Introducing Information as a Joint Function *(Joint Force Quarterly 89, Brig Gen Alexus G. Grynkewich, 2nd Quarter, April 2018)*

“...information may prove to be the preeminent commodity and decisive factor in military operations. As such, the Chairman’s JP 1 issuance is a call to action for the joint force to move rapidly to build information into operational art and design in order to deliberately leverage the informational aspects of military activities. We have not always done this right...we cannot afford to repeat past mistakes.”

The Practical Implications of Information as a Joint Function *(Joint Force Quarterly 89, Gregory C. Radabaugh, 2nd Quarter, April 2018)*

“The importance of understanding the informational aspect of the operating environment was underscored by the Chairman of the Joint Chiefs of Staff’s addition of Information as a Joint Function (IJF)...This change comes amid an erosion of the U.S. military’s competitive advantage in a security environment marked by challenges from Russia, China, Iran, North Korea, and violent extremist organizations (VEOs)...” “With IJF, commanders must now understand the centrality of dynamic integration of information with other joint functions...to positively alter relevant actor perceptions and behaviors...”

Paradigm Change: Operational Art and the Information Joint Function *(Joint Force Quarterly 89, COL Scott K. Thomson and Christopher E. Paul, 2nd Quarter, April 2018)*

“Skillful leveraging of information power has enabled competitors and adversaries such as Russia, China, and VEOs to realize important gains... The NSS is particularly direct in admonishing that “U.S. efforts to counter the exploitation of information by rivals have been tepid and fragmented. U.S. efforts have lacked a sustained focus and have been hampered by the lack of properly trained professionals...””

Quick Reaction Test (QRT) for Information Joint Function (IJF) in the Joint Planning Process (JPP)

During the February 2018 IO Executive Steering Group, JS J7 identified three Joint Tier 1 exercises during FY 19 as opportunities to examine solutions for the Joint Concept for Operating in the Information Environment and employ the Information Joint Function. JIOWC EO and JS J7 JED are developing a Quick Reaction Test (QRT) nomination package for submission to the Joint Test and Evaluation Program Office. A QRT provides quantitative operational test and evaluation information used for analyzing joint military capabilities and develops potential options for increasing military effectiveness. Upon approval in October the test will include one of the identified Tier 1 exercises with this problem statement, “The Joint Force ability to integrate physical and informational power to affect relevant actor behavior is hampered by a lack of guidance, processes and products inside the Joint Planning Process that would otherwise facilitate understanding, managing, and leveraging information during the design, planning and execution of operations.” The results of the QRT will inform ongoing doctrine development and future training.

Update on the Joint Concept for Operating in the Information Environment (JCOIE)

The JCOIE has been approved by all Service Chiefs. Next and final step is review and signature by VCJCS. IPower News will continue to keep you updated on JCOIE approval and implementation.

Recurring Training Topic: “Threat/Observations in the Information Environment” will be published in July 2018

The training will cover dynamics, events, and developments of interest in the Information Environment, ways in which the DoD and U.S. are targeted in the IE, highlights of adversary and competitor activity in the IE, and ways in which the Joint force and DoD can be more resilient.
Foreign Disinformation is a Threat to Military Readiness, Too (Defense One, 16 Feb 18)
“Troops—and their families—need training to spot and discard false narratives and information. Just as foreign actors seek to shape opinions and actions by the general American public...they are also working to influence the U.S. military community. Recent research by Oxford University has revealed how foreign actors are targeting service members, civilians, and their families. Immediate efforts are needed to mitigate this threat...”

Russians Posed as ISIS Hackers, Threatened US Military Wives (Military.com, 8 May 18)
“Army wife Angela Ricketts was...in her Colorado home...when a message appeared on her iPhone..."Dear Angela! Bloody Valentine’s Day!" "We know everything about you, your husband and your children," the message continued, claiming that the hackers operating under the flag of Islamic State militants had penetrated her computer and her phone... Ricketts was one of five military wives who received death threats from the...CyberCaliphate...Except it wasn’t ISIS...the women were targeted not by jihadists but by the same Russian hacking group that intervened in the American election” The Russian effort appears to be more directed at intimidating US military personnel and their families than demanding any particular policy change.

Logical Fallacies Fuel Kremlin Disinfo (Digital Forensic Research Lab, 22 Apr 18)
“The Kremlin and the pro-Kremlin media have a comprehensive toolkit when it comes to the creation and dissemination of disinformation, including logical fallacies to construct seemingly compelling arguments... They exploit our mental shortcuts...require critical analysis to spot...have exploited a wide variety of logical fallacies..., and deepen divisions in the Western societies...[here] are the eight most common logical fallacies and examples of how the Kremlin and its disinformation networks have used them to dismiss, distort, distract and dismay.”

