Information as a Joint Function

On 12 July 2017, the CJCS approved Information as the seventh joint function. The definition is below.

"The information function encompasses the management and application of information and its deliberate integration with other joint functions to influence relevant-actor perceptions, behavior, action or inaction, and support human and automated decision making. The information function helps commanders and staffs understand and leverage the pervasive nature of information, its military uses, and its application during all military operations. This function provides JFCs the ability to integrate the generation and preservation of friendly information while leveraging the inherent informational aspects of all military activities to achieve the commander's objectives and attain the end state."

This change has been incorporated into JP 1, Change 1 dated 12 July 2017.

Next Steps for Doctrine to Incorporate Information as a Joint Function

The inclusion of the seventh joint function in JP 1 will necessitate the updating of some key joint publications out of cycle. The JS J39 along with the JS J7 is planning on holding a working group at NDU in early September to begin this process. The first order of business will be looking at JP 3-0 to include a definition of the new joint function (the description is in JP 1) along with looking at the rest of the joint functions to make sure that the new joint function fits/complements them correctly. Once the initial rough draft for JP 3-0 is complete, the working group will look at laying out the framework for the complete rewrite/renaming of JP 3-13. The new JP (the number could also change) will be dedicated to addressing the new joint function. Whether or not a separate publication for IO is needed will also be addressed during the rewrite. This effort will be led by the JS J39 (with JIOWC) and the JS J7. While the new JP is being written, the community will also do an out of cycle look at JP 5-0 and JP 2-0 to bring them into alignment with the new joint function. The remainder of the JPs will probably be reviewed as per the JS J7's normal schedule.

Joint Concept for Operating in the Information Environment (JCOIE)

The Joint Information Operations Warfare Center has been working with stakeholders from the Services and Academia to develop a concept for Joint Force operations in a more pervasive and connected information environment. This Joint Concept for Operating in the Information Environment (JCOIE) aims to institutionalize and operationalize the Joint approach to information. This requires an understanding of information, the informational aspects of military activities, and informational power.

To achieve enduring strategic success in this increasingly pervasive and connected information environment, the Joint Force must build information into operational art to design operations that leverage the inherent informational aspects of military activities. Informational aspects of military activities are characteristics or elements an observer uses to build a story that provides meaning. The Joint Force must understand how to leverage informational aspects to change or maintain perceptions, and attitudes that drive desired behaviors. The team has been working the JCOIE since June 2015, and it is expected to be signed in late October 2017.

Dominating Duffer's Domain

The RAND Corporation published a small book on information operations called Dominating Duffer's Domain, Lessons for the U.S. Marine Corps Information Operations Practitioner by Christopher Paul and William Marcellino. It is written from the aspect of the military classic The Defence of Duffer's Drift by Major General Sir Ernest Swinton.
fictitious narrator, Captain I. N. Hindsight, takes readers repeatedly through the same mission over the course of six dreams in which he makes shortsighted decisions, critical miscalculations, and smaller mistakes that contribute to spectacular failures until his accumulated lessons ultimately allow him and the command he supports to succeed. The fabricated instructional scenario draws on actual historical operations, alternative directions that these operations could have taken, and realistic challenges that a Marine Corps information operations planner might face. The 26 concise lessons in this volume offer insight that, ideally, the practitioner will not need to acquire through practice.

The authors also adapted, from an Army Captain’s point of view, the *Dominating Duffer's Domain, Lessons for the U.S. Army Information Operations Practitioner*.

---

**Weaponization of Information**

*The Weaponization of Information: The Need for Cognitive Security.* This testimony before the Senate Armed Services Committee, Subcommittee on Cybersecurity, by Rand Waltzman, RAND Corporation, was presented on April 27, 2017. From the conclusion: “We have entered the age of mass customization of messaging, narrative, and persuasion. We need a strategy to counter Russian, as well as others, information operations and prepare the United States organizationally for long-term IO competition with a constantly changing set of adversaries large and small. It is said that where there is a will, there is a way. At this point, ways are available. The question is, do we have the will to use them?”

