The Gathering Storm:
A Charge to Fight the Information War

Word Count: 2478

The Strategic Environment

Do you see the gathering storm? It's there, lurking at the forefront of our national consciousness. It's growing – an existential maelstrom – into a raging tempest of values and philosophy. It is a storm of ideas, a conflict of information, a clash of civilizations. It may be this generation's prime heroic obligation: to fight and win the Information War. I speak, of course, of great power competition and the war of active measures.

The Information War is not a Cold War as some suggest.[1] It is anything but cold. The common use of the Soviet-style "active measures" proves as much.[2] It is a war that spreads insurgent ideas through the interconnections of our modern age like a disease through a caged population. It is a war marked by China's use of news manipulation and influence operations to outflank American partnerships in Southeast Asia and Latin America.[3] It is a war marked by Russia's use of social media to sow distrust within Western society.[4]

Incipient in nature, China and Russia seek to undermine the norms of Western society such as liberty, truth, consent of the governed, and equality before the law. Active measures are not ships, submarines, or aircraft. They are ephemeral, normative, and informational. One cannot attack information with a bomb. It requires persistence, strategy, and integrated forces driving towards a central message. Our new warfighting domain is information. The Navy must mature its ability to fight the Information War and do so quickly.

A Call to Arms

In "A Design for Maintaining Maritime Superiority 2.0," the Chief of Naval Operations identifies four lines of effort to meet the Navy's modern strategic goals. The Navy must "strengthen naval power at and from the sea, achieve high-velocity outcomes, strengthen our Navy team for the future, and expand and strengthen our network of partners."[5] However, the Navy will fail to meet these goals unless it drives to fight and win the Information War.

In 2009, the Navy established the IWC with three missions to meet this threat. First, information warriors are charged to provide battlespace awareness by collecting

---

[1] Admiral James Stavridis, US Navy (ret.), "New Cold War at Sea is Brewing," *USNI Proceedings*, May 2017.
[2] Vishnu Kannan, "Senate Intelligence Committee Report on Russian Active Measures: Part One," *Lawfare*, 25 July 2019.
[3] Lara Seligman, "U.S. Military Targets Growing Russian and Chinese Influence in Latin America," *Foreign Policy,* 19 November 2018.
[4] Scott Shane, "Five Takeaways From New Reports on Russia's Social Media Operations," *The New York Times,* 17 December 2018.
[5] Chief of Naval Operations, "A Design for Maintaining Maritime Superiority 2.0," 17 December 2018. https://news.usni.org/2018/12/17/design-maintaining-maritime-superiority-2-0

and interpreting data and information to provide warfighting commanders supremacy on the battlefield. Next, information warriors assure effective command and control capabilities between commanders and their forces. Finally, information warriors integrate information related capabilities (IRCs) into offensive fires to achieve freedom of maneuver across all warfighting domains. These IRCs cover more than a dozen tactical proficiencies that include electronic warfare (EW), military deception (MILDEC), military information support operations (MISO), cyberspace operations (CO), public affairs (PA), and civil-military operations (CMO).

Battlespace awareness, assured command and control, and integrated fires. With a directed purpose to leverage these disciplines to fight the Information War, the IWC can achieve the CNO's drive for maritime superiority in the 21st Century. However, the IWC is still not positioned to fight and win in the new tactical information environment. I propose an IWC paradigm shift along four lines of effort that can help the Navy triumph on the information battlefield. With key changes to its organization, training, operations, and partnerships, the IWC will forge a new path to global security through winning the Information War against China and Russia.

Organization

Organization is that critical foundation that reveals if the IWC has the organic skills and resources to meet the information warfare (IW) threat that challenges the Navy's lethality. In order to enable its information warfighting ability, the IWC should integrate the Public Affairs Community into its ranks

The Public Affairs Community is a natural partner to the IWC. In fact, Joint Publication 3-13 on Information Operations identifies public affairs in line with EW, MILDEC, MISO, and CO as the most important IRCs for an effective IO campaign.[6] By incorporating the Public Affairs community under the IWC umbrella, we can create further opportunities to enhance the lethality of our information forces.

If an operational unit's Public Affairs team had a deep understanding and appreciation for IWC capabilities across battlespace awareness, assured command and control, and integrated fires, they could integrate their public messaging to counter adversary propaganda. By using real time intelligence, Public Affairs professionals could drive their message composition and dissemination with tested precision. The Naval Intelligence community would benefit from Public Affairs providing collection requirements for these purposes. This functional integration would improve the intelligence mission by identifying the critical nodes and centers of gravity for adversary IO across operational threat environments. Further, it would assist the public affairs mission by helping to identify when, where, and how to reach the best audiences. Such strategic communications and engagements are the bedrock of an effective IO campaign.

