**Director of the JIOWC Retires**

Mr. Gregory C. Radabaugh, a member of the Senior Executive Service; Director, Joint Information Operations Warfare Center, a Chairman Joint Chiefs of Staff Controlled Activity at Joint Base San Antonio, Texas retires on 19 October after serving as the Director for over six years. His retirement culminates a career of over 44 years of dedicated service to the country.

Mr. Radabaugh entered the Air Force as an enlisted linguist in 1974, flying reconnaissance missions overseas. He was commissioned in 1979 and served in a variety of service and national level positions. He left active duty and joined the civil service in 1989. He remained part of the Air Force Reserve until his retirement in 2004. He was designated an Intelligence Community Officer in 2003. An expert in information operations and cyberspace operations, he has lectured at the John F. Kennedy School of Government, Harvard University, and at numerous conferences at home and abroad.

The Joint Staff J3 and J39 leadership are actively seeking a replacement for Mr. Radabaugh.

**Information Joint Function Training**

The JIOWC Enterprise Operations Division recently released the first package of a three-iteration spiral training for the Information Joint Function. This initial package is a pre-doctrinal basic familiarization for the joint function. It is intended to broach the topic with the Joint Force and provide some initial information as the doctrine is just beginning its development. The second package is projected to be released in the February 2019 timeframe as the doctrine begins to take shape. The final package is due out sometime in the summer of 2019 as the doctrine is being finalized and published. The familiarization training can be found at: Information Joint Function Familiarization - 25 Sep 2018. (CAC Required). If you cannot access the training and have not received it already, contact one of the POCs at the bottom for a copy.

**“Russia is Winning the Information War in Iraq and Syria: UK General”** (Defense One, Katie Bo Williams, 8 Oct)

“Moscow is “better than us” in using social media to shape the strategic landscape, says a former deputy commander of the West’s anti-ISIS coalition.

A senior general in the international fight against ISIS has a pointed warning for Western governments with troops in Iraq and Syria: You’re being played by the Russians.”

**"The surprising test ground for DoD information operations"** (Fifth Domain, Mark Pomerleau, 5 Sep)

"The Department of Defense’s cyber community has found an unexpected proving ground to cut its teeth on operations: the Middle East.

Lt. Gen. Stephen Fogarty, speaking to Fifth Domain Aug. 21 in an interview at TechNet Augusta, said cyber operators in the Middle East have worked “at a higher tempo than other commands” and in the process have developed “proficiencies.”"
"Where do information operations fit in the DoD cyber enterprise?" (Fifth Domain, Mark Pomerleau, 26 Jul)

"Events such as interference in the 2016 election are demonstrating how the internet has amplified the reach and impact of age-old military tactics such as information or influence operations.

These new cyber-enabled information operations have many in the U.S. government and thought leadership community concerned both about the United States' ability to counter and coordinate similar activities, especially given the Department of Defense divested a lot of its information-related capability at the conclusion of the Cold War."

"New cyber authority could make ‘all the difference in the world’" (Fifth Domain, Mark Pomerleau, 17 Sep)

"Cyber leaders from the Department of Defense are optimistic about a new White House policy aimed at accelerating cyber operations and said the changes could make "all the difference in the world.""

"Is Social Media Empowering Or Silencing Our Voices?" (Forbes, Kalev Leetaru, 8 Oct)

The early days of social media saw the platforms embrace a popular image as absolute defenders of free speech, empowering the disenfranchised by handing them a global megaphone with which to speak directly to the world. The Arab Spring cemented the idea that social media could even topple dictatorships by freeing citizens all over the globe to come together. As terrorists began to use their platforms to recruit and promote violence, Twitter famously rebuked Congress’ request to reign in violent use of its platform by proclaiming that in the name of free speech it would never censor a terrorist. The past several years have seen this image come crashing down as it collided with the geopolitical reality of the world in which the social platforms exist. Most importantly, governments throughout the world, both democratic and autocratic, have awoken to the immense power of single centralized information and communications platforms to surveil their citizens at unprecedented resolution and to control and censor their speech. Is this new second era of social media empowering or silencing the world’s citizens?

