Mastering Cyberspace in MILITARY OPERATIONS

EUCOM GAINS BATTLEFIELD ADVANTAGES THROUGH THE USE OF INFORMATION SYSTEMS

By **U.S. European Command**

Attack your enemy where he is unprepared, appear where you are not expected.
— Sun-Tzu, *The Art of War*

As the information age continues to change our world dramatically, an understanding of cyberspace using a familiar set of terms and a logical battlefield framework is essential to victory. Today, as throughout history, successful leaders must identify and take advantage of key moments in time and space to win. Operations in cyberspace are no different. Understanding the potential impact that cyberspace has on operations, developing a framework to understand and manage these effects, and empowering cyber mission forces can offer a distinct advantage.

Cyberspace adds a level of complexity in which actors can generate effects across a full range of military and civil activities because information systems are becoming increasingly prevalent in nearly every aspect of military operations. To win in the 21st century, leaders must know the capabilities and limitations of their systems through a methodology that brings coherence and understanding to the potential impacts of cyberspace.

Understanding the significant potential impact of cyberspace is essential to maintaining cyber superiority: It's the ability to effectively use systems at the right time and tempo. Cyberspace is a man-made dominion that consists of geography, hardware, logical networks (software/apps), personas (user ID and logon information) and people. Today, nearly 40 percent of the world's population has Internet access compared to less than 1 percent 20 years ago. So maintaining safety in cyberspace is becoming increasingly more difficult. The number of Internet users increased tenfold between 1995 and 2001, reaching 1 billion in 2005, with another billion by 2010, and surpassing 3 billion total users in 2015, according to the Internet Live Stats website. With over 7 billion people on the planet today, nearly half the world's population has access to this operational environment, the International Telecommunications Union's website stated.

A British Signals Regiment soldier prepares communications equipment for Exercise Combined Endeavor, the pre-eminent command, control, communications and computer exercise for NATO and Partnership for Peace multinational operations. MAJ. JASON ROSSI/U.S. AIR FORCE

When you include the coming wave of the Internet of things, including lights, cameras and cars, the number will surge to an estimated 20 billion to 30 billion — approximately three to five times the number of people on the planet. This means that, because all networks are linked in some manner, commanders will face increasing challenges to recognize change, act to assure cyber superiority and conduct operations.

Developing a framework to improve understanding of cyberspace enables leaders to rapidly recognize change and lead transitions. The Capstone Concept for Joint Operations in 2020 describes how future adversaries can become more capable using cyberspace and continue to challenge our ability to operate. Leaders must have a methodology to rapidly relate geography, hardware, logical networks, personas and people into a simple framework that enables change recognition and allows them to act, because both framework and methodology are essential to winning.

One method is to use the terrain analysis model known as observation, cover and concealment, obstacles, key terrain, avenues of approach, or OCOKA, a term that most military planners are familiar with. Just as these factors must be analyzed with respect to the mission, type of operation, level of command and composition of forces, along with weapons/equipment expected to be encountered, leaders can also use this framework in cyberspace. Observation of fields of fire can be used to identify potential engagement areas where maneuver force systems and platforms are most susceptible to observation and kinetic or nonkinetic fire. Understanding these danger areas will help protect assets.

The importance of cover and concealment in placing tactical military hardware is analogous to the importance of personas in protecting network access. The process of devising cover and concealment of tactical hardware is straightforward, but logical networks, personas and people require much more thought and teamwork to reduce risks and exposure. In a tactical environment, obstacles are typically natural or man-made terrain features that stop, impede, slow or divert movement. These same concepts apply in cyberspace. Understanding how to create obstacles by using hardware, such as firewalls and proxy servers, and software, such as digital identification and two-factor authentication, is essential to disrupting an adversary's ability to influence operations.

Identifying key or decisive terrain is more than relating hardware to a physical location; it involves identifying key systems like missile defense, fire control, and electric power plants that are essential to successful operations. Each of these are examples of logical networks and could be key terrain. People and personas could also be key terrain because they serve as access points to systems. Identifying key terrain enables leaders to turn each feature into a named area of interest and determine placement of the appropriate overwatch.

A Ukrainian soldier attends a 2014 Cyber Endeavor seminar, part of a U.S. European Command initiative to improve collective cyber security of NATO allies and partners. MAJ. JASON ROSSI/U.S. AIR FORCE

Finally, understanding avenues of approach, also known as attack vectors, is central to understanding the vulnerabilities of your formation. Leaders who analyze avenues of approach against their cyber systems, including those that could impact the hardware, logical networks, personas and people, are better prepared to allocate cyber mission forces and set defensive postures as they conduct operations. Using OCOKA to analyze geography, hardware, logical networks, personas and people improves awareness while helping leaders develop a better understanding to act faster and lead change, providing them and their formations an advantage.

Empowering formations to act as part of the cyber mission force is essential to victory. As the number of threats continues to grow, leaders should encourage teams to get "into the cyber fight" to maximize the effectiveness of our cyber mission forces. The Capstone Concept for Joint Operations states: "Being able to operate on intent through trust, empowerment and understanding" is part of the joint strategy to ensure our leaders can operate in complex environments to prevent conflict, shape security environments and win wars while operating as part of a joint force.

Mastering cyberspace in operations requires an understanding of the environment, a framework to recognize and lead change, and the ability to empower every person as part of the cyber mission team. Leaders will continue to adjust their military decision-making and battlefield calculus as they play out conflicts in their minds through phasing, branches, sequels, and sequencing to determine key terrain, key tasks and key decision points. As cyberspace continues to grow, leaders must adopt a common frame of reference that empowers their teams to recognize change and lead transitions to win in the 21st century. □