A Design for Maintaining Maritime Information Superiority 2.0

Essay submitted to the U.S. Naval Institute
and the
Naval Intelligence Professionals
2019 Naval Intelligence Essay Contest

2500 words
(does not include title page or endnotes)

The Chinese and Russian militaries, identified as *the* principal priorities in the 2018 US National Defense Strategy, have determined that the modern *character of war* has changed.[1] They believe that military competition has shifted decidedly to the information domain. This is not about influencing strategic narratives with social media. They contend that military forces must vie for battlespace information superiority at the operational-level of war. If there has been a fundamental shift in military competition toward the information domain, then the *Design for Maintaining Maritime Superiority 2.0* will likely fall short of its desired end state: "A dominant naval force… ready for decisive combat operations." The Navy Information Warfare Community (IWC), organized around intelligence, cryptology, cyber, communications, and oceanography designators, must act with urgency to shore up the *Design*, implement information-centric operational concepts and correct the *Design's* course.

Belgrade, 99/05

On 7 May 1999, the NATO alliance was 45 days into its air campaign to end Serbian atrocities in the breakaway Yugoslav province of Kosovo. That night, 10,000 pounds of US ordnance slammed into the Chinese embassy in Belgrade. A B-2 stealth bomber had achieved direct hits on the embassy, mistakenly identified by intelligence analysts as a Yugoslav supply headquarters, which was actually 300 meters away.[2] Twenty years later, the US military is only beginning to come to terms with the scope and scale of the challenges that emerged from the rubble of that Chinese diplomatic compound.

The 1999 US airstrike was a seminal event for the Chinese military, the People's Liberation Army (PLA). Shortly after the bombing, China's highest military decision-making body, the Central Military Commission (CMC), convened an emergency meeting.[3] In response to what they were certain was a brazen act of US aggression, the CMC launched the 995 High-Technology Development Program. "995" refers to the year and month the program was established – May 1999 – memorializing the humiliation suffered by the Chinese military and their inability to respond to the US attack.

The impromptu CMC session took a decision to accelerate the development of high-technology armaments, often referred to in the West as "assassin's mace" weapons.[4] Regrettably, this moniker gives these capabilities an aura of mystery and menace. However, China's high-tech investments were about much more than creating an asymmetry in the correlation of forces. The 995 Program provided the PLA with capabilities to realize asymmetric operational concepts based on information dominance.

Following overwhelming US military successes during the 1991 Gulf War, Chinese military scholars had divined that information warfare (IW) was a critical combat capability. DoD guidance like *Joint Vision 2010*, written in 1996, espoused an absolute imperative for the US military to gain and maintain battlespace information superiority.[5] Nascent Chinese IW theory built upon these US proclamations that were further compounded by visions for dominant battlespace awareness and net-centric warfare espoused by the likes of Admiral Bill Owens and Vice Admiral Arthur Cebrowski.[6]

Recognizing the genius in these information concepts, the Chinese believed that the character of war, what the Chinese call the *form of war*, had changed profoundly in the information age. Beginning in the late-1990's and declared officially and prominently in 2004, the PLA was directed to fight and win *informationized* wars.[7] *Informationization*, while a seemingly awkward term, is analogous to *mechanization*. If machines had transformed industrial age warfare, then information would transform information age warfare.[8]

In the late-1990s, however, Chinese military capabilities that might otherwise enable information-centric concepts were lagging. In 1998, a noted China military analyst offered an assessment of the PLA's IW efforts:

> *"To sum up, the available evidence suggests that the PLA does not currently have a coherent IW doctrine, certainly nothing compared to U.S. doctrinal writings on the subject. While PLA IW capabilities are growing, they do not match even the primitive sophistication of their underlying strategies, which call for stealth weapons, joint operations, battlefield transparency, long-range precision strike, and real-time intelligence. … [T]he Chinese military cannot reasonably expect anything approaching 'information dominance' for the foreseeable future."*[9]

