Wargaming and the Education Gap: Why *CyberWar: 2025* Was Created

David Tyler Long

ABSTRACT

Wargames have been an integral part of planning operations since the 19th Century. They are designed to teach and educate players on specific learning objectives using real-life problem sets to advance knowledge and understanding of those problems. With the increased focus on cyberspace operations in the past decade, wargaming is the key to teach cyber-based operations and prepare for the future. *CyberWar: 2025* is an innovative and newly designed interactive wargame that brings together cyber practitioners, policy writers, and decision-makers to gain experience and understanding through iterative gameplay within a virtual environment.

I. INTRODUCTION

The cyber domain has emerged in the past decade, with governments racing to keep pace with twenty-first-century technological changes to remain competitive in an era of potential cyber warfare. What started with William Gibson's short story "Burning Chrome" (1982) and his underground but well-known hit novel Neuromancer (1984), the cyberpunk world of hacking and digital espionage has rapidly progressed from science fiction into reality. Gibson's term, "cyberspace," also made the leap from science fiction to describe the new, global, low-intensity fighting domain.[1] Any government entity, terrorist organization, or even a rogue actor can ping, probe, attack, interrupt, deface, or block digitally stored data on any server or device on an open internet-connected network. Cyber touches just about everything in today's world from economics, logistics, transportation, infrastructure, and communication and information systems. In short, any chip-enabled device that transmits or processes data can be jammed, manipulated, accessed, monitored, and controlled through means of cyber tools and actions.

The main issue with cyber is not only what it can do or the means of how it can be used, but how fast it is evolving. Cyber is not a singularity, it cannot be contained or locked into place, and it certainly will not allow itself to remain stagnant. Cyber policy in itself should be the same; it should not be a single document that encompasses specific areas of cyber; instead, it should always be evolving to meet the emerging threats in cyberspace. The world has observed how cyber can be used as a means to engage in low-intensity conflicts (in Estonia in 2007 and then in Georgia in 2008, for example) and as a tool for conducting information operations (the 2016 Democratic National Committee cyber-attacks). Nation-state, non-state, and individual entities have widely adapted cyber-attacks through means such as: denial-of-service, malware, man-in-the-middle, spoofing, social engineering, and exploiting. These cyber-attacks have been used as a way to deny, degrade, disrupt, destroy, or manipulate the adversary in cyberspace.[2]

In recent history, the most common cyber threats have been cyber-crimes, espionage, and intellectual property theft; however, disinformation and malware applications have become more prevalent since 2016.[3] Current policy and doctrine cannot keep up simply because cyberspace is still widely misunderstood, undefined, and rapidly changing. To advance cyber policy and to successfully defend networks from adversarial cyber-attacks, defense planners should turn to wargaming for inspiration. Because many defense planners are typically removed from cyber operations, wargaming provides them a unique vantage for testing the suitability of any single policy by emulating notional cyber crisis scenarios that they otherwise would not experience. Cyber wargames also have tremendous academic value in education, whether they be used to educate cyber operators, cyber unit commanders and staff, or policy makers.

In 2017 at the Naval Postgraduate School, my research colleague, U.S. Army CPT Chris Mulch, and I designed and developed an interactive web-based cyber wargame called *CyberWar: 2025* to simulate and educate players on cyberspace operations. Our end state for *CyberWar: 2025* was to release a fully functional interactive cyber wargame for use in cyber operations and planning instruction courses. We understood the vital application of wargaming and software-based serious games or games for training (GFT), such as Engagement Skills Trainer (EST), America's Army, and Virtual Battlespace 3 (VBS3), to train and educate the military personnel on specific, mission-required tasks.[4] Therefore, we adapted these concepts to address the critical gap of cyberspace operations education within the Department of Defense cyber mission. This article aims to fill the gap in cyberspace operations education and understanding. Moreover, in doing so, to ultimately influence cyber policy through insights gained by cyber wargaming.

