Cyber War: 2025

Suggested Reading

Department of Defense, "Cyberspace Operations," Joint Publication 3-12 (Washington, DC: Department of Defense, 2018), esp. chapters II and IV: https://fas.org/irp/doddir/dod/jp3_12r.pdf

David Tyler Long, "Wargaming and the Education Gap: Why *CyberWar: 2025* was Created," *The Cyber Defense Review* (Spring 2020): 185–198.

MSG David Tyler Long, "Cyberspace Operations Training Using *CyberWar: 2025*," *CTX* vol. 10, no. 2 (Summer 2020): https://nps.edu/documents/110773463/122717000/Vol10N02+CTX+.pdf#page=35

Key Concepts

CyberWar: 2025 is a turn-based multiplayer cyber wargame that highlights the three core cyber-effect categories of defensive cyberspace operations (DCO), offensive cyberspace operations (OCO), and computer network exploitation (CNE). The premise of *CyberWar: 2025* was to create a collaborative training environment in which leaders, policymakers, and non-technical personnel partner with those who have experience in cyberspace operations, cybersecurity, or a similar technical field. *CyberWar: 2025* simulates a realistic cyberspace operational environment and models the effects of current real-world cyber activities in a non-technical and straightforward manner. The complexity of *CyberWar: 2025* lies within the core game mechanics of randomization and dynamic board changes, which challenge each player from one round to the next.

The objective of *CyberWar: 2025*, like many strategic games, is a simple one: to accrue territory, eliminate competitors, and dominate the gameboard. A player achieves these objectives by gaining access to and controlling key server nodes, defending one's network, and knocking adversaries out of the game by denying or destroying critical nodes and networks. Developing and executing a sound strategy through the use of defensive, offensive, and exploitative cyber effects are key to victory.

Three Defensive Cyberspace Operations (DCOs): *Analyze, Secure*, and *Expel*
Analyze is an enhanced scanning effect that scans the player's entire network of linked server nodes to reveal any opponents that are covertly operating within the player's network. It is also able to attribute a *manipulate* effect to the attacker who launched the effect.
Secure is the base action for all defensive cyber operations. As in the real world, this cyber effect hardens a server node by increasing its defensive value. Unlike the real

world, however, the *secure* value also serves as the attack value when launching OCO and CNE cyber effects against other players, thus influencing the strength of the attack.
Expel removes any hidden or exploiting opponents from a player's overtly controlled server node. An exploiting player can also use it to remove other covert players from the node, but control of the node remains with the node's overt owner.

Three Offensive Cyberspace Operations (OCOs): Acquire, Manipulate, and Deny
Acquire is the base action for all offensive operations. If an adjacent server node is unoccupied, *acquire* automatically brings that node under the player's overt control.
Manipulate is similar to *acquire*, with an added feature: it allows the attacker to deceive—or "spoof"—the defender into thinking the attack came from one of the other players.
Deny permanently disables a server node and removes it from further use in the game, thus limiting player movement on the board. It can be thought of as the "nuclear option."

Three Computer Network Exploitation (CNE) Effects: *Scan*, *Exploit*, and *Implant*
Scan is the base action for all exploitation operations. It reveals the defensive value of an adjacent server node and any overt and covert links to and from that node.
Exploit is a covert *acquire* effect, in which the attack remains hidden from the targeted node's owner. This reflects the difficulty of attribution in actual cyberspace.
Implant can be used against a server node or an opponent's base. When used against a node, it reduces the node's defensive value to 1, leaving it vulnerable to occupation. When used against a base, *implant* denies the targeted player a turn in the next round. This is similar to a ransomware attack in real life, except that the game does not allow the targeted player to pay a ransom in Action Points and restore the turn.

Overt and Covert Cyber Operations
One of the most prominent aspects of cyberspace is that much of its activity takes place out of sight, "below the radar." Anonymity is both a feature and a bug of cyberspace: on the one hand, users are able to share information, ideas, and opinions more freely than if they were easily identifiable. On the other hand, bad actors such as internet trolls and criminals, as well as state-level adversaries, can hide effectively while causing real harm.

Players in *CyberWar: 2025* can choose whether to exert overt or covert control over server nodes as they build their networks and seek to undermine opponents. Overt control is a way of staking a claim and establishing dominance; it also may be a useful way of drawing other players' attention away from covert activity the player is conducting elsewhere.

Key Mechanisms

The first fundamental mechanism of *CyberWar: 2025* is that the player roles are agnostic. Instead of assigning players specific roles that reflect current cyber-threat problem sets, such as states, hackers, criminals, and so on, and giving them a defined set of capabilities, all players in this game are equal cyber actors on the gameboard. Players can adjust their role at any time during the game session to suit their cyber strategy and are free to experiment and adapt to the continually changing game environment. This open structure helps players quickly grasp the value, scope, and limitations of cyber strategies and effects.

The second key mechanism is the randomization of cyber effects, which is achieved through the integration of a dice roll and the player's attack/defense base value, or Server Node strength (which increases or decreases according to the player's activities). The dice roll yields a randomized value between 1 and 100, simulating a 100-sided die. Base value and the dice roll combine to provide the player's attack/defend value; if it is higher than the opponent's value, then the action is successful. This randomization also ensures that no two game sessions are identical, even though their outcomes may be similar.

The third mechanism that underlies gameplay is a single-player viewpoint that can be clouded by the "fog of war." These aspects reflect the real world in that actions in the cyber domain are not readily observable because cyberspace is not tactile. The "fog of war" effect derives directly from the single-player view: while players see all actions happening within their domain, actions occurring outside of their domain are hidden. As players venture out on the board and expand their cyber networks by using OCO or CNE cyber effects, the larger operational environment becomes more visible to them.

Finally, every player must take into account resource management and the timing of effects when planning and executing a cyber strategy. To be successful in the game, players must invest resources in the cyber effects they use to execute their game strategy. Developing and launching each cyber effect has a cost; these accrue when the cyber effects cross over domain boundaries. The purpose of this mechanic is to simulate the real-world operational costs required to initially gain access to a network, such as bypassing a firewall, intrusion detection system, or network gateway.