Then came the 995 Program. Major General Yao Youzhi, a former director at the influential PLA Academy of Military Sciences, acknowledged in a 2012 speech that the 995 Program had been created in response to the Chinese embassy bombing and had been directly responsible for accelerating Chinese military development. The general asked who should be thanked. He answered his own question – "We should be grateful to the Americans."[10]

For twenty years, the 995 Program has been a catalyst for developing capabilities to actualize Chinese information-centric operational concepts.[11] Unfortunately, Naval Intelligence and the US Intelligence Community have largely focused on the hardware that has emerged from the PLA's rapid development without bringing China's underlying operational concepts into clear relief.

Great Power Information Competition

China's informationized warfare strategy and Russia's "New Generation Warfare" concept are complex and layered, but both approaches ultimately consider information dominance as *the* main line of effort. They seek to compensate for shortfalls in technology and force structure relative to the US military by creating asymmetries in the information space – strategies to level the battlespace by denying information to superior US capabilities while ensuring information flow for themselves.

Information control is at the center of Chinese informationized operational concepts. China's informationized strategy relies heavily on long-range precision strike, but as a supporting element. One should not underestimate the potency of PLA platforms and weapons, but such a focus on maneuver and firepower should not obscure an understanding of *how* the PLA will employ these capabilities. The Chinese strategy essentially seeks to seize battlespace initiative by first gaining information superiority. PLA operational concepts degrade and destroy adversary C4ISR.[12] Long-range fires contribute to this preliminary action by destroying information nodes and driving reconnaissance, including space-based sensors, far from the battlespace. The net effect is a disaggregation of the adversary joint force into vulnerable elements unable to sense and communicate that are then annihilated by PLA fires.

Russian New Generation Warfare (NGW) strategy contains many of the same tenets as China's informationized warfare strategy. The Russian concept of *information confrontation* serves as an organizing principle for NGW, prioritizing and choreographing all military and non-military campaign efforts.[13] Battlespace effects are achieved through denial and deception (*maskirovka)*, operations in the electromagnetic spectrum, and computer network attacks to shape perception and decision-making at all levels of warfare. Russian military and non-military elements, employed in a holistic, coordinated manner, create information strikes that subvert adversary situational awareness, allowing Russian forces unconstrained freedom of action.[14]

An inability to comprehend just how important information control is to Chinese and Russian operational art reflects "mirror imaging" of the highest order. Institutionally and inexorably wedded to "firepower" and "maneuver" at the center of US operational concepts, US intelligence has responded to demands from leadership for analysis focused on categories of adversary capabilities that they themselves covet. Certainly, there are some who understand these US competitors' information-centric operational concepts. But leaders who continue to focus on procuring "hulls" and "airframes" have largely waved away discussions of battlespace information control to return to their passion for "salvo sizes" and "exchange ratios."

US military leaders have begun to acknowledge that they cannot continue to embrace industrial age, mechanized warfare concepts. General Joseph Dunford, Chairman of the Joint Chiefs of Staff, described contemporary changes to the character of war shortly after the release of the 2018 National Defense Strategy: "Advancements in space, information systems, cyberspace, electronic warfare, and missile technology have accelerated the speed and complexity of war. As a result, decision space has collapsed."[15] While it may not be surprising that information is rapidly changing the character of war, the Chairman's observations are also a tacit admission that Chinese and Russian strategies and their information-centric concepts are working; that they have become significant threats. The US military is just beginning to grasp that these strategies – strategies that our competitors have been developing for decades – have effectively shifted military competition into the information domain.

A *Design* without *Character*

The *Design for Maintaining Maritime Superiority 2.0* is essentially silent on the changing character of war and achieving information superiority as an operational imperative. A graphic that appears in the *Design* depicts information warfare as undergirding military power throughout the competition-conflict spectrum. Beyond this, however, the *Design's* lines of effort make no mention of information warfare. The *Design* instead focuses on recapitalizing the fleet with submarines, ships and aircraft. There are references to supporting "networks," "grids" and "data," but how those capabilities might contribute to combat information superiority is not explicit. *2.0* is a marked departure from the first iteration of the *Design*, a document half as long that discussed the role of operational information twice as much. *Design 1.0* mandated the advancement of information warfare capabilities and envisioned power projection in highly "informationalized" and contested environments.