II. WARGAMING CYBER

Wargaming has been around for centuries, from the earliest introduction of the first board games in the Roman Era, to the introduction of Chess in the Medieval and Renaissance eras, to the evolution of Chess into Kriegsspiel by the Prussians in the 19th Century, to their extensive use of wargames in World War I, and by many others in following conflicts.[5] The earliest uses

of wargaming involved waging a mock war with moveable game models or pieces on a tabletop map; however, as wargames have evolved into more substantial and complex systems, they often use computers to calculate algorithms and provide an interface for players to advance the game state.[6] The premise of wargaming is to support problem solving and education by using consistent feedback through shared experiences. A scenario, game end state, game database or recording method, objectives, players, digital or physical models, rules and procedures, and an analytical, post-game review are what generally constitute a wargame. Since the 1970s, military map and model wargames evolved into what are now called serious games.[7] Commercial and academic sectors adopted this form of gaming for education, training, and operations research purposes. Serious games have become the form of modern wargaming in which games are a means to gain insight and train players while making the training fun and meaningful.[8] By gamifying the act of waging war, players learn and adapt by, with, and through each other to explore and solve complex situations as well as prepare for the unknown future while maintaining a high level of engagement within the wargame scenario.[9]

Wargaming has thus become a method for formulating, enacting, and analyzing courses of action to achieve a specific aim, whether military kinetic operations, emergency and disaster relief efforts, or doomsday scenarios. One desired goal of wargaming is associated analysis because it is the means of quantifying the data of wargame outcomes for operational purposes.[10] The commonality between most map and model wargaming events is that they are dealing mainly with the physical domain. An event that is tactile and physically observable by nature where the rules are clearly defined such as time, resources, locations, distances, and sequence of actions. Wargaming the physical domain is well understood and practiced, but how can we wargame the cyber domain?

To accurately depict the cyber domain, we need to understand what is observable. For example, network traffic is observable with specific tools or equipment. As such, the time, distance, and location between two network traffic points can be determined because of the physics involved. However, because no two routes are the same or are rarely used simultaneously, the time and distance calculations can be asymmetrical. This asymmetry is the result of hardware limitations, software algorithms, and the protocols used in network data transmission. Consider, for example, a bullet fired from a weapon at a target. In the physical domain, the Law of Universal Gravitation and the three Laws of Motion influence the bullet to move in one general direction towards the target.[11] However, if the bullet misses or does not reach its target, it will eventually impact somewhere or in something along its fired path. This event is observable and can be repeated numerous times with minimal change in the predicted outcome. Conversely, in the cyber domain, there are slightly different rules when it comes to what is observable. For the sake of argument, launching a "cyber bullet," or an offensive cyber-attack, may or may not hit its intended target.[2] In reality, the cyber bullet may not hit anything and will cease to exist. This phenomenon stems from several factors, such as Time to Live (TTL), Address Resolution Protocol (ARP), which is heavily documented in the IEEE 802 standards family and RFC 1180

protocol suites that could potentially influence the flow of data packets.[13] For these reasons, among others, wargaming in the cyber domain is a complicated endeavor, but not impossible.

Generally, wargame design requires deconstructing a problem set down into individual components that are understandable and easy to manage. Wargaming in the cyber domain is no different. Cyber, because of its vast complexity, can be broken down into the significant elements that are aimed at reinforcing the desired learning goals and objectives of the wargame. All other characteristics should be combined or abstracted for simplicity. Establishing a set of rules and game mechanics that mimic the environment as closely as possible is also important. This foundation is the intermediary between the players and the rules. Thus, solid game mechanics, dynamics, and aesthetics (MDA) build the foundation of great wargames. Motivation, goals, player movement, and competition are a few of the mechanical properties, while game state changes, feedback, icons, avatars, and game board pieces making up the dynamics and aesthetics.[14] As stated in *Interactive Wargaming CyberWar: 2025*, we stated that:

> 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. 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. Finally, aesthetics are the visual aspects within the game that connect the design value of the game to human emotion and player experiences. The MDA framework easily ties to its lay counterparts in the form of rules, game, and, ultimately, fun. 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.[15]

The MDA framework is the direct psychological connection between the game designer and the player in which each phase of the framework provides and encourages an experience-driven stimulus or behavior.[16] A major driving factor of *CyberWar: 2025* that involves the MDA framework is the dynamic of player versus player competition. Players become emotionally invested in winning by using the cyber effects at their disposal to outwit and defeat opposing players. This dynamic is the driving force for follow-on game sessions and in indirectly inspiring players to learn and be more successful or daring with their cyber strategy. Relying heavily on the MDA framework to design wargames significantly improves player engagement, therefore increasing the player's understanding and educational value of the wargame.

