Far too often, cyberspace is a warfighting domain that is neglected or misrepresented in wargaming — and misunderstood in the planning of operations. Merlin is a cyber module for wargames designed to address those gaps.

Historically, cyber operators and traditional operators on land, air, and sea have not interacted enough. The two communities lack critical knowledge about each other and of the skills that future warfare will require:

- An understanding of the impact of cyber operations on traditional warfare.
- The ability to synchronize and integrate operations.
- A full understanding of how cyber can best support traditional operators.
- A common language to develop all-domain campaigns that include cyberspace.

At each turn in a wargame incorporating Merlin, players can create offensive or defensive cyber tradecraft by describing a few key characteristics:

- **Target/defended asset**, e.g., sensors, weapons systems or communications infrastructure
- **Access approach**, e.g., remote access or human-enabled access
- **Effect**, e.g., deny adversary use of networked communications (offensive), contain, publicize (defensive)
- **Outcome**, e.g., adversary (offensive) or U.S. (defensive) headquarters is unable/able to communicate with deployed forces

This four-part taxonomy is key to enabling planners from both cyberspace and physical domains to communicate simply and intuitively, using common terms. Whether for wargaming or for actual operational-level planning, our classification system can be used to describe any cyber activity, offensive or defensive.
Every cyber effect played in a Merlin game is sent to the “Merlin Spell Book,” a Python-based tool that uses empirical data to track cyber tradecraft. Each time a team uses a cyber weapon, the Spell Book assigns requirements and results:

- **Personnel** required for development and execution
- **Time** required for development and execution
- Probability of **success**
- Probability the adversary will discover and **burn** the tradecraft, blocking its further use

Merlin caps the cyber personnel resources each team can use, but those resources are “backcasted”—employed before the date of the game scenario. The artificial ability of players to execute cyber effects instantly while backcasting the requirements encourages creativity and continual involvement of the cyber domain in the action. Backcasting actually increases lessons learned about the role of time and resources in cyberwarfare.

Merlin was developed by the CNA wargaming team for the Air Force Research Laboratory to help cyberspace domain planners and physical domain planners communicate and coordinate. It is available in classified and unclassified versions.