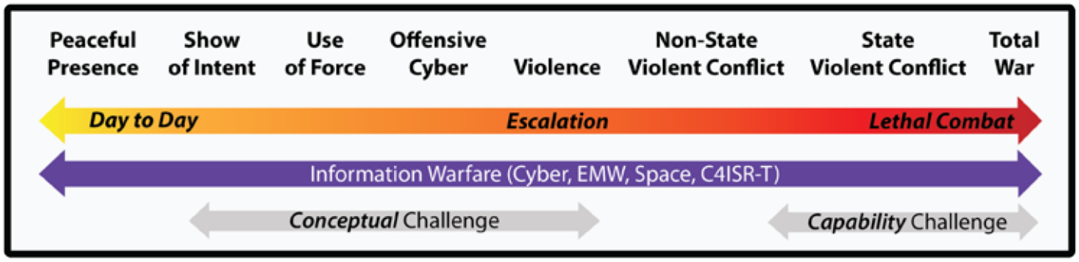

Figure 1. "The **Competition-Conflict Spectrum for the Military Dimension of Power"**

The Navy Information Warfare Community should respond with urgency to changes in the character of war and the information-centric threats posed by military challengers. The following recommendations are aligned with the *Design's* lines of effort (LOE):

LOE Blue: Strengthen Naval Power at and from the Sea

Invest in IW Capabilities. The IWC must advocate for significant increases in C4ISR, especially C4ISR organic to Navy platforms to face the onslaught of adversary counter-C4ISR capabilities. Investments in exquisite networks to distribute information among combat forces are not enough.[16] Frankly, if the Navy doubled its investments in capabilities like reliant ISR, redundant communications, denial and deception, electronic warfare and the personnel to realize those capabilities, it would still not be enough to counter present day Chinese threats to information superiority. The Design appears incongruent with the National Defense Strategy that calls for increased investments in C4ISR and prioritizes capabilities that will gain information superiority over adversaries.[17]

LOE Gold: Strengthen Our Navy Team for the Future

Develop Deep, Penetrating Knowledge of the Adversary. The IWC's Naval Intelligence component must return to what World War II legend Captain Joseph Rochefort said was an intelligence officer's "one job, one task, one mission" – to tell the commander what the adversary is going to do tomorrow.[18] The Fiscal Year 2020 officer promotion board convening orders contain new language from years past: "Intelligence officers are experts on the adversary and threats, and developing deep expertise on our Nation's strategic competitors is an imperative."[19] While that is (or should be) an objectively true statement, the orders place no value on threat expertise as a discriminator over career diversity and leadership. Naval intelligence has become so consumed with its myopic focus on pathways to command that it has lost sight of its "one job."

Inevitably, calls to increase focus on developing adversary expertise will revive years-long debates about whether the present-day Naval Intelligence emphasis on "operational intelligence" (OPINTEL) is enough.[20] In the context of the US military's return to great power competition, it is not. Great power competition is long-term competition. In that sense, what the adversary will do "tomorrow" takes on new meaning. Naval Intelligence must invest in expertise that builds upon traditional OPTINEL skills and incorporates knowledge of adversary military doctrine, organizational culture, language, history and technological trajectories to better inform US Navy training, capability development, and operational plans.

LOE Green: Achieve High Velocity Outcomes

"RED Team" Plans and Exercises. The *Design* directs efforts to use "RED teams" to expose weaknesses and vulnerabilities in plans as early as possible. Over the past several years, there have been clarion calls, many in the pages of *Proceedings*, for more and better adversary RED teams to represent opposition forces (OPFOR) in exercises and war games.[21] Standing RED teams staffed and trained by the IWC would be the operational expression of "deep, penetrating knowledge of the adversary" necessary to drive fleet innovation and capability development.