However, several challenges emerged from exploring how best to develop wargames in the cyber domain. For example, in the physical domain, a map is used to define the attributes of terrain and borders to contain players within a given operational environment. Within the cyber domain, the terrain and borders remain undefined.[17] Additionally, unlike the physical domain, the cyber domain lacks the real physical obstacles that are readily accessible to the game's designers. Avatars, game board pieces, player movement, and competition has to be built and

defined. Specific learning cyber objectives have to be clear, concise, and well established to support the mechanics and dynamics of the MDA framework. These learning objectives must tie to current cyber policy while at the same time, adapt to emerging threats and best cyber practices in order to maintain validity and realism within the cyberspace operations field of study. There also needs to be unstated and non-explicit mechanics to address the risk probability of cyberspace operations, referring back to the "cyber bullet" example, which takes into account dynamic actions within a rapidly changing environment.[18] Realism, complexity, and high replay value are also vital in all wargaming sessions. The end goal is to keep players engaged during a game and learning through repetition, mistakes, and consecutive games[19]. Finally, we wanted to create a game that could assist defense planners in developing cyber policies that would have wide-use application for multiple organizations and entities without being constrained for DoD use only. It is with these design challenges in mind that we created *CyberWar: 2025*.

III. THE GENESIS OF *CYBERWAR: 2025*

In the field of cyber wargaming, there were few options available before the creation of *CyberWar:2025*; most cyber-based wargames were marketed for business and industry.[20] Although revolutionary, these wargames were limited to cybersecurity, incident response, and recovery from a cyber-attack. *CyberWar: 2025* is unique in its ability to allow players to experience a multifaceted attack-and-defend scenario in a simulated cyberspace environment. The overall objective of *CyberWar: 2025* is to accrue as much territory as possible from competing players by accessing and maintaining control of key server nodes and networks, defending your network from these adversaries, and ultimately knocking out adversaries from the game by denying or destroying critical server nodes in their network. Victory implies that players develop and execute a sound cyber strategy using defensive, offensive, or exploitative cyber effects. *CyberWar: 2025* thus gamifies the cyber realm by abstracting and combining the cyber specific minutia of network protocols, devices, and tools into a simplified view and design of cyber-effects, server nodes, network links, and player bases. Designed and developed at the Naval Postgraduate School in 2017, *CyberWar: 2025* began as an innovative wargame concept that underwent four key evolutions before becoming the educational solution that it is now.

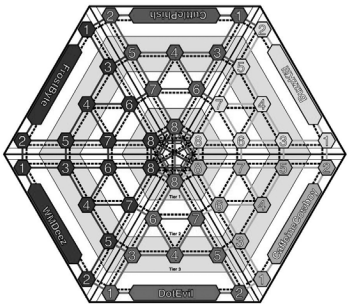

Figure 1. Development View of *CyberWar:2025*

The first evolution of *CyberWar: 2025* took shape in the design of a single large hexagonal game board, composed of six player bases divided into six equal domains, with each holding forty-eight small interconnecting server nodes. Each tier, ranging from one to four, represented the additional cost incurred by the player when executing cyber effects on a tier outside the player's domain. This tiered approach restricts the player's operational movement to the center of the board while signifying that each server node is a control point. The separate domains denoted that other players were operating as unknown actors within the cyberspace domain, each vying for control of the server nodes. Removing player-specific roles such as state or non-state actors allowed players to experiment with their cyber strategy in an equal playing environment devoid of specific game traits or unique player characteristics. During this evolution, cyber effects, costs, and adjudication rules were tested and refined.

