Overview of IRCs (INFO1 SMARThook)

The INFO1 SMARTbook discusses the following IRCs in greater detail:

Public Affairs See pp. 3-5 to 3-16.

Army public affairs is communication activities with external and internal audiences (JP 3-61). Public affairs operations help to establish conditions that lead to confidence in the Army and its readiness to conduct unified land operations.

Civil Affairs & Civil-Military Operations See pp. 3-17 to 3-26.

Civil affairs operations encompass actions planned, executed, and assessed by civil affairs forces. Civil-military operations are activities of a commander performed by designated civil affairs or other military forces that establish, maintain, influence, or exploit relations between military forces, indigenous populations, and institutions.

Military Deception (MILDEC) See pp. 3-27 to 3-32.

Military deception (MILDEC) involves actions executed to deliberately mislead adversary military, paramilitary, or violent extremist organization decision makers. The intent of MILDEC is to feed information that deliberately misleads the enemy decision makers as to friendly military capabilities, intentions, and operations and lead the enemy to take actions (or inactions) that contribute to accomplishment of the friendly mission.

Military Information Support Operations (MISO) See p. 3-33.

Military information support operations are planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals in a manner favorable to the originator's objectives (JP 3-13.2).

Operations Security (OPSEC) See pp. 3-39 to 3-44.

Operations security is a capability that identifies and controls critical information, indicators of friendly force actions attendant to military operations, and incorporates countermeasures to reduce the risk of an adversary exploiting vulnerabilities (JP 3-13.3).

Cyberspace Electromagnetic Activities (CEMA) See p. 3-45.

Cyberspace electromagnetic activities is the process of planning, integrating, and synchronizing cyberspace and electronic warfare operations in support of unified land operations (ADRP 3-0).

Cyberspace Operations (CO) See pp. 3-47 to 3-54.

Cyberspace operations are the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace (JP 3-0).

Electronic Warfare (EW) See pp. 3-55 to 3-60.

Electronic warfare is military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy (JP 3-13.1).

Space Operations See pp. 3-61 to 3-70.

Space operations are operations that occur in the space domain and seek to gain superiority over enemies and adversaries in the space domain and its corresponding environment.

Additional IRCs See pp. 3-71 to 3-74.

Additional IRCs discussed include integrated joint special technical operations (IJSTO); special access programs (SAP); personnel recovery (PR); physical attack; physical security; presence, profile, and posture (PPP); soldier and leader engagement (SLE); police engagement; and social media.