BLUE commanders may have a false sense of their capability to operate effectively against RED threats. In operational-level war games and planning scenarios, RED normally presents as "drunk and angry," swinging indiscriminately and inviting a fight, highlighting RED's position and conveniently providing BLUE with a pretext to respond kinetically. Recall, however, the adversary operational concepts that focus on information superiority. Realistically, BLUE will be frustrated by RED deception and engaged in a dynamic and probably decisive fight for information superiority before the shooting starts. RED operations, enabled by C4ISR and electronic warfare capabilities that overmatch BLUE are designed to confound and ultimately undo plans to "impose costs." If adversary information capabilities and operational concepts are not faithfully and accurately represented in war games and exercises, our forces will be neither decisive nor dominant in real-world operations.

Advance Information-Centric Operational Concepts. The IWC should *lead* and not simply support the *Design's* mandate to strengthen and improve concept development. The US military does not currently have a coherent doctrine for information warfare at the operational-level of war (seriously). The "five pillars of information warfare" – operational security, electronic warfare, psychological operations, military deception, and physical destruction – have been disaggregated into independent doctrines, few receiving enough sunlight to grow in the oppressive shadow of "cyber." The *Joint Concept for Operations in the Information Environment* addresses control of the strategic narrative in conflict and offers no solutions for operational-level IW application.[22] The IWC and its component communities are in a unique position to lead in developing operational concepts to combine intelligence with integrated IW capabilities and kinetic actions to achieve battlespace information superiority.

LOE Purple: Expand and Strengthen Our Network of Partners

Send IWC Forward. If the US Navy is going to engage in the "high end of maritime conflict" with allies and partners *and* our challengers are pursuing information-centric operational concepts, then information and intelligence links between US and allied forces will become a lucrative target. Developing and hardening communications and intelligence partnerships with allies and partners is an imperative. Regrettably, naval attaché positions in critical allied nations as well as in China and Russia are now open to all designators; discreet community billet allocations were dissolved in 2015. IWC officers should be encouraged to compete for attaché positions to gain critical in-country experience. Intelligence officer tours in China or Russia would contribute to the cadre of personnel with deep knowledge of competitor nations. While Foreign Area Officers (FAOs) are doing great things for Navy engagement, the IWC has ceded far too many opportunities in the attaché corps.

High-Velocity Outcomes… Inbound

"Information won't kill me!" is a refrain often heard from operators when advocating for information-centric concepts and IWC leadership in operations. While "information" may not be the "what" that kills you, it has become the "how." In the information age, the stakes are high. The fallout from the Chinese embassy bombing stands as a reminder of the lasting strategic consequences of faulty information and intelligence failure.

The volume and velocity of information in the modern battlespace, now enabled by artificial intelligence, has created a sea change in the character of war. High-end information effects and long-range strike will generate inbound high-velocity threats that may well lead to undesirable high-velocity outcomes. The Information Warfare Community must embrace the changing character of war and guide the Navy on a course that will allow it to prevail against challengers to US maritime superiority.

Notes

[1] The *character of war* should not be confused with the *nature of war*. According to Clausewitz, the nature of war is enduring – "an act of force to compel our adversary to do our will." The character of war, essentially *how* adversaries engage in conflict, changes over time due to variables such as technological developments, culture, law and politics.

[2] The intended target was the Yugoslav Federal Directorate of Supply and Procurement. Thomas Pickering, "Oral Presentation to the Chinese Government Regarding the Accidental Bombing of The P.R.C. Embassy in Belgrade," (official memorandum, Washington: Department of State, June 17, 1999).

[3] Zhang Wannian Writing Team, *张万年传 [Biography of Zhang Wannian]*, (Beijing: Liberation Army Press, 2011), 416, *as cited in* Tai Ming Cheung et al, "Planning for Innovation: Understanding China's Plans for Technological, Energy, Industrial, and Defense Development (Report prepared for the U.S.-China Economic and Security Review Commission, Univ. of California, Institute on Global Conflict and Cooperation, July 2016), 26.