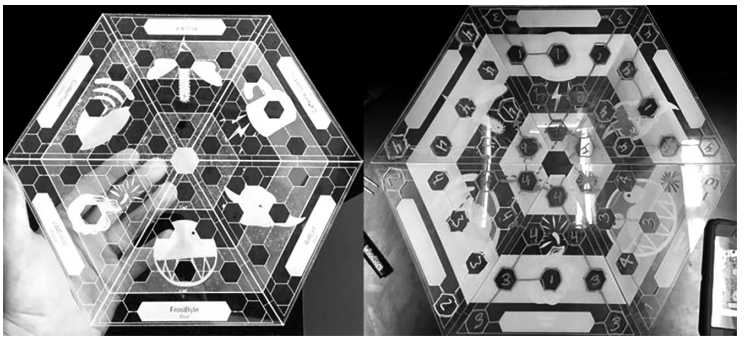

Figure 2. Both Player and Observer Table-Top Boards

The second evolution proved simple enough to play as a tabletop game. This version used six small laser-etched acrylic boards for the players, with a larger six-piece board for the observers and adjudicators. Players were tasked with developing offensive and defensive cyber strategies to disarm or defeat opponents using any of the combined nine cyber effects in the game. Cyber effects available to each player for Defensive Cyber Operations (DCO) or Computer Network Defense (CND) included: Secure, Expel, and Analyze. Overt cyber effects for Offensive Cyberspace Operations (OCO) or Computer Network Attack (CNA) included: Acquire, Manipulate, and Deny. Finally, covert cyber effects for Computer Network Exploitation (CNE) included: Scan, Exploit, and Implant. Each cyber effect had an associated cost, depending on which and where the effect was used. Decisions were written down on acrylic boards using chalk ink markers. Boards where then collected and the game director calculated the results to determine who was winning and losing territory and ultimately the wargame. Consequently, a looming drawback to this approach that emerged was the timing factor. The game mechanics limited course of action selection for six people to approximately twelve rounds, which took about two hours to play, given deliberations. This constraint called for a more efficient solution.

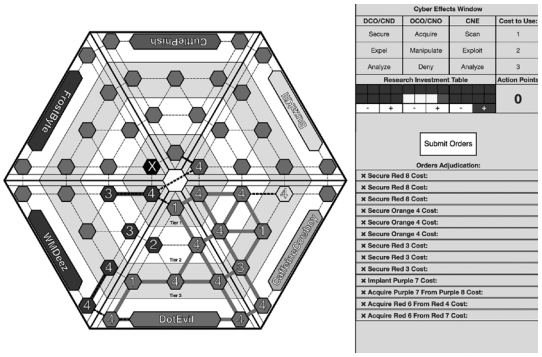

Figure 3. *CyberWar: 2025* Beta Version

The third evolution aimed to reconstruct an interactive and playable beta version of *CyberWar: 2025* in a software environment for responsive game state feedback. In nine months, the computer version of *CyberWar: 2025* was developed entirely from scratch using JavaScript code in order to support cross-platform play with commonly used web browsers such as Firefox, Chrome, and Safari. This improved *CyberWar: 2025*'s efficiency as it became possible to play over forty rounds in a game session within an hour; however, game sessions were limited to time or rounds because the endgame of domination and a few other plugins were not fully developed. The goal of this evolution was to conduct rigorous tests and evaluations through live trial-and-error game sessions. These game demonstrations proved valuable as they provided a platform to track and collect any issues, MDA or otherwise, and garner player reactions and feedback from the game. While the feedback was extremely positive, *CyberWar: 2025* needed several more changes to become a fully functional and interactive wargame.

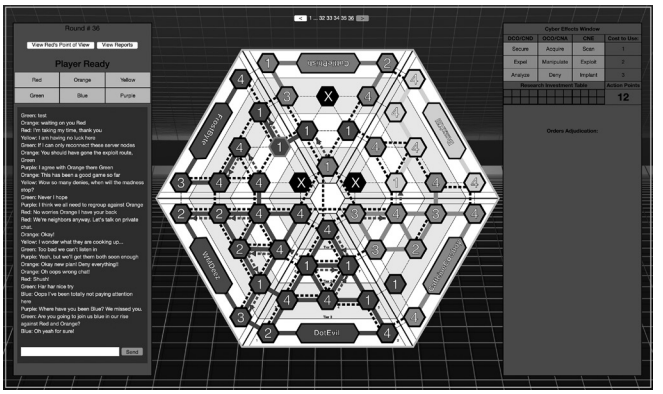

Figure 4. *CyberWar: 2025* Version 1.1 Board from DotEvil's View

The fourth evolution, or the version 1.1 release of *CyberWar: 2025* focused on the implementation of private and public chat to facilitate in-game communication, enable alliances, and provide the ability for players to conduct information operations against others. Other features

included a single endgame scenario, end-of-round reports, game history, minor aesthetic game board changes, a player ready indicator, and an unrestricted observer view. The majority of these changes were issues that were addressed as player feedback during prior beta testing sessions. The final result of this development evolution is to install *CyberWar: 2025* onto the Naval Postgraduate School's GlobalECCO server and open the wargame up to public play over the open internet.[21]