Similarly, RAND’s Christopher Paul and Miriam Mathews discuss potent aspects of the Russian propaganda model, and likely effective solutions in dealing with it, in “The Russian ‘Firehose of Falsehood’ Propaganda Model: Why It Might Work and Options to Counter It”

---

**Crafting an Information Warfare and Counter-Propaganda Strategy**

*Armed Services Committee Hearings: Crafting an Information Warfare and Counter-Propaganda Strategy for the Emerging Security Environment.* This link provides access to both video of testimony on 15 March 2017 and PDF documents by Matthew Armstrong (King’s College, London), the Honorable Michael Lumpkin (former Assistant Secretary of Defense for Special Operations/Low-Intensity Conflict), and Mr. Timothy Thomas (Senior Analyst, Foreign Military Studies Office, Ft. Leavenworth, KS). Of prime interest is Mr. Thomas’ testimony: *Russia’s Views on Modern Warfare and Use of Information Operations: The Integrations of Roles.* From the paper’s conclusion: “Russia is motivated by dangers and threats to its information space, whether they be political, economic, military, diplomatic, or others. Software writers and their teams, along with a thriving hacker and troll community, continue to cause problems for the West”.

Further, Mr. Thomas’ 2015 paper, *Russia’s Military Strategy and Ukraine: Indirect, Asymmetric—and Putin-Led* should likely be required reading for all IO officers. From the abstract: “This article details the development of Russia’s military strategy and how elements of that strategy may have been applied in Ukraine. It examines both traditional and contemporary elements of strategy, with a particular focus on the effect of Russian President Vladimir Putin’s competitive logic and the General Staff’s reliance on non-military methods of thought. With regard to the latter, General of the Army Valeriy Gerasimov, Chief of the Russian General Staff, noted that today, non-military measures in operations are used over military operations by a ratio of 4:1.” In these papers and testimony is not only information by which to understand a primary competitor, but also insights into successfully waging and countering information operations against capable adversaries or competitors.

---

**Social Media**

One area that has gained quite a bit of interest is that of Social Media. A study by RAND on *Monitoring Social Media, Lessons for Future Department of Defense Social Media Analysis in Support of Information Operations* by William Marcellino, Meagan L. Smith, Christopher Paul, Lauren Skrabala. This report reviews the analytic approaches that will be most valuable for information operations, as well as legal, ethical, policy, technological, and training considerations. It also includes a set of recommendations to help DOD navigate this terrain while building a robust, effective social media analysis capability to support operations worldwide.
Information Operations in the News

*How Russia Targets the U.S. Military*: With hacks, pro-Putin trolls and fake news, the Kremlin is ratcheting up its efforts to turn American service members and veterans into a fifth column. While a bit provocative, this piece is a good reminder to keep our folks alert and practice good OPSEC in one’s personal and professional life.

*Students Are the Newest U.S. Weapon Against Terrorist Recruitment*: While this is a U.S. example, it is worth considering, wherever we are in the world, those audiences that may be in a position to advance U.S. and allied interests. As we find ourselves in ceaseless operations and competition in the IE, consider making creative use of (to the extent possible) all accessible assets.

*DIA Reveals New Details of Russian Information Warfare*: Report highlights Moscow’s ‘information confrontation’ plans for future conflict. This open media article provides commentary on Russian information operations, including the “cyber-enabled psychological warfare operations.” The author reports the DIA notes “Russia views the information sphere as a key domain for modern military conflict.” Information warfare is highlighted as “a key means of achieving its ambitions of becoming a dominant player on the world stage.” The report makes reference to their *Russia Military Power: Building a Military to Support Great Power Aspirations* report. In particular, see “Core Russian Military Capabilities” on pp. 29-45 for address of core Russian capabilities, including those we’d consider to be IO and Information Related Capabilities (IRC).

---

Information Operations Continuing Training

“IOII for the IO Planner” was distributed 7 Aug 17. https://intelshare.intelink.gov/sites/jiowc/sub/FS/FD/default.aspx

New Joint IO Proponent (JIOP) Website

The Joint IO Proponent is now on INTELINK.

---

DoD Information Operations Center for Research

The IOCR is hosted by the Naval Post-graduate School (NPS). The mission of the DoD Information Operations Center for Research is to provide graduate-level IO education, facilitate the exploration of new IO concepts, conduct research and analysis, and support relevant field experimentation. https://my.nps.edu/web/dod_iocr

---

Newsletter submissions:
Please submit ideas/inputs to Mr. Brent Fountain at brent.j.fountain.ctr@mail.mil and Mr. Michael Adams at michael.f.adams3.ctr@mail.mil, for possible inclusion in an upcoming newsletter.

NOTE: If a link does not work, please try a different internet browser before contacting the aforementioned.