Integrate to Dominate

Second Place Award

**2016 *U.S. Naval Institute*
and the
Naval Intelligence Professionals
*2016 Naval Intelligence Essay Contest***

**By
CDR Michael Dahm, USN**

Integrate to Dominate

DESIGN
MAINTAINING

U.S. Naval Intelligence must look back on its history and forward to future challenges to reshape itself and take the lead in integrating the Information Warfare Community.

The U.S. Navy's 2016 strategic guidance, *A Design for Maintaining Maritime Superiority*, invokes lessons from the masters - Mahan, Corbett, Clausewitz, Sun Tzu and Mao.[1] The *Design* also cites emerging forces that will shape future challenges to U.S. military advantages. U.S. Naval Intelligence must reshape itself by similarly examining historical truths and leveraging its deep understanding of potential adversaries to divine whether the nature of warfare has changed in the information age. Moving forward, Naval Intelligence should take a leading role in evolving the Information Warfare Community (IWC) that the Navy created in 2009 to integrate the Intelligence, Cryptology, Communications (Information Professional), and Oceanography Communities.

The Blackest Day

The *Design* mandates, "[b]egin problem definition by studying history – do not relearn old lessons."[2] Considering an example of how *not* to fight reveals a history that must not repeat itself.

World War II 's Battle of Savo Island in August 1942, was the opening naval engagement in the Guadalcanal campaign to dislodge the Japanese from the Solomon Islands. Then Chief of Naval Operations (CNO), Fleet Admiral Ernest King, said the battle was "the blackest day of the war."[3]

Savo Island overlooks the western approaches to Savo Sound ("Iron Bottom Sound") where the Marines had staged their Guadalcanal landings on 7 August 1942. In response to the surprise invasion, the Imperial Japanese Navy's Eighth Fleet immediately dispatched a surface force to destroy the Allies in night combat. At 0130, 9 August, the Japanese task force commander, Vice Admiral Gunichi Mikawa, gave the order to attack the Allied Western Screening Group

---

[1] U.S. Navy, *A Design for Maintaining Maritime Superiority (Version 1.0)*, Jan 2016: 4.
[2] Ibid. 7.
[3] Wolfert, Ira "Guadalcanal Risk Explained by King," *New York Times,* 22 Oct 1945: 5.

protecting the amphibious transport ships still offloading at Guadalcanal. Forty minutes after the shooting started, Mikawa gave the order to withdraw.[4]

The night action resulted in the sinking of four Allied heavy cruisers – *USS Quincy*, *Vincennes*, and *Astoria* as well as the Australian *HMAS Canberra*. The destroyer *USS Jarvis* was heavily damaged and was sunk later that day in a Japanese air attack. In the end, the Allies counted 1,275 dead and over 700 wounded. The Japanese losses amounted to only 58 dead, 70 injured and light damage to three ships.[5] Despite Mikawa's decision not to continue his attack against the amphibious ships, the devastating Allied losses and unlocated Japanese ships had the intended effect. The U.S. withdrew its transports from Guadalcanal leaving the Marines stranded ashore with only limited supplies to press their attack. The Battle of Savo Island remains the worst open-water defeat in U.S. Navy history.[6]

Intelligence and information played a prominent role in the Battle of Savo Island. Many of the key elements in the battle relate to fields that today fall within the purview of the Information Warfare Community (IWC). The Japanese capitalized on insightful intelligence assessments, signals intelligence, coordinated reconnaissance, and excellent command, control and communications. Admiral Mikawa enjoyed superior battle-space awareness to include a practiced understanding of deception and the operational environment – using the cover of night and local thunderstorms to obscure his approach. By comparison, the U.S. Navy and its Allies failed to manage the information environment in almost every conceivable way.