[4] "杀手锏" is often translated as "assassins mace," but it is a Chinese figure of speech roughly analogous to "trump card" – winning capabilities that are unexpected and decisive.

[5] US Joint Chiefs of Staff, *Joint Vision 2010* (US Government Printing Office: Washington, DC, 1996), 16.

[6] ADM William Owens, "The Emerging System of Systems," *Proceedings*, May 1995, 35-39. VADM Arthur Cebrowski and John Garstka, "Network-Centric Warfare – Its Origin and Future, *Proceedings*, January 1998, 28-35.

[7] China Ministry of National Defense,《2004 年中国的国防》白皮书 [China's National Defense in 2004, white paper] (Beijing: PRC State Council Information Office, December 2004).

[8] 信息化作战 (informationized warfare) may be translated literally as "warfare transformed by information."

[9] James C. Mulvenon, "The PLA and Information Warfare," in *The People's Liberation Army in the Information Age*, ed. James C. Mulvenon and Richard H. Yang (Santa Monica, CA: RAND Corporation, 1999), 185.

[10] Cheng, "Planning for Innovation," 27.

[11] Li Daguang, "从装备发展看解放军建军 90 周年" ["Perspectives on PLA Equipment Development on the 90th Anniversary of the Founding of the Army"], *中国军转民 [China Defense Industry Conversion]*, July 2017, 8.

[12] C4ISR – "Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance."

[13] Sergei Chekinov and Sergei Bogdanov. "The Nature and Content of New-Generation War," *Voennaya Mysl [Military Thought],* Oct-Dec 2013, 18.

[14] Dmitry Adamsky, *Cross-Domain Coercion: The Current Russian Art of Strategy,* (Institut Francais des Relations Internationales (IFRI) Security Studies Center, November 2015), 30.

[15] Joseph Dunford, "The Character of War and Strategic Landscape Have Changed," *Joint Force Quarterly* 89, 2nd Quarter (2018): 2.

[16] The *Design* discusses developing a "comprehensive operational architecture" to support Distributed Maritime Operations (DMO). While this appears to be an initiative to create a communications and data network, it falls well short of integrating broader IW capabilities into DMO.

[17] James Mattis, *Summary of the 2018 National Defense Strategy of the United States of America* (Washington, DC: US Department of Defense, 2018), 6.

[18] Rochefort's full quote regarding the attack on Pearl Harbor was*, "I can offer a lot of excuses, but we failed in our job. An intelligence officer has one job, one task, one mission -- to tell his commander, his superior, today what the Japanese are going to do tomorrow."* John Schindler, *Leadership Embodied: The Secrets to Success of the Most Effective Navy and Marine Corps Leaders*, ed. Joseph. Thomas (Annapolis: Naval Institute Press, 2014), 76.

[19] For example, Gregory Slavonic, ORDER CONVENING THE FY-20 PROMOTION SELECTION BOARDS… LIEUTENANT COMMANDER" (official memorandum, Washington, DC: Department of the Navy, May 16, 2019), 17.

[20] For example, CAPT (ret) Bill Bray, "Naval Intelligence: Build Regional Experts," *Proceedings*, December 2017. CDR Kenneth Klima, "Maximizing the U.S. Navy Operational Intelligence Advantage," *Proceedings*, February 2019.

[21] For example, CAPT Dale Rielage, "War Gaming Must Get Red Right," *Proceedings*, January 2017; ADM Scott Swift, "Fleet Problems Offer Opportunities," *Proceedings*, March 2018; CAPT Henry Kim, "Surface Warfare Needs Aggressor Squadrons," *Proceedings*, May 2019.

[22] US Joint Chiefs of Staff, *Joint Concept for Operating in the Information Environment (JCOIE)* (Washington, DC: US Department of Defense, July 25, 2018).