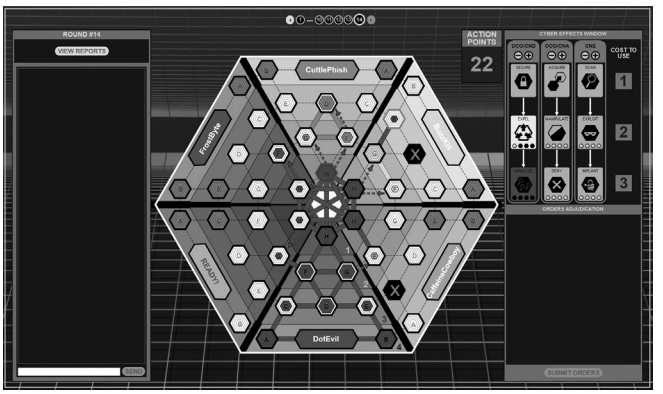

Figure 5. *CyberWar: 2025* Version 1.2 Board Redesign

The NPS GlobalECCO team updated the visuals of *CyberWar: 2025* to make the board view more aesthetically engaging, appealing, and accessible for players by using simplified icons, clearer colors, and icon-based round reports. Version 1.2, the final design for *CyberWar: 2025*, is available for public use on Global ECCO once users have created an account

IV. THE MECHANICS OF *CYBERWAR: 2025*

CyberWar: 2025 sets itself apart from traditional wargaming because players interact with the game through a web browser which provides efficient, timely, and accurate orders adjudication, thus eliminating the factor of human error in calculating results. Using their mouse to click on server nodes adjacent to those the player has already acquired and linked to their base, the browser shows a drop-down actions menu of potential actions from which the player can choose. Upon selecting and confirming these actions, the player's orders are stored in an adjudication queue until the player submits their orders to the server. Each player has a private client view, separate from another player's view, so players cannot interfere with another player's actions or see what other players are doing between each round. After each player has submitted their orders, the client view transmits these actions to the server for adjudication and the game state is updated to reflect the player's results.

CyberWar: 2025 also uses consecutive rounds to denote the passage of time within a game session. While time is not proportional to reality (e.g., one round equals a year), when players take actions or put investments to unlock additional cyber effects, these actions and cyber

effects do not become available until the following round. Resources, in the form of Action Points, represent the currency in which a player has to accumulate and manage throughout the entirety of a game session. Action Points are acquired through gaining and holding territory by accessing the server nodes on the board, either overtly or covertly. After each round successfully adjudicates, the number of positively linked server nodes to that player's base are tallied; that amount is the number of Action Points a player can spend to enact their cyber strategy. These Action Points are for further investment into the remaining six cyber effects or to be used as the cost necessary to launch these cyber effects against other players. Players are recommended to use all their Action Points since they do not carry-over for future rounds.

In the beta version of *CyberWar: 2025,* games were limited to time and rounds played and the player with the most Action Points at the end was deemed the winner; however, with the release of version 1.1, endgames were implemented. The only endgame option currently available is domination. In domination, players fight to hold on to their server nodes and maintain network links. The loss of too many critical server nodes and network links will remove the player from the game, with the player remaining claiming victory.

V. HOW ACTIONS IN *CYBERWAR: 2025* RELATE TO THE OPERATIONAL ENVIRONMENT

Several underlying game mechanics within *CyberWar: 2025* directly simulate real-world effects and events that have been observed in the cyberspace operational environment. The cyber effects of Secure, Acquire, Analyze, Expel, and Scan are straightforward in their correlation between the modeled game environment and the real world. The only slight difference is with the Secure cyber effect. The association of the Secure cyber effect to reality is with the standard practice of hardening servers and other devices on a computer network. The additional mechanic of increasing the sever node value that does not relate is the mathematical probability involved in launching a cyber effect and its success rate. Having a stronger or better computer in cyber does not mean that there is a higher chance of success in a cyberspace operation.

In Department of Defense Joint Publication 3-12, Manipulate is a cyber-attack which "controls or changes information, information systems, and/or networks" for denial or misinformation effects on the intended target.[22] When players use the Manipulate cyber effect, they are by definition launching a spoofing network attack and misattributing their action as another player. However, the attacker can also mask their overt action as their victim, which emphasizes the common practice of "hiding in plain sight." The victim of the attack will think, however, that the attack is coming from another player of whomever the attacking player's manipulate effect identifies. The reasoning behind this cyber effect is to show that cyberspace operations do overlap into the information operations realm. When a defending player notices that an adversary has acquired one of their server nodes within their domain, the typical reaction is to retaliate or acquire that server node immediately. However, if the defending player executes

Scan or Analyze, the attacking player will be correctly identified, and the following actions are solely up to the cyber strategy of the defending player.