The Japanese emphasis on night tactics had been well documented by U.S. intelligence. In the Interwar Period, the U.S. Navy's Office of Naval Intelligence (ONI) had noted Japanese Navy

---

[4] Ohamae, Toshikazu, (Captain, former Imperial Japanese Navy) "The Battle of Savo Island," *Proceedings,* Dec 1957: 1271-3, 1276.

[5] Warner, Denis, and Peggy Warner. *Disaster in the Pacific: New Light on the Battle of Savo Island*. Annapolis, MD: Naval Institute, 1992. 211-2.

[6] Savo Island represents a defeat in underway combat. Arguably, the U.S. Navy suffered greater losses in ships and personnel in some victories including large multi-day engagements like *The Battle of Leyte Gulf*. Of course, the Japanese attack on ships at anchor in Pearl Harbor remains the greatest, single battle loss in U.S. Navy history.

developments in night combat capabilities.[7] Subsequent Naval War College games also demonstrated the devastating effects of Japanese night torpedo attacks.[8] Still, U.S. Navy leadership failed to consider the Japanese would conduct a night raid at Guadalcanal.

On 7 August, after getting underway from New Guinea, the Japanese task force had been sighted sailing toward the Solomons by a U.S. submarine and at least two B-17s.[9] U.S. commanders dismissed the reports, believing the small task force would not be bold enough to attack the numerically superior Allied force. Besides, they believed any Japanese close approach would be detected by Allied aircraft. But long-range reconnaissance and intelligence were poorly coordinated among the Allies and between two major commands, the Southwest Pacific and South Pacific Area. Lack of synchronization compounded by communication breakdowns and time-late reporting inhibited the flow and exchange of information.[10]

There had also been a significant setback in U.S. signals intelligence but there was no corresponding effort to compensate with more robust reconnaissance. U.S. victories at Coral Sea and Midway had been enabled by successfully deciphering intercepted Japanese codes. But the Japanese had changed their cryptographic keys on 28 May 1942, just before the Battle of Midway, thwarting U.S. collection. Japanese communications about their plans for a night raid at Savo Island had been intercepted, but were not decoded until two weeks after the attack.[11]

U.S. commanders' were also overconfident in their ships' new radar capabilities. The limitations of the new technology were not well understood, especially in the cluttered operating environment of the Solomons.[12] The Japanese ships were never detected on radar. Even after

---

[7] Mahnken, Thomas. "Asymmetric Warfare at Sea - The Naval Battles off Guadalcanal, 1942–1943." *Naval War College Review*, 64. 1 (2011): 101-2. *citing* "Night Training and Operations," ONI Report 261, 18 Oct 1934, 907-3000, box 77, ONI Monograph Files, RG 38, NA.

[8] Ibid. 102. *citing* Coffey, R.B. "Tactical Problem V-1933-SR (Operations Problem IV-1933-SR)," 16 Jan 1934, RG 4, Naval Historical Collection, Naval War College, Newport, R.I., 25.

[9] Bates, Richard and Walter Innis. *The Battle of Savo Island, August 9th, 1942*. Rep. no. AD/A-003 037. Department of Analysis, Naval War College. 1950. 98-103.

[10] McCool, Thomas, *Battle of Savo Island, Lessons Learned and Future Implications*. Thesis. U.S. Army War College, 2002. 16.

[11] Quantock, David, *Disaster at Savo Island, 1942*. Thesis. U.S. Army War College, 2002. 18.

[12] Bates. 350.

the attackers were sighted at 3700 yards, the Allies suffered from poor command, control and communications, which threw any attempt at a coordinated defense into disarray.[13]

Professor Thomas Mahnken wrote of Savo Island and other Guadalcanal naval engagements, "In each of the campaign's battles, the side that possessed a superior awareness of the tactical situation prevailed. It was, in other words, the ability to collect, interpret, and act upon information rather than technology that marked the difference between victory and defeat."[14]

In the words of CNO King's flag secretary, Captain George Russell, the Battle of Savo Island was "an object lesson in how not to fight."[15] The "fog and friction" of war was readily apparent and the battle highlighted deficiencies in command, material and training. A fundamental failing, however, was that the U.S. had failed to manage combat intelligence and information while the Japanese were highly successful in leveraging those elements in their asymmetric attack.

