“US officials sound the alarm over daily conflicts” (C4ISRNET, Mark Pomerleau, 15 Feb 19)
"With greater fervor than in recent years, U.S. military leaders say they are engaged in a heightened global conflict every day in the information space.

"I don’t think the salvo has been fired, they’re firing. We’re at war right now in cyber. We’ve been at war for a decade. If Gen. [Paul] Nakasone or Gen. Glavy, they’d tell you, we’re pouring oil over the castle walls every day," Gen. Robert Neller, the commandant of the Marine Corps, said during a panel discussion Feb. 15.

Adversaries in the information domain — be it cyber, social media, influence, electromagnetic spectrum — are trying to leverage these capabilities to gain an advantage without firing a shot. In recent months, officials said that within this information sphere, the United States is engaged in what is referred to as phase 3 operations with its enemies. This comes despite the fact that formally, there is no declared conflict and physical forces are not involved."

“Future War: Not Back to the Future” (War On The Rocks, Mike Dana, 6 Mar 19)
“In World War II we primarily fought a three-domain fight — sea, air, and land. American factories ensured we had the mobility and mass to overwhelm our enemies in these three domains. Today, and in the future, we will be fighting adversaries in seven domains — sea, air, land, space, cyber, as well as two "new-old" domains: perception and time. Space and cyber operations hold the potential to have more of an impact on future war than the bombs and bullets in wars past. Similarly, the weaponization of social media, as detailed by Peter Singer and Emerson Brooking in the book LikeWar, speaks to the “war of perception” amongst friends and foes alike. Artificial intelligence — better described as augmented intelligence — has the potential to create man-machine teams that will establish overmatch at every level and function of warfare. All of this is new and foreboding — and we need to understand its implications in both armed and unarmed conflict."

“Russian General Pitches ‘Information’ Operations as a Form of War” (New York Times, Andrew E. Kramer, 2 Mar 19)
"General Gerasimov said Russia’s armed forces must maintain both "classical" and "asymmetrical" potential, using jargon for the mix of combat, intelligence and propaganda tools that the Kremlin has deployed in conflicts such as Syria and Ukraine.

And he cited the Syrian civil war as an example of successful Russian intervention abroad. The combination of a small expeditionary force with “information” operations had provided lessons that could be expanded to “defend and advance national interests beyond the borders of Russia," he said."

“Pentagon outlines its first artificial intelligence strategy” (Associated Press, Matt O’Brien, 12 Feb 19)
““Other nations, particularly China and Russia, are making significant investments in AI for military purposes, including in applications that raise questions regarding international norms and human rights,” the report says. The report makes little mention of autonomous weapons but cites an existing 2012 military directive that requires humans to be in control."

“NATO Group Catfished Soldiers to Prove a Point About Privacy” (WIRED, Issie Lapowsky, 18 Feb 19)
"THE PHONY FACEBOOK pages looked just like the real thing. They were designed to mimic pages that service members use to connect. One appeared to be geared toward a large-scale, military exercise in Europe and was populated by a handful of accounts that appeared to be real service members.

In reality, both the pages and the accounts were created and operated by researchers at NATO’s Strategic Communications Center of Excellence, a research group that’s affiliated with NATO. They were acting as a "red team" on
behalf of the military to test just how much they could influence soldiers’ real-world actions through social media manipulation.”

“Navy looks to expand the reach of its information warfare teams” (C4ISRNET, Mark Pomerleau, 15 Feb 19)
“The Navy is considering extending its information warfare enterprise beyond the tactical space to compete with adversaries on a broader level, one that may not include specific battlefields, though details regarding how the service may do this aren’t yet apparent.

Vice Adm. Matthew Kohler, deputy chief of naval operations for information warfare and director of naval intelligence, said the service is considering an information warfare construct that would reach beyond the tactical, carrier strike group level.”

“How to recognize fake AI-generated images” (Medium, Kyle McDonald, 5 Dec 18)
“In 2014 machine learning researcher Ian Goodfellow introduced the idea of generative adversarial networks or GANs. “Generative” because they output things like images rather than predictions about input (like “hotdog or not”); “adversarial networks” because they use two neural networks competing with each other in a “cat-and-mouse game”, like a cashier and a counterfeiter: one trying to fool the other into thinking it can generate real examples, the other trying to distinguish real from fake.”