Implant is a dual-use cyber effect. Firstly, it modifies the other actions of Acquire, Exploit, Manipulate, and Deny by improving the attacker's odds of success during adjudication. For example, when an attacking player's server node is at the maximum value, and the defending player's server node is the same, Implant reduces the defending player's server node to its minimum for that round, thus increasing the odds of success. *CyberWar: 2025*'s Implant effect is a combination of disrupt and degrade in the JP 3-12, because of its dual use as a modifier for offensive and exploitation cyber effects in-game. Implant by itself is always a success just like Scan, Analyze, and Secure; however, the follow-on actions may not always succeed. Secondly, when Implant is used on an adversary's base and is successful, the defending player is temporarily locked out from play for one round in the following turn. This secondary use of Implant is closely related to the ransomware attacks like WannaCry and NotPetya, although players cannot pay out Action Points to revive their network, which is a specific requirement in ransomware.[23] Implant is a straightforward vulnerability cyber effect and similar to its real-life counterparts; however, Implant is over-simplified to reduce the *CyberWar: 2025*'s overall complexity and game mechanics.

The Deny cyber effect is directly tied to the Deny and Destroy definitions within the JP 3-12 of Cyberspace Operations.[24] Within *CyberWar: 2025*, Deny is the "nuclear option" of permanently removing a server node from the game board. The only difference between Deny in the game versus reality is that in most cases when a server or a device is destroyed in the real-world, it can be replaced or rebuilt; *CyberWar: 2025* does not have this mechanic developed as of the version 1.1 release.

There are also a couple of side mechanics that have a direct relationship within the cyberspace operational environment. The most important one is the idea of blockchain by creating a network of networks within the game. In CyberWar: 2025, it is essential to understand the practical application of redundant network paths. When a player has a vast server node network, and a critical server node is denied, that player's entire cyber strategy is drastically less effective. That is until the player regains the lost server node or rebuilds an alternate path, both of which require time, resources, and luck. Another important side-mechanic is the methodology of exploitation. Using Exploit in *CyberWar: 2025* allows an attacking player to gain access to an adversary's server node covertly. However, there can be multiple exploited players on any one server node at a time, which is the exact opposite of the Acquire cyber effect, which only allows one player overt control of a server node. Exploited server nodes are not advertised to the defending player. The only way to identify and remove covert players from their network is to Scan or Analyze and then execute an Expel cyber effect on that specific server node. In the JP 3-12 (R) dated 05 February 2013, exploitation was not explicitly addressed in terms of pertinent it is to the cyber mission. However, in the June 2018 publication of the JP 3-12,

exploitation covers topics of target access: intelligence, surveillance, reconnaissance, command, control, and enabling offensive capabilities.[25] Exploitation is vital to cyberspace operations because it drives the intelligence cycle and enables follow-on actions. Exploitation is represented in *CyberWar: 2025* by allowing players to operate well within an adversary's domain and execute cyber effects without having to be overtly identifiable.

VI. FILLING THE CYBER EDUCATIONAL GAP THROUGH EXPERIENCE

CyberWar: 2025 was designed to be played iteratively and supported though feedback during instructor-led sessions. It is a means to simulate abstracted and high-level cyberspace operations in an engaging and responsive learning environment. The underlying mechanics do not exclusively teach cyber or cyberspace operations; however, *CyberWar: 2025* opens up the room for discussion between both seasoned cyber practitioners and those who are new or have little to no experience with or understanding of cyber-based operations. Through open dialogue in post-game sessions, players discuss their envisioned cyber strategy and describe their experiences and whether their strategy was successful or not. During live sessions, players are open to asking questions on how specific cyber effects work and the conditions in which to use them; this happens when players are first introduced to the game and its interface. For example, in the initial stage of a new game session, players have unlocked for them the primary cyber effects of Secure, Acquire, and Scan to execute their strategy. Limiting the players to these effects early on keeps players focused on the essential tasks of seek, attack, and defend. However, as players progress and acquire more server nodes, they are able to unlock the additional cyber effects, if they choose to do so. This phase of the game is where the questions on *CyberWar: 2025*'s mechanics begin. When players discuss their actions openly, at least for players who are learning the game for the first time, they understand the game better and can adapt to the mechanics of *CyberWar: 2025* quickly.

