CURTIS E. LEMAY CENTER
FOR DOCTRINE DEVELOPMENT AND EDUCATION

ANNEX 3-12 CYBERSPACE OPERATIONS

INTRODUCTION TO CYBERSPACE OPERATIONS

Last Updated: 30 November 2011

Cyberspace superiority may be localized in time and space, or it may be broad and enduring. The concept of cyberspace superiority hinges on the idea of preventing prohibitive interference to joint forces from opposing forces, which would prevent joint forces from creating their desired effects. "Supremacy" prevents effective interference, which does not mean that no interference exists, but that any attempted interference can be countered or should be so negligible as to have little or no effect on operations. While "supremacy" is most desirable, it may not be operationally feasible. Cyberspace superiority, even local or mission-specific cyberspace superiority, may provide sufficient freedom of action to create desired effects. Therefore, commanders should determine the minimum level of control required to accomplish their mission and assign the appropriate level of effort.

Cyberspace. Cyberspace is "a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[1]

Cyberspace operations. **"**The employment of cyberspace capabilities where the primary purpose is to achieve military objectives or effects in or through cyberspace."[2]

Cyberspace superiority. The operational advantage in, through, and from cyberspace to conduct operations at a given time and in a given domain without prohibitive interference.[3]

[1] Joint Publication (JP) 3-12(R [redacted]), *Cyberspace Operations*
[2] JP 3-0, *Joint Operations*
[3] Approved Air Force Space Command (AFSPC) definition of cyberspace superiority, derived from multiple AFSPC and LeMay Center cyberspace operations working groups, 2009-2010.

UNDERSTANDING CYBERSPACE

Cyberspace is a domain. Cyberspace operations are not synonymous with information operations (IO). IO is a set of operations that can be performed in cyberspace and other domains. Operations in cyberspace can directly support IO and non-cyber based IO can affect cyberspace operations.

Cyberspace is a man-made domain, and is therefore unlike the natural domains of air, land, maritime, and space. It requires continued attention from humans to persist and encompass the features of specificity, global scope, and emphasis on the electromagnetic spectrum. Cyberspace nodes physically reside in all domains. Activities in cyberspace can enable freedom of action for activities in the other domains, and activities in the other domains can create effects in and through cyberspace.

Even though networks in cyberspace are interdependent, parts of these networks are isolated. Isolation in cyberspace exists via protocols, firewalls, encryption, and physical separation from other networks. For instance, classified networks such as the US Armed Forces Secure Internet Protocol Router network (SIPRnet) are not hardwired to the Internet at all times, but connect to it via secure portals. Additionally, the construction of some hard-wired networks isolates them from most forms of radio frequency (RF) interference. These factors enable these networks to be isolated within cyberspace, yet still allow controlled connectivity to global networks.

Cyberspace segments are connected and supported by physical infrastructure, electronic systems, and portions of the electromagnetic spectrum (EMS).[4] As new systems and infrastructures are developed, they may use increasing portions of the EMS, have higher data processing capacity and speed, and leverage greater bandwidth. Systems may also be designed to change frequencies (the places where they operate within the EMS) as they manipulate data. Thus, physical maneuver space exists in cyberspace.[5]

Logical maneuverability in cyberspace is often a function of the security protocols used by host systems. Systems seeking connectivity with a secure host will have more difficulty gaining access than systems seeking connectivity with unsecured hosts. Additionally, defense against entry by undesired systems resides in the code or logic of the host system. Once a connection between systems is established, a potential intruder must exploit a fault in logic to enter the system. Code writing can thus be a form of logical maneuver in cyberspace. The potential intruder writes malicious code to

---

[4] Definition of EMS: "The range of frequencies of electromagnetic radiation from zero to infinity. It is divided into 26 alphabetically designated bands." (JP 3-13.1)

[5] For additional information on the "Physical, Syntactic, and Semantic layers of Cyberspace" see Chapter 10 of "*Conquest in Cyberspace,"* Libicki, Martin C., RAND Corporation, Cambridge University Press, 2007.

gain maneuverability against targeted systems. As a defender becomes aware of unwanted presence within the system, the defender will alter the system's code to deny entry. The intruder, wishing to remain "on target," adapts the malicious code accordingly. This process is the equivalent of forces maneuvering to gain positions of advantage in the traditional air, land, space, and maritime domains. Both logical and physical maneuver space is required — one is often useless without the other.