The official Navy explanation for the losses at the Battle of Savo Island was "complete surprise."[16] That surprise resulted, not from a failure of any one element of intelligence, but from a systemic failure to integrate intelligence analysis, coordinate surveillance and reconnaissance and understand the operating environment. It was an example of how *not* to achieve battlespace awareness. Naval Intelligence must embrace that object lesson as it looks toward future conflicts.

The "Form of War"

The *Design for Maintaining Maritime Superiority* highlights three interrelated forces that are increasingly important and pose growing challenges for the U.S. Navy – the expansion of the

---

[13] Ibid. 136.
[14] Mahnken. 115.
[15] Warner. 226.
[16] Ibid. 225.

global maritime system, the rise of the global information system and the interrelated force of expanding technological creation and adaptation.[17] The *Design* describes the prominent role of information in modern warfare, describing information systems as accelerating changes that may ultimately undermine U.S. military advantages. Interestingly, the document goes on to invoke a Chinese term suggesting that information warfare may have fundamentally changed the nature of future conflicts.

The *Design* mandates that U.S. Navy concepts and capabilities must address an ability to operate in a "highly 'informationalized' environment."[18] Generically, "informationization" has been described as being to the information age what "industrialization" was to the industrial age. But in the context of a naval strategy, it represents a decidedly Chinese concept. Any web search of "informationization" plus "navy" or "military" yields results exclusively related to Chinese military theory.[19]

More often than not, Chinese "informationization" is mischaracterized by Western commentators. DoD's annual report to Congress on Chinese military power describes informationization as being "roughly analogous to the U.S. military's concept of 'net-centric' capability: it is a force's ability to use advanced information technology and communications systems to gain operational advantage over an adversary."[20] Regrettably, that definition falls well-short of capturing the depth of the Chinese concept. Deputy Secretary of Defense Robert Work got closer with his characterization of Chinese informationalized warfare as "the combination of cyber, electronic warfare, information ops, deception and denial to disrupt [an adversary's] command and control" and deliver decision-advantage to the Chinese.[21]

---

[17] U.S. Navy, *Design*. 2-3.
[18] Ibid. 6.
[19] "Informationization" is also rendered in English as "informationalization" or "informatization." "Informationize" in Chinese - "xìnxīhuà"
[20] U.S. Office of the Secretary of Defense. *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China, 2016*. 43.
[21] Work, Robert. "Deputy Secretary of Defense Speech." Army War College Strategy Conference. U.S. Army War College, Carlisle. 8 Apr 2015.

Informationization does acknowledge the prominence of information technology in warfare but, as Work suggests, the Chinese military conceptualizes informationization much more broadly.

"Informationization" was first featured in China's strategic military guidance in 2004.[22] By Chinese assessments, informationized warfare had emerged as a new "form of war" – the objective basis that drives military operations and modernization.[23] According to the People's Liberation Army seminal publication, *The Science of Military Strategy*, informationized warfare involves the struggle for "three dominances" – air, maritime, and information – with information dominance as the most significant. Air and maritime dominance cannot be achieved without information dominance; information dominance cannot be sustained without the other two.[24]

To answer the information dominance imperative, the Chinese necessarily conceptualize information operations (IO) more broadly. U.S. doctrine describes IO narrowly as an offensive capability used to influence an adversary's decision-making.[25] Chinese writings describe IO in terms of both offense and defense – more akin to the U.S. definition of information superiority – ensuring that China obtains timely, accurate, and relevant information to gain initiative and decision-advantage while denying an adversary the same.[26]

The Chinese have evolved their information warfare (IW) concepts from a different origin than the U.S. The U.S. holds cyber capabilities as the foundation for future IW. The Chinese military have built their IW doctrine on the Soviet concept of "radio electronic combat."[27] Chinese IW

---

[22] Information Office of the State Council of the People's Republic of China, *China's National Defense in 2004*.