As a game session progresses through round after round, players will find that the network map ebbs and flows in control based on the multiple actions from each player. *CyberWar: 2025* is designed so that each consecutive round in a single game session provides new challenges for a player overcome. For example, a player who has held a defensive strategy so far may find that in the next round, several players have infiltrated their network. Therefore, they are forced to counter-attack and regain the server nodes in their domain. Another example is when the playable game board is drastically reduced or when players' network is diminished in size because of a successful adjudication from a deny cyber effect. From this point on, players are forced to work around or adopt a new cyber strategy because of the condensed amount of available server nodes left on the board. The dynamic changes that can occur are all viable teaching points that an instructor will explain in the post-game analysis of a session.

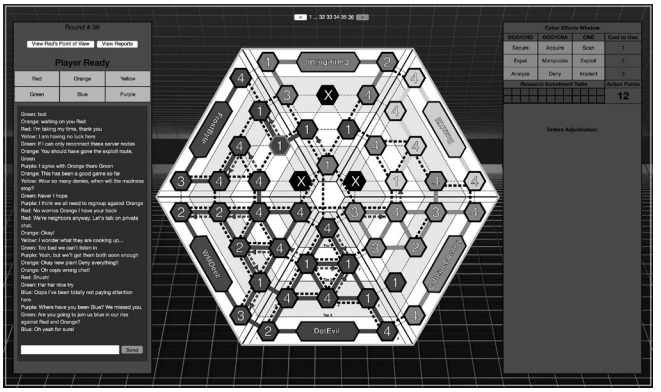

Figure 6. *CyberWar: 2025* Version 1.1 Board Entire Observer View

When a game session concludes, the instructor can reopen the discussions using the observer view of the game board. Going back in time using the history tab embedded in the client game view, the instructor can replay the game round by round, conversing with players directly on their cyber strategies, desired expectations, and outcomes. At the same time, the adversarial players can comment on how their actions may have impacted the initial player's strategy. After the game review is complete, players are recommended to replay the *CyberWar: 2025* a second time and encouraged to adopt a different cyber strategy to see if their outcomes change.

The significant benefit in *CyberWar: 2025* is that every game is unique because of the underlying adjudication mechanics and various player actions. With each new game session, players will rarely have the same experience in successive games. Through playing iterative game sessions, players learn by gaining experience through trial and error. During the beta testing phase of *CyberWar: 2025*, there were over 25 live player demonstrations, each averaging four hours in length per session. The structure of each demonstration was a quick initial block of instruction on the game and then a quick "hands-on" play session. Immediately afterward, *CyberWar: 2025* was played for approximately an hour and a half with a 30-minute post-game review. Finally, the game was played again for another hour and a half with another 30-minute game review. Players consistently noted that they felt more comfortable with the game during the second play session, and most players adopted a cyber strategy vastly different from their first playthrough. It is also crucial to note that players interacted with each other and the game director during the post-game review discussions. When the *CyberWar: 2025* demonstration concluded, players and observers felt more comfortable with and knowledgeable about cyberspace operations.

CONCLUSION

Wargaming is an integral part of planning and execution of operations and it has influenced policy and doctrine across all services of the military and government. The practical application of wargaming is limitless with new ideas and innovations being tested every year. We have conducted wargames for land, sea, and air warfare; cyberspace should be no different. *CyberWar:2025* is that means for wargaming cyberspace operations, and it is a starting point for future cyber wargames.

Author Bio

David Tyler Long

United States Army Master Sergeant David "Ty" Long is a field operations and cyber researcher for a Department of Defense testing and evaluation center at Kirtland Air Force Base, Albuquerque, NM. He is the creator and developer of *CyberWar: 2025*, which was the direct result of the research work that he and co-writer, Major Chis Mulch, completed during their Master's studies in Political Warfare and Information Strategy at the Defense Analysis Department, Naval Postgraduate School. Their thesis, titled "Interactive Wargaming *CyberWar: 2025*," described the vital need for cyber wargaming and the development of CyberWar: 2025. Master Sergeant David Long is also a senior software engineer and formerly cyber-warfare and information operations practitioner for the United States Department of Defense.