Russia Steps Up Hacking, Spurring U.S.-U.K. Warning on Risk (Bloomberg, 16 April 18)
“Russia is using compromised computer network equipment to attack U.S. and British companies and government agencies, the two countries warned in an unprecedented joint alert.” “Russian state-sponsored actors are using compromised routers to conduct spoofing ‘man-in-the-middle’ attacks to support espionage, extract intellectual property, maintain persistent access to victim networks and potentially lay a foundation for future offensive operations...”

Artificial Intelligence and National Security (Belfer Center Study, July 2017)
This Belfer Center report documents a number of interesting national security implications: “[Artificial Intelligence] AI-forgery capabilities are real enough that they can sometimes fool the untrained eye and ear. In the near future, they will be good enough to fool at least some...forensic analysis...The existence of widespread AI forgery capabilities will erode social trust, as previously reliable evidence becomes highly uncertain...Today, when people see a video of a politician taking a bribe, a soldier perpetrating a war crime, or a celebrity starring in a sex tape, viewers can safely assume that the depicted events have actually occurred... But that world of truth—where seeing is believing—is about to be upended by artificial intelligence technologies...The growth in this technology will transform the meaning of evidence and truth in domains across journalism, government communications, testimony in criminal justice, and, of course, national security.” For a powerful/relevant demonstration of emerging technology applications to the IE, see “Face2Face: Real-time Face Capture and Reenactment of RGB Videos” (University of Erlangen-Nuremberg, the Max Planck Institute, and Stanford University): https://www.youtube.com/watch?v=ohmajTcPNk

Sweden Releases To-Do List for War (Defense News, 23 May 18)
“Be on the lookout for false Information. States and organizations are already using misleading information in order to try and influence our values and how we act. The aim may be to reduce our resilience and willingness to defend ourselves. The best protection against false information and hostile propaganda is to critically appraise the source:
• Is this factual information or opinion?
• What is the aim of this information?
• Who has put this out?”
• Is the source trustworthy?
• Is this information available somewhere else?
• Is this information new or old and why is it out there at this precise moment?
• Search for information – the best way to counteract propaganda and false information is to have done your homework.
• Do not believe in rumors – use more than one reliable source in order to see whether the information is correct.
• Do not spread rumors – if the information does not appear trustworthy, do not pass it on.”

USAF News: NEW USAF 14F Badge! (Twitter @GenDaveGoldfein, May 18)

Information operations officers get their own school (AF Times, 13 Mar 18)
“Air Force officers in the newly formed 14F information operations career field will get their own technical training school in late fiscal 2019...the Air Force said the new school will be set up at Hurlburt Field in Florida...a 14- to 15-week-long Initial Skills Course and will consolidate and integrate content from several related training courses.”

Navy Information Warfare Effort Set to Expand, Evolve (USNI News, 7 Feb 18)
“...the Navy’s force of information warfare professionals continues to expand and evolve into a greater role supporting tactical warfighters, Vice Adm. Matthew Kohler said on Tuesday. “Kohler...highlighted three initiatives in the information warfare community to create Warfare Tactics Instructors, establish a training group to oversee unit-level IW training, and formalize a position of “IW commander afloat.”

Marine Corps strengthens psychological operations with new job field (Marine Times, 15 May 18)
“The Corps plans to create another track field for its information warriors. It continues to build its intelligence and information warfare capabilities in preparation for a looming conflict with more sophisticated adversaries. Now, Marines who specialize in psychological operations, or what the Corps now calls Military Information Support Operations, or MISO, will soon be getting a new primary job field known as 0521...”

Marines get new information warfare leader (C4ISRNet, 18 May 18)
“Maj. Gen. Lori Reynolds has been nominated for a third star and to serve as the recently established deputy commandant for information, according to a May 18 announcement... Reynolds...will succeed Lt. Gen. Daniel O’Donohue, who is moving to the joint
staff...The Marines established...the deputy commandant for information, in summer 2017 to better compete in a 21st century world, aligning all information-related capability under a single entity.”

This March 2018 publication documents lessons learned and changes being made in U.S. Army Information Operations. “Following the 2014 Russian actions in Ukraine, the U.S. Army expanded its presence in Europe in...actions designed to reassure NATO allies and deter potential aggression. U.S. Army support to Atlantic Resolve illuminated a number of challenges that weaken the ability...to fight and win in the information environment. With the recognition of how America’s competitors use information found in the December 2017 National Security Strategy, the Army should consider whether lessons learned from Atlantic Resolve might inform larger discussions on the future of how the Army fights and wins in the information environment.”

IPower News:
IPower News is located at https://intelshare.intelink.gov/sites/jiowc/sub/FS/FD/PublicDocuments/IPOWER%20News and https://my.nps.edu/web/dod_iocr. Submissions can be made at any time to Mr. Brent Fountain at brent.j.fountain.ctr@mail.mil and/or Mr. Jonathan Drummond at jonathan.t.drummond.ctr@mail.mil. Submission does not guarantee inclusion or a specific schedule. NOTE: If a link does not work, please try a different internet browser before contacting the aforementioned. If there are any other problems receiving files, please contact Mr. Fountain.