[23] "Form of war" in Chinese - zhànzhēng xíngtài. *See* Ming Fangqiu, "Form of War Changing Toward Informationized War," *China National Defense News (in Chinese)*, 27 Jun 2003, http://www.china.com.cn/chinese/junshi/354618.htm.

[24] China Academy of Military Sciences (AMS). *The Science of Military Strategy (in Chinese)*. Ed. Shou Xiaosong. 2013 ed. Beijing: Military Science Press, 2013. 129-30.

[25] U.S. Department of Defense, *Information Operations, Joint Pub 3-13*, 20 Nov 2014: ix-x.

[26] China Academy of Military Science (AMS). *Lectures on the Science of Information Operations (in Chinese)*. Ed. Ye Zheng. Beijing: Military Science Press, 2013. 5. *See also,* U.S. Department of Defense, *Dictionary of Military and Associated Terms, Joint Pub 1-02*, 15 Feb 2016: 111. "***Information Superiority*** - The operational advantage derived from the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same."

[27] Wortzel, Larry. *The Chinese People's Liberation Army and Information Warfare*. Strategic Studies Institute & U.S. Army War College Press, Mar 2014. 11.

incorporates both hard-kills and soft-kills and also includes elements not traditionally associated with IW or electronic warfare (EW) such as "electro-optical confrontation" and "hydro-acoustic confrontation." Cyber capabilities have only recently been integrated to realize the Chinese concept of "Integrated Network Electronic Warfare (INEW)" pioneered by Chinese IO luminary General Dai Qingmin in the early-2000s.[28]

China further elevated informationization in defining the "form of war" in its 2015 military strategy.[29] Wen Bing, a researcher at China's Academy of Military Sciences, explained that this was a qualitative change – information had previously held a leading role, but in 2015, information had assumed a dominant role in warfare.[30] After launching the *Design* in early-2016, VADM Ted Branch, then Director of Naval Intelligence, stated: "The CNO has directed that we 'double-down' on the information domain and information warfare."[31] One wonders if that was because the Chinese had "doubled-down" first.

Achieving information superiority in a future conflict will not be a supporting action for China. It will be their main line of effort. The degree to which the Chinese have emphasized information warfare to gain an asymmetric advantage cannot be overstated. Just as the Japanese effectively used intelligence and information where the Allies had failed, so too are potential adversaries seeking to develop tactical, operational and strategic capabilities across the information domain to challenge U.S. maritime superiority.

Intelligence in Combat

---

[28] China AMS, *Lectures*. 7-8.

[29] Fravel, M. Taylor. "China's New Military Strategy: Winning Informationized Local Wars," *China Brief*, Vol. XV. No. 13 (2015): 3.

[30] Guo Yuandan. "Fight the War at Sea? China Should Make Preparations for Military Struggle at Sea." *Huanqiu Shibao ("Global Times" in Chinese)*, 26 May 2015. http://mil.huanqiu.com/strategysituation/2015-05/6526726_2.html

[31] Anderson, Sharon. "Deputy Chief of Naval Operations for Information Warfare - Taking the Pulse of the Fleet," *CHIPS Magazine*, Jan-Mar 2016.

The *Design's* mission statement stresses that the U.S. Navy will deter aggression, but if deterrence fails, the Navy will conduct decisive combat operations to defeat any enemy.[32] Information warfare will likely play a decisive role in future conflicts whether the U.S. faces the comprehensive juggernaut of Chinese IW, an IW dagger wielded by the Russians, or a truly free-form IW threat from a non-state actor. The battlefields of Southwest Asia have presented challenges, but those information environments have been largely free from active interference. Naval Intelligence and the IWC have yet to be tested against a high-end IW threat especially in a maritime environment.