NOTES

1. William Gibson, *Burning Chrome*, Reprint edition (New York: Harper Voyager, 2003); William Gibson, *Neuromancer* (New York: Ace Books, 1984).
2. Department of Defense, "Joint Publication 3-12 Cyberspace Operations" (Department of Defense, June 8, 2018), II–7, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf?ver=2018-07-16-134954-150.
3. Misha Glenny and Camino Kavanagh, "800 Titles but No Policy—Thoughts on Cyber Warfare," *American Foreign Policy Interests* 34, no. 6 (November 1, 2012): 287, doi:10.1080/10803920.2012.742410; Carl Bildt et al., "The Arms Race in Cyberspace," *Project Syndicate*, November 17, 2017, https://www.project-syndicate.org/bigpicture/the-arms-race-in-cyberspace.
4. United States Army, "Engagement Skills Trainer (EST)," *USAASC*, December 21, 2015, http://asc.army.mil/web/portfolio-item/engagement-skills-trainer-est/; United States Army, *America's Army*, Windows (United States Army, 2002), https://www.americasarmy.com/; Susan G. Straus et al., "Collective Simulation-Based Training in the U.S. Army: User Interface Fidelity, Costs, and Training Effectiveness" (Santa Monica, CA: RAND Corporation, n.d.), 1–3, https://www.rand.org/pubs/research_reports/RR2250.html; Christopher Herr and Dennis M. Allen, "Video Games as a Training Tool to Prepare the Next Generation of Cyber Warriors," S*oftware Engineering Institute*, July 2015, 5, doi:10.1145/2751957.2751958.
5. Roger C. Mason, "Wargaming: Its History and Future," *The International Journal of Intelligence, Security, and Public Affairs* 20, no. 2 (May 4, 2018): 77–83, doi:10.1080/23800992.2018.1484238.
6. David Tyler Long and Christopher M. Mulch, "Interactive Wargaming CyberWar: 2025" (Naval Postgraduate School, 2017), 11, Calhoun, http://hdl.handle.net/10945/56758; Mason, "Wargaming: Its History and Future," 88.
7. Mason, "Wargaming: Its History and Future," 91.
8. Torsten Reiners and Lincoln C. Wood, eds., *Gamification in Education and Business* (Cham: Springer International Publishing, 2015), 4, doi:10.1007/978-3-319-10208-5.
9. Peter Perla and Ed McGrady, "Why Wargaming Works," Naval War College Review 64, no. 3 (January 2011): 2.
10. Peter P. Perla, "War Games, Analyses, and Exercises," *Naval War College Review* 40, no. 2 (1987): 1, https://digital-commons.usnwc.edu/nwc-review/vol40/iss2/7.
11. "Law of Gravity," accessed July 25, 2019, https://physics.weber.edu/amiri/physics1010online/WSUonline12w/OnLine-CourseMovies/CircularMotion&Gravity/reviewofgravity/ReviewofGravity.html; "Newton's Three Laws of Motion," accessed July 25, 2019, https://www.pas.rochester.edu/~blackman/ast104/newton3laws16.html.
12. Department of Defense, "Joint Publication 3-12 Cyberspace Operations," II–7.
13. "LMSC, LAN/MAN Standards Committee (Project 802)," accessed July 25, 2019, http://www.ieee802.org/; C. J. Kale and T. J. Socolofsky, "TCP/IP Tutorial," accessed July 25, 2019, https://tools.ietf.org/html/rfc1180.
14. 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.
15. Long and Mulch, "Interactive Wargaming CyberWar: 2025," 26–27.
16. Hunicke, Leblanc, and Zubek, "MDA: A Formal Approach to Game Design and Game Research," 2.
17. Department of Defense, "Joint Publication 3-12 Cyberspace Operations," I–12.
18. "Learning Cyber Operations Through Gaming: An Overview of Current and up and Coming Gamified Learning Environments | CSIAC," accessed July 25, 2019, https://www.csiac.org/journal-article/learning-cyber-operations-through-gaming-an-overview-of-current-and-up-and-coming-gamified-learning-environments/.
19. Herr and Allen, "Video Games as a Training Tool to Prepare the Next Generation of Cyber Warriors," 7.
20. Tucker Bailey, James Kaplan, and Allen Weinberg, "Playing War Games to Prepare for a Cyberattack," *McKinsey Digital*, July 2012, https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/playing-war-games-to-prepare-for-a-cyberattack.
21. "Home - GlobalECCO," accessed July 26, 2019, https://globalecco.org/.
22. Department of Defense, "Joint Publication 3-12 Cyberspace Operations," II–7.
23. Josh Fruhlinger, "The 6 Biggest Ransomware Attacks of the Last 5 Years," *CSO Online*, April 5, 2019, https://www.csoonline.com/article/3212260/the-5-biggest-ransomware-attacks-of-the-last-5-years.html.
24. Department of Defense, "Joint Publication 3-12 Cyberspace Operations," II–7.
25. Ibid., IV–9, IV–8, II–1.