in the game. In the table below, we have identified how the actions within *CyberWar: 2025* are related to the learning objectives.

Table 2. Learning Objectives Representation in *CyberWar: 2025*

Learning Objective	**How it is represented in CyberWar: 2025**
Understanding the fundamentals of cyberspace operations.	• Player's actions when using cyber effects on other players. • Player reacting to various cyber effect actions from other players during game play. • Player acquiring and defending sever nodes using OCO, DCO, and CNE cyber effects.
Understanding cyberspace threats.	• Player launching cyber effect actions against other players or receiving actions from other players. • Player using CNE cyber effects to covertly infiltrate an opposing player's domain.

Learning Objective	**How it is represented in CyberWar: 2025**
Targeting in cyberspace.	• Player launching Acquire and Scan cyber effect actions on other players.
Providing intelligence support to cyberspace operations.	• Player launching Acquire/Scan cyber effect actions on other players. • Player alliances, supported cyber effect actions, and player to player communications.
Understanding defensive and offensive cyberspace operations.	• Player launching cyber effect OCO/CNE actions against and from opposing players. • Player executing Secure cyber effect on player's own server nodes. • Player discovering and removing exploited players within player's own network using DCO cyber effects.
Understanding cyberspace as a domain.	• Board layout and design from the player's own local domain to neighboring player domains and foreign domains which are on the opposite side of the board. • Player bases, server nodes, and tiers levels.
Understanding cyber threat actors.	• Player using DCO cyber effects to remove infiltrated players from player's own network. • Player using CNE cyber effects to infiltrate opposing player's domains.

Learning Objective	**How it is represented in CyberWar: 2025**
Understanding High Value Target List (HVTL) and High Payoff Target List (HPTL).	• Player identifying each player on the board and how well they are playing in conjunction with their own cyber strategy. • Player interactions with other players to support their cyber strategy.
Understanding cyberspace infrastructure and key terrain.	• Board layout and design. • Player maintaining control of their own server node network and defending their base against opposing players.
Describing OCO/DCO actions and effects.	• Player launching cyber effect actions against other players or receiving actions from other players.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Adams, Mackenzie, and Maged Makramalla. "Cybersecurity Skills Training: An Attacker-Centric Gamified Approach." *Technology Innovation Management Review* 5, no. 1 (2015): 5–14.

Adkins, Sam S. "The 2016-2021 Global Game-Based Learning Market – Serious Play Conference." Ambient Insight, July 26, 2016. http://seriousplayconf.com/downloads/the-2016-2021-global-game-based-learning-market/.

Anders, Frank. "Gaming the Game: A Study of the Gamer Mode in Educational Wargaming." *Simulation & Gaming* 43, no. 1 (February 1, 2012): 118–32. https://doi.org/10.1177/1046878111408796.

———. "Unexpected Game Calculations in Educational Wargaming: Design Flaw or Beneficial to Learning?" In *DiGRA '11 - Proceedings of the 2011 DiGRA International Conference: Think Design Play*. DiGRA/Utrecht School of the Arts, 2011. http://www.digra.org/wp-content/uploads/digital-library/11310.31521.pdf.

Arenas, Fil, and Andrew Stricker. "Gamification Strategies for Developing Air Force Officers." *Learning Solutions Magazine*, June 17, 2013. https://www.learningsolutionsmag.com/articles/1190/gamification-strategies-for-developing-air-force-officers.

Babel. "The Compiler for Writing Next Generation JavaScript," 2017. https://babeljs.io/.

Bohemia Interactive. "Bohemia Interactive Simulations," 1999. https://bisimulations.com.

Bunchball. "Bunchball," April 29, 2011. http://www.bunchball.com.

Burke, Brian. *Gamify: How Gamification Motivates People to Do Extraordinary Things*. Brookline, MA: Bibliomotion, 2014.

Caffery Jr., Matthew. "Toward a History-Based Doctrine for Wargaming." *Air and Space Power Journal* 13, no. 3 (Fall 2000): 33–56.

Central Intelligence Agency. *Information Operations and Intelligence Community Related Activities*. Director of Central Intelligence Directive 7/3. Central Intelligence Agency, July 1, 1999. https://fas.org/irp/offdocs/dcid7-3.pdf.

CyberCIEGE. Windows. Monterey, CA: Naval Postgraduate School and Rivermind, Inc., 2004. http://my.nps.edu/web/cisr/cyberciege.