The suggestions below seek to strengthen the ability of Naval Intelligence and the IWC to prevail in combat operations and are aligned to the *Design's* four lines of effort.[33]

●   **Strengthen Naval Power at and from the Sea**

Naval Intelligence must lead development of information and intelligence warfighting doctrine and operational concepts in "informationalized" environments. The U.S. Navy and Marine Corps developed new doctrine for everything from modern amphibious warfare to aircraft carrier operations between 1923 and 1940. Naval Intelligence must develop its own "Fleet Problems" and test its doctrine in an empirical process that will hone its warfighting capabilities and create a demand signal for new intelligence concepts and new technologies.[34]

"Cyber" has been conspicuously absent from this commentary on Naval Intelligence and information warfare. While this may sound like heresy, the Navy is over-invested in cyber. This is especially true if those investments come at the expense of developing other elements of information warfare, including more traditional intelligence capabilities. Cyber will absolutely be an important element in future conflicts. But just as the U.S. Navy did not understand the

---

[32] U.S. Navy, *Design*. 1.
[33] Ibid. 6-8.
[34] *See, for example, the "Fleet Problem" proposal in* Crooks, DeVere and Mateo Roberaccio. "The Face of Battle in the Information Age," *Proceedings*, Jul 2015: 52.

utility and limitations of radar at Savo Island, how U.S. cyber capabilities will be integrated at the operational level of war with other information warfare and conventional capabilities is not yet clear.

Intelligence and information warfare doctrine, organizations, architectures, technologies and processes must be integrated and stressed under combat conditions in order to realize operational concepts and spur innovation. Naval Intelligence must be able to maneuver in the combat information space and not simply offer "resilience" in a distributed architecture. U.S. Naval Intelligence professionals and "information warriors" must leverage wargaming, modeling and simulation to anticipate threats to intelligence capabilities, perform "damage control," and learn to fight intelligence, surveillance, and reconnaissance (ISR) architectures and processes in combat conditions.

The Chinese military is organizing around their information warfare doctrine. In early-2016, as part of a broader military reorganization, the Chinese announced the creation of the "Strategic Support Force" (SSF). The SSF will reportedly integrate all Chinese information warfare capabilities across space, cyberspace, and the electromagnetic spectrum providing offensive capabilities, targeted reconnaissance and tracking of adversaries, and defense of Chinese physical and virtual networks.[35] The IWC, seven years into its integration, is still seemingly consumed with standing up organizations and processes, spreading workloads across federated architectures and renaming itself. None of this is to suggest that the U.S. must follow the Chinese SSF model. It should be noted, however, that the *Design* directs that U.S. Navy's nascent concept of Electromagnetic Maneuver Warfare must be expanded to "encompass all of information warfare, to include space and cyberspace."[36] The IWC would do well to move more quickly than our adversaries on the *Design's* direction to integrate.

---

[35] Zhao Lei, "New Combat Support Branch to Play Vital Role," *China Daily*, 23 Jan 2016.
  http://www.chinadaily.com.cn/china/2016-01/23/content_23209861.htm
[36] U.S. Navy, *Design*. 6.

- **Achieve High Velocity Learning at Every Level**

Legacy education and training must be turned upside down if Naval Intelligence wants to be a component of a warfare community on par with air, surface and submarines. Today, the IWC places specialization training before establishing a basic knowledge of the information warfare doctrine and operational concepts (that still need to be developed). Naval Intelligence and the other IWC personnel attend respective individual community training upon accession. They subsequently complete a very basic IWC familiarization personnel qualification, test, and oral board during their first tour to become IWC qualified.[37] That is largely the beginning and end of cross-IWC training.