"Welcome to the Disinformation Game—You’re Late" (The Strategy Bridge, Michael P. Ferguson, 29 Aug)

Reports of Russian disinformation in the news have triggered a combination of hyperbole and hysteria from the western world, as if such measures reflect a deviation from the tradition of Russian statecraft. In March 2017, the European People’s Party gathered in Malta to discuss why they believe Russian disinformation is the greatest threat to freedom and democracy. Earlier this year, a report from Washington-based think tank the Atlantic Council recommended an increase in federal funding that supports investigative journalism to counter false narratives of foreign origin in the media.

"The Weaponization of Everything" (Defense One, Nathan Freier and Jonathan Dagle, 9 Sep)

There is a transformation afoot in great-power conflict. In a twist to the well-worn caution, “if all you have is a hammer, everything looks like a nail,” China and Russia are redefining both. These competitors have discovered that nearly everything that can generate strategic leverage is a potential hammer, while everything of major interest to the United States and her allies can make effective nails. And so, as these rivals smell blood (or weakness) in the competitive water, they are on the offensive nearly everywhere, seeking to diminish American influence and strategic position through persistent and effective gray-zone maneuver.

"Russia’s Use of Media and Information Operations in Turkey" (RAND, Katherine Costello, 2018)

Russian media have sought to undermine Turkey’s political and security cooperation with the United States and Europe by exacerbating mutual skepticism and highlighting policy differences. In Turkey, Russian media have also contributed to anti-American discourse and have reinforced and informed the Turkish government’s own propaganda pursuits. This analysis assesses how Russia has used media and information operations to pursue its foreign policy goals related to
Turkey. It examines Russian media responses to three significant events in Turkey: (1) Turkey's November 2015 shootdown of a Russian military aircraft, (2) the July 2016 Turkish coup attempt, and (3) the December 2016 assassination of the Russian ambassador.

"The future operating environment is here. It's in Syria" (Army Times, Todd South, 8 Oct)
"There’s a lot of talk in military circles about future threats, operating environments and shifting the focus to a more complex fight. But military and civilian leaders, fresh from Operation Inherent Resolve, have brought back a message from the battlefield – the future is now."

"U.S. Army soldiers participated in third annual ‘Cyber Blitz’ exercise" (Defence Blog, 4 Oct)
"According to 780th Military Intelligence Brigade (Cyber), U.S. Army has taken the opportunity at the ‘Cyber Blitz’ exercise to exercise new concepts, capabilities and techniques for everything from offensive cyberspace operations (OCO) and defensive cyberspace operations (DCO), to electronic warfare (EW) and information operations (IO).

Cyber Blitz is an annual exercise co-hosted by U.S. Army Communications-Electronics Research, Development and Engineering Center (CERDEC) and the CCoE that informs the Army on how to employ cyberspace electromagnetic activities, or CEMA, across all aspects of Army doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy, or DOTMLPF-P."

**VULCAN-SOF**
JIOWC recently introduced VULCAN – SOF as a platform to capture technology that could enable operations in the information environment (OIE). Vulcan is an open technology scouting platform used by the Defense community to accelerate its ability to deliver innovative solutions to the Warfighter. The JIOWC is merging its Capabilities and Tools database into Vulcan to allow greater visibility to our community and provide broader technology solutions able to meet OIE requirements. Vulcan’s effectiveness is based on an interconnected community of Government scouts and technology developers striving to solve warfighter challenges. VULCAN – SOF’s user base is 250+ Government Organizations and 10,000+ from the Commercial sector. For more information please visit [https://www.vulcan-sof.com/login/auth](https://www.vulcan-sof.com/login/auth) or contact JIOWC’s POC MAJ Alfred D. Mesa at alfred.d.mesa.mil@mail.mil.

**IEAA – FY19 Schedule and Course Information**
IEAA has distributed their course schedule for FY19. You will find more information on this course (and others) at the JIOWC Force Development Training Intelink webpage.

**IPower News:**
IPower News is located at [https://intelsheart.intelink.gov/sites/jiowc/sub/FS/FD/PublicDocuments/IPOWER%20News](https://intelsheart.intelink.gov/sites/jiowc/sub/FS/FD/PublicDocuments/IPOWER%20News) and [https://my.nps.edu/web/dod_iocr](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.