IPOWER NEWS

From the JIOWC Director: The JIOWC presents this newsletter to the information, IO, and extended communities to share current information and relevant actions. Articles are included for situational awareness, but inclusion does not indicate endorsement/agreement.

National Security Strategy – Signed 12-18-17

The National Security Strategy emphasizes the importance of weaponized information and its use in statecraft (pages 34-35), "America's competitors weaponized information to attack the values and institutions that underpin free societies, while shielding themselves from outside information. They exploit marketing techniques to target individuals based upon their activities, interests, opinions, and values. They disseminate misinformation and propaganda. Risks to U.S. national security will grow as competitors integrate information derived from personal and commercial sources with intelligence collection and data analytic capabilities based on Artificial Intelligence (AI) and machine learning." The NSS specifies five priority actions: 1) Prioritize the competition, 2) Drive effective communications, 3) Activate local networks, 4) Share responsibility, and 5) Upgrade, tailor, and innovate our delivery platforms.

National Defense Authorization Act (NDAA) for Fiscal Year 2018 – Signed into law 12-12-17

Section 1637: Requires four actions: 1) establish a designated senior official to "implement and oversee the processes and procedures" identified in this section, 2) CCMD regional IO planning, 3) Implementation Plan for the Department of Defense's "Strategy for Operations in the Information Environment", and 4) recommend training and education programs.

IO Executive Steering Group (ESG) – 16 Feb 18, OUSD(P) Memorandum for Record dtd 28 Feb 18

Discussion amongst the attending members centered on the NDAA taskings and where and to what level the authority should be focused. The ESG co-chairs agreed to recommend USD(P) to the SecDef as the initial Designated Senior Official (DSO) for Information. The ESG concurred that further analysis and discussion are required to fully define tasks, workload, and resource requirements associated with the designation.

Also discussed in reference to the NDAA was the requirement for Combatant Commands' (CCMD) current and planned regional information strategies and ensuring they are aligned with the current National Defense Strategy. The Joint Staff Deputy Director for Global Operations was tasked to lead the efforts with the CCMDs.

Other discussions focused on the Joint Concept for Operating in the Information Environment, the OIE Capability Based Assessment (CBA), and the potential of using upcoming CCMD exercises to begin exercising Information as a Joint Function. An update on all of these areas will be provided at the next ESG scheduled for May 2018.

Recurring Training Topic "IO in Joint Planning Process (JPP)" will be published in March 2018.

IPOWER NEWS

Information Joint Function Workshop at NDU College of Information and Cyberspace, Dec 17

The workshop started the process for building the educational foundations necessary to address the challenges of information as a Joint function. Workshop findings are expected to be released April 2018.

"The Good Operation" (MOD UK, Jan 18)

This handbook draws on the key lessons from the Iraq Inquiry (Chilcot) Report and other recent experiences to provide an induction tool, training resource and aide memoire for operational policy professionals. The handbook was established as a key guide for policy and strategy making across UK Defence, for both civilian staff and military personnel and integrates the importance of Strategic Communication (StratCom) and Information Operations throughout with 13 specific references in the 59 page handbook. The handbook has been cascaded across UK Defence HQs and our Partners Across Government and importantly for iPower community colleagues, stresses to mainstream policy and strategy staff the centrality of influence and the enduring maxim that 'you cannot not communicate'. The strategic narrative is a theme throughout the handbook; ensuring that it is credible, grounded in audience insight and ensuring that there is no gap between public rhetoric and our ability to deliver. If you are seeking 'evidence' of why IPower needs more emphasis in your HQ, we suggest using this UK example.

IPower readers that can spare some time to read through the handbook will see the weakness in that it portrays 'the good operation' (singular) and not the 'good operations' (plural) that we are committed to at the moment. This is a necessary simplification in order to get key teaching points across to readers clearly; the real-world challenge we face is managing and supporting multiples of the 'good operation' without the narratives conflicting or creating target audience fratricide. It is also necessarily linear in approach as a training resource and we have more to do to get new operational policy professionals to see the Information Environment as a complex-adaptive system where any action in one area can have offset and tangential impact on other audiences. That said, the 'Good Operation' handbook has been widely well received and as more of our current operations and contingencies are focused on DETER and REASSURE effects where informational power is subordinate to our hard power advantages, we look forward to developing more examples of where the cognitive effect on strategic audiences has been at the centre of policy and strategy making.

Our thanks to Lt Col Hobbs (UK) for this submission. For more information on the IPower aspects of the UK 'Good Operation' handbook, contact him at Robert.Hobbs863@mod.gov.uk.