CyberStrike - GlobalECCO. Web. Monterey, CA: Naval Postgraduate School, 2011. https://globalecco.org/play.

CyberStrike Advanced - GlobalECCO. Web. Monterey, CA: Naval Postgraduate School, 2011. https://globalecco.org/play.

Dale, Steve. "Gamification: Making Work Fun, or Making Fun of Work?" *Business Information Review* 31, no. 2 (June 1, 2014): 82–90. https://doi.org/10.1177/0266382114538350.

Davis, Nils. "The 'Drive' To Gamification: Motivation 3.0 and Game Mechanics." *Hardcore Product Management* (blog), September 4, 2012. https://pmhardcore.com/the-drive-to-gamification-motivation-3-0-and-game-mechanics/.

Department of Defense. "DOD Terminology Program," 2017. http://www.dtic.mil/doctrine/dod_dictionary/.

Department of Defense. *Joint Publication 3-12 (R) Cyberspace Operations.* Department of Defense, February 5, 2013. http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf.

Dismounted Soldier Training System. Intelligent Decisions, 2017. http://www.intelligent.net/news/dismounted-soldier-training-system-0812.

Dunnigan, James F. *The Complete Wargames Handbook: How to Play, Design, and Find Them*. Revised, Subsequent edition. New York, N.Y: Quill, 1992.

"Enabling Learning Objectives." Unpublished manuscript, May 2017. Microsoft Word file.

Freeman, Michael E. "Pushing the Envelope of Pedagogical Gaming: Dark Networks." *PS: Political Science & Politics* 50, no. 04 (October 2017): 1083–88. https://doi.org/10.1017/S1049096517001251.

Garamone, Jim. "Cyber Command Deputy Details Formation of Cyber Mission Force." U.S. DEPARTMENT OF DEFENSE, June 22, 2016. https://www.defense.gov/News/Article/Article/809904/cyber-command-deputy-details-formation-of-cyber-mission-force/.

Gjertsen, Eyvind Garder B. "Use of Gamification in Security Awareness and Training Programs." *98*, 2016. https://brage.bibsys.no/xmlui/handle/11250/2403232.

Griffin, Daniel. "Resources: Gamification in e-Learning." Ashridge Executive Education. Accessed August 14, 2017. https://www.ashridge.org.uk/virtual-ashridge/elearning-insights/resources-gamification-in-e-learning/.

Hardingham, Ian. *Frozen Synapse: A Simultaneous Turn-Based Strategy Game / Turn-Based Tactical Game!* Mode 7 Games, 2011. http://www.frozensynapse.com/.

Hays, Robert T. "The Effectiveness of Instructional Games: A Literature Review and Discussion." Orlando, FL: Naval Air Warfare Center Training Systems Division: DTIC Document, 2005.

Herr, Christopher, and Dennis M. Allen. "Video Games as a Training Tool to Prepare the Next Generation of Cyber Warriors." *Software Engineering Institute*, July 2015. https://doi.org/10.1145/2751957.2751958.

Hunicke, Robin, Marc Leblanc, and Robert Zubek. "MDA: A Formal Approach to Game Design and Game Research." *Press*, In Proceedings of the Challenges in Games AI Workshop, Nineteenth National Conference of Artificial Intelligence, 2004, 5.

Hussain, Talib S., and Susan L. Coleman, eds. *Design and Development of Training Games: Practical Guidelines from a Multidisciplinary Perspective*. New York, NY: Cambridge University Press, 2015.

Khosrow-Pour, Mehdi, ed. *Encyclopedia of Information Science and Technology, 3rd Ed.* 3rd ed. IGI Global, 2015. https://doi.org/10.4018/978-1-4666-5888-2.

Kim, Jung Tae, and Won-Hyung Lee. "Dynamical Model for Gamification of Learning (DMGL)." *Multimedia Tools and Applications* 74, no. 19 (October 1, 2015): 8483–93. https://doi.org/10.1007/s11042-013-1612-8.

Laamarti, Fedwa, Mohamad Eid, and Abdulmotaleb El Saddik. "An Overview of Serious Games." *International Journal of Computer Games Technology* 2014 (2014): 1–15. https://doi.org/10.1155/2014/358152.

Lavrenov, Anton. "Konva.Js - JavaScript 2d Canvas Library." Konva.js - JavaScript 2d canvas library. Accessed October 14, 2017. https://konvajs.github.io/index.html.