[6] Joint Staff, "Joint Publication 3-13 Information Operations," November 2014.

Partnerships

Partnerships are the fundamental fact of mission success that allows a complex organization to amplify its own capabilities with strategic augmentations. The IWC is a partnership organization. It was founded when the Naval Intelligence, Cryptologic Warfare, Information Professionals, and Meteorologists joined to meet future IW threats. Such critical partnerships enable the IWC missions that serve all warfighting commanders. However, these intra-service partnerships are insufficient. The IWC should expand international, inter-service, and inter-domain partnerships as well.

On the international front, the Naval Intelligence community must lead the IWC to foster more comprehensive and beneficial intelligence sharing partnerships with our foreign allies. The Five Eyes partners are valuable, but this partnership neglects the key tenet of information warfare: Information Warfare is asymmetric. It does not require significant resources or historic lines of communication. It is a reflexive warfighting domain with low barriers to entry. Therefore, the IWC must develop new intelligence relationships specifically geared towards IO and counter-IO.

These new relationships should acknowledge that unconventional partners have a significant part to play in future global stability through the information environment. The most useful international partners are those not just strong in military and economy, but those strong in information, international goodwill, and trust. For example, Naval Intelligence professionals should push for a new IW-centric multilateral partnership that includes India, Japan, and states from ASEAN, the Baltics, and Latin America.

These nations represent more than 40% of the world's increasingly wealthy and healthy population living under democratic governments. This audience is a critical component of strengthening naval power at and from the sea. The information environment is the most effective domain to do so. The purpose of this international IW bulwark is to enable rapid intelligence sharing for counter-IO and counter-malign foreign influence of the Chinese and Russian regimes.

Most notably, this partnership would also add a critical capability to our Naval Forces – the ability to use these partnerships to amplify the Navy's message to broad international audiences. This integrated message must be built on a common intelligence picture of the most significant strategic IO threats. Further, our naval exercises, port visits, and key leader engagements with these nations will foster good will among these critical and vast populations.

On the inter-service front, the Cryptologic Warfare Community (CWC) must lead the IWC to foster more regular and tactical partnerships with IO professionals from other services. The value in such mission-oriented partnerships cannot be overstated. Historically, the Navy does not maintain tactical proficiency in IO capabilities like MISO and MILDEC. To drive tactical warfare capabilities that can

win the Information War, the Navy must integrate operations with the Army, Air Force, and Marine Corps. The Army's 1st IO,[7] the Air Force's 39th IO,[8] and the Marine Corps Information Operations Center[9] are consummate professionals with decades of experience in the IO disciplines of MISO and MILDEC. The CWC, already proficient in other IRCs like CO and EW, should take point on integrating these additional IO fires into full spectrum naval warfare by internalizing the proven tactics, techniques, and procedures from the other services.

Finally, the Public Affairs Community should lead the IWC in engaging civilian sector companies such as social media giants, news organizations, and broadcast media corporations. These partners, both domestic and international, can preserve the free-flow of truthful and legitimate information. This expanded public-private partnership will serve a similar function for the Navy as the U.S. Information Agency (USIA) did for the U.S. government during the Cold War. Arguments against reinstating a new USIA are well established and beyond the scope of this article.[10] However, USIA did provide an operational arm for critical components of IW such as international educational exchanges, speaking tours, and media services. The Public Affairs Community can build such operational capabilities for the IWC. A coalition of public-private IWC partnerships operationalized through the Public Affairs Community will strengthen naval power globally by engaging the information environment.

Training

In order to meet the Information War strategic threat environment, enhanced organization and partnerships require a robust training program geared towards employing IO at all levels of war. Today's status quo sees the IWC with five disparate training paths and few overlapping skillsets. While the independent training pipelines are crucial for proficiency in each designator's mission set, a common core must be established that meets two objectives related to maintaining maritime superiority: tactical IO employment and operational IO planning.

First, the Navy's Center for Information Warfare Training (CIWT) must develop tactical IO as a core discipline for all junior officers in the IWC. This training must include IO targeting and directing IO fires across all IRCs. CIWT can look to the Army and Air Force training programs for inspiration and curriculum development. The Army offers a short Tactical Information Operations Planners course that covers tactical IO employment across IRCs such as operational security (OPSEC), MISO,

---

[7] U.S. Army 1st IO Command. https://www.arcyber.army.mil/Organization/1st-IO-Command/
[8] U.S. Air Force 39th IO Squadron. https://www.afcyber.af.mil/About-Us/Fact-Sheets/Display/Article/965285/39th-information-operations-sq/
[9] Marine Corps Information Operations Center. https://www.quantico.marines.mil/Tenants/Marine-Corps-Information-Operations-Center/
[10] Matthew Armstrong, "No, We Do Not Need to Revive the U.S. Information Agency," *War on the Rocks,* 12 November 2015.