Integrated training and application of information warfighting knowledge, skills and doctrine must become foundational in order to provide the necessary context for what should be follow-on training in an IW specialty. U.S. Naval Intelligence must continue to pursue its core mission to develop a deep understanding of potential adversaries to educate the Fleet about future threats. Balancing these requirements will be challenging but necessary if the IWC ever hopes to develop an integrated warfighting culture.

- **Strengthen Our Navy Team for the Future.**

In support of developing an integrated information warfighting culture, the IWC must follow through on its commitment to integrate. The *Naval Intelligence Strategic Plan, 2013-2017*, established a mission objective to integrate the IWC stating, "Effectively integrating the full capabilities of the entire [IWC] is critical to successful Intelligence Operations."[38] Naval Intelligence must lead the IWC in this effort because, more than any other component, Naval Intelligence has been the ultimate integrator, coordinating reconnaissance and collection, analyzing all-source intelligence, assessing the operational environment, and communicating intelligence across the force.

---

[37] U.S. Navy, *IWCO Qualification Program, OPNAVISNT 1412.13.*
[38] U.S. Navy, *Naval Intelligence Strategic Plan, 2013-2017*, 18.

While reorganizing into a new warfare community and establishing a new information warfare paradigm in the Navy, there have been attempts to establish credibility by suggesting that IWC officers should hold exclusive title to Information Warfare Commander in the Composite Warfare Commander construct or, perhaps, ascend from Restricted to Unrestricted Line Officers. [39] These suggestions are ambitious goals that may eventually come to pass. For the moment, however, integration, development of IW doctrine and honing warfighting skills in simulated combat conditions must be the prerequisite effort.

- **Expand and Strengthen Our Network of Partners.**

The Design acknowledges that even as we face new challenges, the Navy will continue to face a budget environment that will force tough choices, but must also inspire new thinking.[40] The Department of Defense's Third Offset Strategy invites such inspired new thinking to create innovations that will increase military capability while maintaining economy of force. What have come to be known as the First and Second Offset Strategies – characterized by tactical nuclear weapons and precision-guided munitions respectively – were suites of capabilities to offset superior Soviet numbers during the Cold War.

Technology research and development (R&D) currently drives IW concepts and processes. That trend should be reversed. Naval Intelligence and the IWC should lead the way and partner with DoD and other services to advocate for funding of IW doctrine and operational concepts that shape R&D of advanced IW technologies as part of the Third Offset Strategy. DoD has allocated $18 billion over the Future Years Defense Program (FYDP) for R&D related to advanced capabilities that will help realize the next Offset Strategy.[41]

---

[39] *See, for example,* VADM Brown, Nancy *et al*, "Creating Cyber Warriors," *Proceedings*, Oct 2012.
[40] U.S. Navy, *Design*. 4.
[41] Mehta, Aaron, "Defense Department Budget: $18B Over FYDP for Third Offset," *Defense News*, 9 Feb 2016.

Be Battle-Minded

Rear Admiral Richmond Turner, responsible for operations at Guadalcanal in 1942, commented to Admiral Nimitz on the inquiry into the Battle of Savo Island:

> "I have concluded that our forces, both sea and land, at that time simply were not battle-minded… The Navy was still obsessed with a strong feeling of technical and mental superiority over the enemy… The net result of all this was a fatal lethargy of mind which included a confidence without readiness, and a routine acceptance of outworn peacetime standards of conduct."[42]

The Battle of Savo Island is a stark reminder of the power of the many facets of information warfare. In recent conflicts, the U.S. has been operating in uncontested information environments under benign electromagnetic conditions. In implementing the *Design for Maintaining Maritime Superiority*, Naval Intelligence and the IWC must be battle-minded in placing the past in context, projecting future threats and evolving into a combat-capable warfighting community.

---

[42] Warner. 253. *citing* RADM Turner, Richmond, *Memorandum for CinCPac*, in Hepburn, Aurthur. *Informal Inquiry into the Circumstances Attending the Loss of the Vincennes, etc. on August 9th, 1942*. 13 May 1943.