WAR GAMING
UNITED STATES NAVAL WAR COLLEGE

Role of Cyber in War Gaming[1]

Stephanie Helm
Senior Military Analyst
War Gaming Department

War games are valuable in helping military leaders think objectively about future complex problems. As the War Gamer's Handbook explains:

> War games are a tool for exploring decision-making possibilities in an environment with incomplete and imperfect information (Herman, Frost, & Kurz, 2009). Additionally, a value unique to all war games is the occurrence of previously unknown issues, insights, or decisions that arise during the conduct of a game. War game participants may make decisions and take actions in a game that even they would not have anticipated, if not for the game environment (Perla, 2012).

What better way to address the role of cyberspace in future operations? With the establishment of U.S. Cyber Command and development of the future cyber force structure to support military operations, military leaders will be faced with some measure of uncertainty and unknowns when integrating cyberspace capabilities with other military operations. This is unfamiliar territory for most combat arms professionals. Furthermore, doctrine is scarce and operational lessons learned are not widely available to aid commanders. War gaming offers opportunity for non-cyber warfighters to gain familiarity with cyber lexicon and processes and for cyber experts to refine their role in supporting military operations. Together, as part of a shared phenomenological

[1] The opinions, conclusions, and recommendations expressed or implied are those of the authors and do not necessarily reflect the views of the U.S. Naval War College, the Department of the Navy, or the Department of Defense.

experience, the warfighters and cyber professionals can explore the potential value or risk of military cyberspace operations which can lead to insights or support to decision making.

Some war game sponsors are already thinking along these lines. The Navy Title X Global and U.S. Strategic Command Deterrence and Escalation Review and Game (DEGRE) series have included cyberspace operations in their game objectives or research questions for several consecutive years. Through these games and a few others (e.g., Indo-Pacific War Game and Maritime Stability Operations Game), the representation of cyberspace operations has evolved from a very rudimentary, stand-alone cell to a seamlessly integrated component of the player teams. Along the way, the war game project management process, war game team composition and war game designs have accommodated the integration of cyberspace in order to present the players a plausible dilemma and the opportunity to make a cyber-related decision or order a cyber-related action.

Commanders face a variety of challenges when contemplating cyberspace operations within their force operations. Visualization or Common Operational Picture (COP) of the cyber domain is problematic, cyber-dependent operational processes present a vulnerability to mission with unclear mitigating options, cyber-derived intelligence is highly classified and cumbersome to use, cyber force structure is not well defined, attribution of malicious cyber activities is difficult to prove, cyber capabilities (TTPs, weapons, platforms) are highly sensitive and generally not shared outside the cyber community, and cyber law and execution authorities are viewed as overly restrictive or unclear. Including these unique considerations within the intellectual confines of a war game may be useful in helping military leaders to think through the ramifications of cyber-related issues in warfare. The war game is an opportunity for players to explore the cyberspace “art of the possible” along with the realistic challenges of combining cyberspace operations with traditional military warfare to gain insights for future contingencies.

The challenges posed by integrating cyberspace operations in an actual military environment mirror the challenges related to integrating cyberspace operations in war games. Each of the aforementioned cyber-related issues translate to a similar challenge in war gaming. For this reason, each game director must decide how to represent germane cyber issues without miring players in extraneous concerns and adjust the overall process to support cyber integration. The integration of cyberspace operations into war games affects the entire game project management team. In future articles, the techniques and current best practices for game directors, game designers, adjudicators, analysts, knowledge managers, and the ONI Detachment will be examined to establish where cyberspace considerations may be applicable which may help inform future war game efforts.