MILDEC, EW, and Civil Military Operations (CMO).[11] CMO, when combined with the multilateral partnerships discussed in the previous section, would create a formidable high velocity warfighting capability in the information domain. The Air Force also employs a rich initial skills course that covers all tactical IO capabilities during 15-weeks of intensive instruction at Hurlburt Field in Florida.[12] CIWT should create a similar course that provides a common tactical core for all officer designators in the IWC.

Second, CIWT must provide staff IO planning expertise to all senior O-3 and newly promoted O-4 IWC officers. The Navy does not have a dedicated IO Planning Course. Currently, Naval Officers who want to learn the operational level of information war must apply for the Joint Information Operations Planners' Course. Only four such courses are offered annually and priority enrollment goes to those serving in Joint IO billets.[13] To meet the needs for fighting the Information War, the Navy requires more training for operational IO planning.

Two immediate solutions do exist. First, CIWT should approach the Naval War College to incorporate IO planning into the Maritime Operational Planning Course. Though only offered twice annually, this course is dedicated for those serving at maritime headquarters and is structured to meet current maritime threats with advanced studies in operational planning and crisis action planning.[14] The second immediate solution is for CIWT to approach the Army's 1st IO to reserve seats in their annual training program. Army's 1st IO has a robust and experienced training branch that provides more than 20 annual courses in operational IO topics that include specific IRC integration and planning courses as well as Russian and Chinese information warfare threat seminars.[15]

Operations

The IWC can further integrate IO into global maritime operations by investing in cyber-from-sea. By doing so, the IWC will achieve the CNO's strategic goals for high-velocity outcomes and strengthening naval power from the sea. Cyber-from-sea is a woefully misunderstood and controversial concept, but one that can deliver a much needed information warfighting capability to afloat units. While some imagine cyber-from-sea to mean offensive cyberspace operations with exploding power generators and rogue radar systems, it is a more broad IO capability. If properly

---

[11] U.S. Army Combined Arms Center, Tactical Information Operations Planners' Course. https://usacac.army.mil/organizations/mccoe/iop/tiopc

[12] Stephen Losey, "Information operations officers get their own school," *Air Force Times,* 13 March 2018.

[13] National Defense University, Joint Information Operations Planners' Course. https://jfsc.ndu.edu/Academics/Joint-C2-Information-Operations-School-JC2IOS/Information-Operations-Division/JIOPC/

[14] U.S. Naval War College, Maritime Operational Planners Course. https://usnwc.edu/college-of-maritime-operational-warfare/Core-Curriculum/Maritime-Operational-Planners-Course

[15] U.S. Army 1st IO Command, IO Training. https://www.1stiocmd.army.mil/Home/iotraining

enabled, cyber-from-sea can provide afloat units with critical collection, battlespace awareness, integrated fires, and information delivery tools that support the full range of maritime operations.

If the IWC were to invest in a strong social media presence in all major global ports and transit regions, afloat cyber units could use these social media personas to monitor local population sentiment and reflections to naval operations in real time. These operations would provide intelligence, surveillance, and reconnaissance during sensitive activities, or create a measure of effectiveness after an operation.

Further, the IWC could maintain these localized personas to enable IO message delivery to critical audiences. With support from the Public Affairs and Intelligence Communities, cyber-enabled MISO could amplify critical messages the Navy wishes to disseminate to local populations. With support from the CWC, the same capability could also be used for cyber-enabled EW during sensitive missions to deny or degrade unwanted adversary communications. While offensive cyber operations are alluring, cyber-enabled IO is a far more powerful and practical tool for afloat units to fight the Information War.

Winning the Information War

In writing "A Design for Maintaining Maritime Superiority 2.0," the CNO sought to meet the strategic intent of our national leaders. However, success in meeting this long-range strategy requires the IWC to pay immediate attention to the gathering storm – the Information War against China and Russia. By focusing on employing IO in daily maritime operations, the IWC can meet the CNO's critical lines of effort. First, reorganizing to incorporate the Public Affairs Community acknowledges the value of transparency and messaging to global populations. Second, fostering IO partnerships across nations, services, and private companies will serve to strengthen the ramparts against China and Russia's insidious global IW operations. Third, a look inward to evaluate the IWC's training will ensure the service members who fight this Information War have the necessary knowledge, skills, and proficiencies to win. Finally, investing in cyber-enabled IO for afloat units will reveal invaluable tools for providing battlespace awareness and integrating IO fires into maritime operations. By prioritizing and engaging on all four fronts, the IWC will find itself more capable to fight and win the Information War.