

Cyberspace Training Initiative

Sustaining Operations in a denied or degraded Cyber Environment

Supporting Glossary

* This glossary of terms is provided to support and scope the discussion concerning the subject of educating and training joint forces to sustain operations in a denied or degraded cyber environment.

Cyberspace: 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.

Source: CJCS CM-0363-08

Cyberspace Operations: The employment of cyber capabilities where the primary purpose is to achieve objectives in or through cyberspace. Such operations include computer network operations and activities to operate and defend the Global Information Grid.

Source: JP 3-0

Denied Cyberspace Environment: An operating environment in which access to, or normal functions of, a mission-essential network or system are prevented by adversary activity, unintended event, or commander-directed restriction in response to such conditions.

Source: CJCS EXORD, 112040ZFeb11

Degraded Cyberspace Environment: An operating environment in which the availability or reliability of mission essential networks or systems is not assured, whether as a result of adversary action, defensive mitigation measures (such as implementation of “minimize,” use of alternative bandwidth-constrained systems, or additional security measures), inadvertent friendly action, or natural event. May include temporary, intermittent, or localized non-availability (denial) of network or system access due to adversary activity, natural event, or friendly defensive actions such as system isolation in the event of known or suspected compromises.

Source: CJCS EXORD, 112040ZFeb11

Compromise: An operating environment in which the confidentiality, integrity, or non-repudiation of mission essential networks, systems, or data is assessed as questionable, due to insider threat, inadvertent action, or adversary exploitation. In a compromised cyber environment, networks and systems may appear to be operating normally even while being altered or exploited by a criminal or hostile entity. A *compromised cyberspace environment* is inherently harder to detect than a degraded cyberspace environment, and consequences may be more far-reaching. For instance, if C2 or logistical data is intercepted, corrupted, or altered, critical supplies and components, such as aerial refuelers, ammunition, or medical support, may be misrouted or intercepted, or blue force/IFF tracking may be altered so as to create friendly fire incidents or mask adversary activities.

Source: CJCS EXORD, 112040ZFeb11