"Cyber Command granted new, expanded authorities" (Fifth Domain, Mark Pomerleau, 28 Feb 18)

"Under a new plan put in place late last year, the head of U.S. Cyber Command received expanded authorities, but Fifth Domain has learned Congress and the Department of Defense have considered further extending those powers."

"Information Warfare in an Information Age" (Joint Forces Quarterly 85, 2QFY17)

"In the past week, how many devices have you used that were connected to the Internet or relied on an algorithm to accomplish a task? Likely, the number is upward of 10 to 15, and most of those devices are used daily, if not hourly. Examples may include a Fit-Bit, cell phone, personal computer, work computer, home monitoring system, car, Internet television, printer, scanner, maps, and, if you are really tech savvy, maybe your coffee pot or refrigerator."

"Commanding in Multi-Domain Formations" (MAJ Anthony Clas, 1 Mar 18)

"The three pillars of the U.S. Department of Defense strategy are protect the homeland, build security globally, and project power and win decisively. The U.S. military presence around the world resulting from this strategy continues to provide its armed forces opportunities to bridge the gap into the future of warfare—war on a multi-domain battlefield. Multi-domain battle is the conceptual framework used to visualize potential combined arms capabilities across physical and psychological domains required against a near-peer enemy threat in an emerging twenty-first century multi-domain operational environment (MDOE)."

"Russian hackers hunt hi-tech secrets, exploiting US weakness" (Associated Press, 7 Feb 18)

"Russian cyberspies pursuing the secrets of military drones and other sensitive U.S. defense technology tricked key contract workers into exposing their email to theft, an Associated Press investigation has found. What ultimately may have been stolen is uncertain, but the hackers clearly exploited a national vulnerability in cybersecurity: poorly protected email and barely any direct notification to victims."

"Russian Hacker False Flags Work—Even After They're Exposed" (Wired, Andy Greenburg, 27 Feb 18)

"The Kremlin has increasingly turned to false flag hacking operations. And even when those attempts to confuse forensics fail, they still succeed at sowing future doubt. False flags, for the modern nation-state hacker, are quickly becoming as standard a part of the toolkit as phishing links and infected Microsoft Office attachments. Why simply hide your identity when you can simply paste a new one over it, invented or borrowed? Russia's hackers, in particular, have lately experimented with that digital mask-swapping with increasingly deceptive tactics—ones that, even when their deceit is successful dispelled, still manage to muddy the waters of accountability."

"How the Marines are mobilizing forces for information warfare" (C4ISRNET, Mark Pomerleau, 20 Dec 17)

"The Marine Corps is making a fundamental shift to better posture itself and organize in the emerging information environment. While the service recently established a new deputy commandant for information, a three-star position that oversees all aspects of information warfare, the Marines also recently created a new Marine Expeditionary Force Information Group (MIG) at all three MEFs."

"Corps unveils new cyber job field" (Marines Corps Times, Shawn Snow, 2 Mar 18)

"The Marine Corps on Thursday approved the creation of a new cyber occupational field as the force continues to adapt to new emerging threats and an increasingly hostile information environment. Announced in MARADMIN 136/18, the new 1700 cyberspace field includes seven new jobs ranging from cyber weapons, development, and defensive and offensive cyber operators."

IPOWER NEWS

"The Narrative and Social Media" (NATO STRATCOM Center of Excellence, Miranda Holmstrom)

"In the Strategic Communications (StratCom) community, we work to get effects, actions, and changes in behaviour from our target audiences. Intuitively one would argue that we are on a mission to persuade people to do things differently, or at least to change their opinions. 'Winning hearts and minds' may seem easy, especially when you have the truth, logic, or at least a lot of money on your side."

"What Putin Really Wants" (The Atlantic, Julia Ioffe, 17 Dec 17)

"Russia's strongman president has many Americans convinced of his manipulative genius. He's really just a gambler who won big."

"Cyber is being normalized with traditional military operations" (Fifth Domain, Mark Pomerleau, 14 Sep 17)

"Organizations like U.S. Cyber Command are working to integrate cyber teams into theater-wide campaign plans to be used by joint force commanders as they see fit. The most public of these efforts is currently in the Middle East in the fight against the Islamic State group."

IPower News

IPower News is located at https://intelshare.intelink.gov/sites/jiowc/sub/FS/FD/PublicDocuments/IPOWER%20News. Submissions can be made at any time to Mr. Brent Fountain at brent.j.fountain.ctr@mail.mil and Mr. Michael Adams at michael.f.adams3.ctr@mail.mil. Submission does not guarantee inclusion or a specific schedule.

Any problems receiving files contact Mr. Fountain.

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.