Long, David T. "CyberWar:2025." Repository. GitLab, 2017. https://gitlab.nps.edu/dtlong/cyberwar.

Looyestyn, Jemma, Jocelyn Kernot, Kobie Boshoff, Jillian Ryan, Sarah Edney, and Carol Maher. "Does Gamification Increase Engagement with Online Programs? A Systematic Review." *PLOS ONE* 12, no. 3 (March 31, 2017): e0173403. https://doi.org/10.1371/journal.pone.0173403.

Mak, Heong Weng. "U.S. Army Begins Search for Next-Gen Game Based Training." Gamification Co, September 30, 2015. http://www.gamification.co/2015/09/30/u-s-army-begins-search-for-next-gen-game-based-training/.

Marczewski, Andrzej. “Understanding Intrinsic Motivation with RAMP.” Gamification Co, May 1, 2013. http://www.gamification.co/2013/05/01/understanding-intrinsic-motivation-with-ramp/.

Microsoft Studios. *Age of Empires*. Redmond, WA: Microsoft Studios, 1997. https://www.ageofempires.com/.

Pandey, Asha. “6 Killer Examples of Gamification in ELearning.” eLearning Industry, October 6, 2015. https://elearningindustry.com/6-killer-examples-gamification-in-elearning.

Perla, Peter P. *The Art of Wargaming: A Guide for Professionals and Hobbyists*. Annapolis, Md: Naval Institute Press, 1990.

Plunkett, Luke. “America’s Army: Super-Effective.” Kotaku. Accessed November 9, 2017. https://kotaku.com/5407142/americas-army-super-effective.

Prensky, Marc. “‘Simulations’: Are They Games?” In *Digital Game Based Learning*. New York, NY: McGraw-Hill, 2001.

Reiners, Torsten, and Lincoln C. Wood, eds. *Gamification in Education and Business*. Cham: Springer International Publishing, 2015. https://doi.org/10.1007/978-3-319-10208-5.

Riccitiello, John. “Unity Technologies.” Unity3D, June 8, 2005. https://unity3d.com.

Schell, Jesse. *The Art of Game Design: A Book of Lenses*. Second edition. Boca Raton: CRC Press, 2015.

“Terminal Learning Objectives.” Unpublished manuscript, May 2017. Microsoft Word file.

The Vice Chairman of the Joint Chiefs of Staff. “Joint Terminology for Cyberspace Operations.” The Vice Chairman of the Joint Chiefs of Staff, November 2010. http://www.nsci-va.org/CyberReferenceLib/2010-11-joint%20Terminology%20for%20Cyberspace%20Operations.pdf.

Thomas, Neil. *Wargaming: An Introduction*. Stroud: Sutton Publishing, 2005.

Thompson, Michael, and Cynthia Irvine. “CyberCIEGE: A Video Game for Constructive Cyber Security Education.” *Call Signs* 6, no. 2 (2015).

United States Army. *America’s Army*. Windows. United States Army, 2002. https://www.americasarmy.com/.

———. “ART 5.9.1: Conduct Cyberspace Operations.” Department of Defense, February 27, 2013. https://rdl.train.army.mil/catalog-ws/view/100.ATSC/AFBAB9EB-8336-4798-961E-DF8009B23537-1361948176953/report.pdf.

———. “Engagement Skills Trainer (EST).” USAASC, December 21, 2015. http://asc.army.mil/web/portfolio-item/engagement-skills-trainer-est/.

United States Army Cyber Center of Excellence. “Information Assurance Training Center,” 2017. https://ia.signal.army.mil/dodiaa/.

Volo Media Ltd. “Web Version of the Classic Diplomacy Board Game.” Play Diplomacy Online, 2017. http://www.playdiplomacy.com/.

Wells, H. G. *Little Wars*. Dodo Press, 2009.

Zahir, Saboor, John Pak, Jatinder Singh, Jeffrey Pawlick, and Quanyan Zhu. “Protection and Deception: Discovering Game Theory and Cyber Literacy through a Novel Board Game Experience.” *ArXiv:1505.05570 [Cs]*, May 20, 2015. http://arxiv.org/abs/1505.05570.

Zorz, Zeljka. “Cybersecurity Gamification: A Shortcut to Learning.” Help Net Security, December 8, 2016. https://www.helpnetsecurity.com/2016/12/08/cybersecurity-gamification-shortcut-learning/.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California