MERLIN: WARGAMING CYBER OPERATIONS TO TRANSFORM ALL-DOMAIN WARFARE

Merlin brings cyberspace operators and traditional warfare operators together to innovate

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.
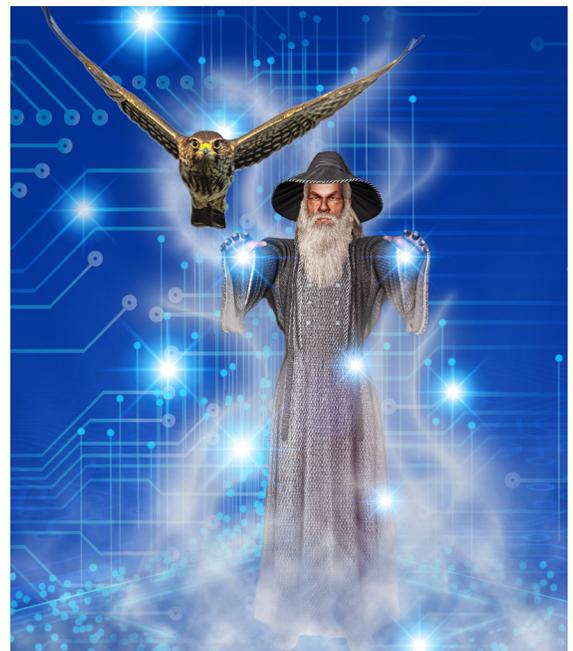
8-Step End-to-End Cyber Tradecraft Development and Execution Process

Joint Targeting Process → Targeting → [Decision Point] → **Method** → Initial Preparation → Final Preparation → Approvals → Execute Mission → [Decision Point] → Operation Assessment

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.

ABOUT CNA

CNA is a nonprofit research and analysis organization dedicated to the safety and security of the nation. It operates the Center for Naval Analyses — a federally funded research and development center (FFRDC) serving the Department of the Navy — as well as the Institute for Public Research. CNA develops actionable solutions to complex problems of national importance. With nearly 700 scientists, analysts and professional staff, CNA takes a real-world approach to gathering data. Its one-of-a-kind Field Program places analysts on aircraft carriers and military bases, in squad rooms and crisis centers, working side-by-side with operators and decision-makers around the world. CNA supports naval operations, fleet readiness and strategic competition. Its non-defense research portfolio includes criminal justice, homeland security and data management.

For additional information, or to set up a time to discuss the module in additional detail, please contact:

Catherine K. Lea | leac@cna.org | 703-824-2371
Jeremy Sepinsky | sepinskyj@cna.org | 703-824-2519