“How One of America’s Premier Data Monarchs is Funding a Global Information War and Shaping the Media Landscape” (Mint Press News, Alexander Rubinstein and Max Blumenthal, 18 Feb 19)
“His boss is Pierre Omidyar, the ebay founder best known for his sponsorship of The Intercept, a flashy progressive publication that possesses the classified documents exfiltrated by NSA whistleblower Edward Snowden. Unlike rival Silicon Valley billionaires Peter Thiel, Jeff Bezos, and Eric Schmidt, Omidyar has mostly managed to keep his influential role in media below the radar. And while he directs his fortune into many of the same politically strategic NGOs and media outlets that George Soros does in hotspots around the globe, he has never been subjected to the public scrutiny and often ugly attacks that dog Soros. And yet Samantha Power, the former U.S. ambassador to the UN and liberal interventionist guru, has explicitly praised Omidyar as someone who is following in the footsteps of Soros.”

“How to Fight Russian Infowar in Central Europe” (Defense One, Radu Magdin, 12 Oct 18)
“Traditional counter-propaganda techniques are increasingly effective. The next steps will require focus, engagement, and new thinking.

After years of low awareness and fragmented approaches, the West is finally coming to grips with Russia’s hybrid warfare in Eastern Europe. The next steps will require focus, engagement, and new thinking.

Since 2014’s surprise military intervention in Crimea — which then-NATO Supreme Allied Commander Philip Breedlove dubbed the most amazing blitzkrieg we have ever seen in the history of information warfare” — a wealth of Western studies have documented the strategies used to undermine the democratic foundations and values of the EU and their promotion in Western Balkans and the countries of the Eastern Partnership. Tactical, strategic, and long-term priorities have been put forward to educate the populace. Policy- and decision-makers can refer to the Center for European Policy Analysis’s 2016 report on winning the information war and the European Parliament’s 2016 analysis on strategic communication to counter propaganda. There are even bodies to coordinate the West’s response: the EU’s East StratCom task force and NATO’s StratCom Center of Excellence.”
“SOCOM needs to step up its propaganda game, Pentagon deputy says” (Military Times, Kyle Rempfer, 6 Feb 19)

WASHINGTON — The Defense Department wants U.S. Special Operations Command to do more than the traditional leaflets-and-loudspeakers approach to information warfare, a senior Pentagon official said this week.

“We need to move beyond our 20th century approach to messaging and start looking at influence as an integral aspect of modern irregular warfare,” Andrew Knaggs, the Pentagon’s deputy assistant secretary of defense for special operations and combating terrorism, said at a defense industry symposium Tuesday.

“CNO Wants More Cyber, IW in Navy’s Wargames” (Breaking Defense, Paul McLeary, 6 Feb 19)

“While Adm. John Richardson didn’t provide any details to flesh out his thinking during an appearance at the Atlantic Council, he said "we’re now getting to the point where we’ve got to start in a robust fashion wargaming these elements of conflict…so we understand [how to respond] when we need the authorities to do the things we need to do.”

Richardson’s comments come after the other services have long since moved out on trying to get their cyber and IW houses in order. The Army, Marines, and Air Force have each already talked about their efforts to incorporate Multi-Domain Operations into their wargaming. The idea is to flesh out ways to attack high-tech defenses with coordinated thrusts across all domains — land, air, sea, space, and cyberspace simultaneously. The Navy hasn’t yet signed on to conducting such operations to quite the same degree, but Richardson’s comments Wednesday may be a signal that the service is getting more serious.

“Facebook’s ‘10 YEAR CHALLENGE’ is just a Harmless Meme—Right?” (WIRED, Kate O'Neill, 15 Jan 19)

“IT’s worth considering the depth and breadth of the personal data we share without reservations...Is it bad that someone could use your Facebook photos to train a facial recognition algorithm? Not necessarily; in a way, it’s inevitable. Still, the broader takeaway here is that we need to approach our interactions with technology mindful of the data we generate and how it can be used at scale. I’ll offer three plausible use cases for facial recognition: one respectable, one mundane, and one risky.”

JIOWC Force Development Training Intelink webpage

JIOWC has created several short, computer-based training modules including: Assessment Primer, IOII for the IO Planner, MILDEC refresher, IO in the Joint Planning Process, Threats in the IE, and Information Joint Function Basic Familiarization. These modules can be reached via the hyperlink embedded in this item’s title.

Info Power News is located at: https://intelshare.intelink.gov/sites/jiowc/sub/FS/FD/PublicDocuments/Info%20Power%20News

IPOWER News archives can be found at: https://intelshare.intelink.gov/sites/jiowc/sub/FS/FD/PublicDocuments/IPOWER%20News%20-%20Archives and https://my.nps.edu/web/dod_iocr

Submissions can be made to JIOWC any time to Mr. Brent Fountain and/or Mr. Jonathan Drummond. Submission does not guarantee inclusion or a specific schedule.

NOTE: If any 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.