Exploitation

Proficiency Code: A

Cyberspace exploitation actions include military intelligence activities, maneuver, information collection, and other enabling actions required to prepare for future military operations. Cyberspace exploitation actions are taken as part of an Offensive Cyber Operations (OCO) or Defensive Cyber Operations-Response Actions (DCO-RA) mission and include all actions in gray or red cyberspace that do not create cyberspace attack effects. Cyberspace exploitation includes activities to gain intelligence and support operational preparation of the environment for current and future operations through actions such as gaining and maintaining access to networks, systems, and nodes of military value; maneuvering to positions of advantage; and positioning cyberspace capabilities to facilitate follow-on actions. Cyberspace exploitation also supports current and future operations through collection of information, including mapping red and gray cyberspace to support situational awareness; discovering vulnerabilities; enabling target development; and supporting the planning, execution, and assessment of military operations. Cyberspace exploitation actions are deconflicted with other United States Government (USG) departments and agencies In Accordance With (IAW) national policy.

Source Material: Joint Publication 3-13 (8 June 2018) Cyberspace Operations.

http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf?ver=2018-07-16-134954-150