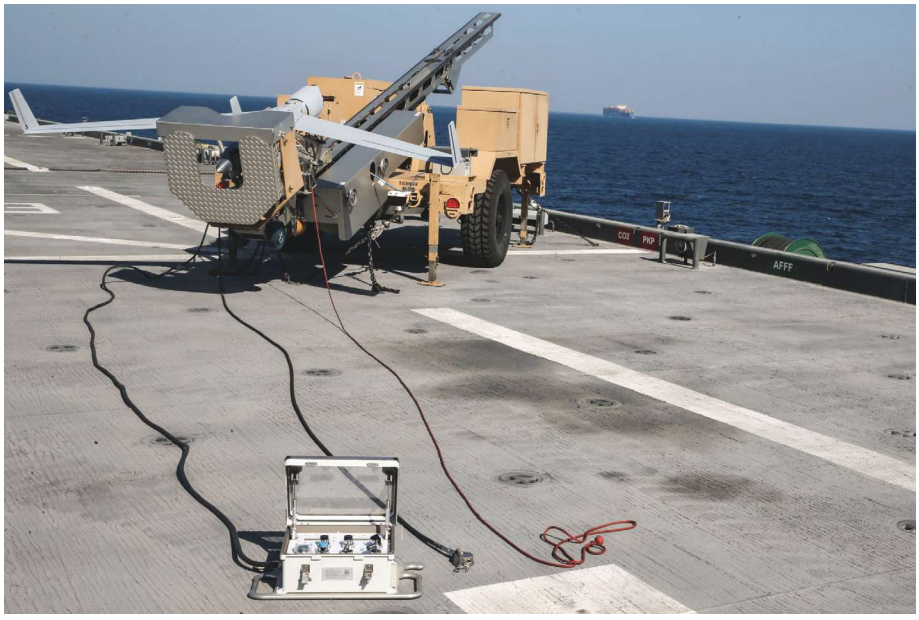
The Competition Continuum

Intelligence support to operations in the information environment

by LtCols Bradley N. Fultz & Aniema G. Utuk

>LtCol Fultz is the CO, 1st Intelligence Battalion, I MEF Intelligence Group, Camp Pendleton.

>>LtCol Utuk is a MAGTF Planner assigned to I MEF Information Group.



Intelligence gathering and reconnaissance missions in the Indo-Pac theater will have to increase as China exerts its influence and military presence in the region. *(Photo by SSgt Anne Henry.)*

Nations do not have friends, they have interests: diplomatic interests, informational interests, and primarily economic interests. America's interests are enduring, evolving, globally integrated, and ultimately exist to serve the citizens. The Nation's robust military enables a pursuit of America's interests at the global level. This costly underpinning is rooted in America's founding and highlighted in Federalist Eleven, where Alexander Hamilton describes the mutually supporting relationship between the Navy, overseas commerce, and domestic employment.[1] Even in the 18th century, the importance of maritime dominance to pursuing the Nation's interests was apparent.

The resurgence of great power competition marks the dawn of a new age, but like the old adage—nothing is new under the sun. Fear, honor, and interests remain the key motivations for conflict.[2] These motivations, however, are scalable depending on the value of the object. Overlapping interests and flashpoints between nations leads to a proportional state of cooperation, competition, or armed conflict that changes with circumstances. History is replete with brilliant descriptors of the interplay between peace, war, and that what lies between: often referred to as gray zone conflict or hybrid warfare.

The existing design framework fails to support the full understanding of a competitive operational environment that sits somewhere between war and peace. As a consequence, the Chairman of the Joint Chiefs released a *Joint Doctrine Note* (JDN), titled the *Competition Continuum*.[3] The competition continuum offers a new paradigm that applies a nuanced look to interstate competition more closely resembling today's realities compared to the existing five-phased designated approach well familiar to planners. The JDN argues the

> joint force is never solely in cooperation (or in competition below armed conflict or in armed conflict) but instead campaigns through a mixture of cooperation, competition below armed conflict, and armed conflict calculated to achieve the desired strategic objectives.[4]

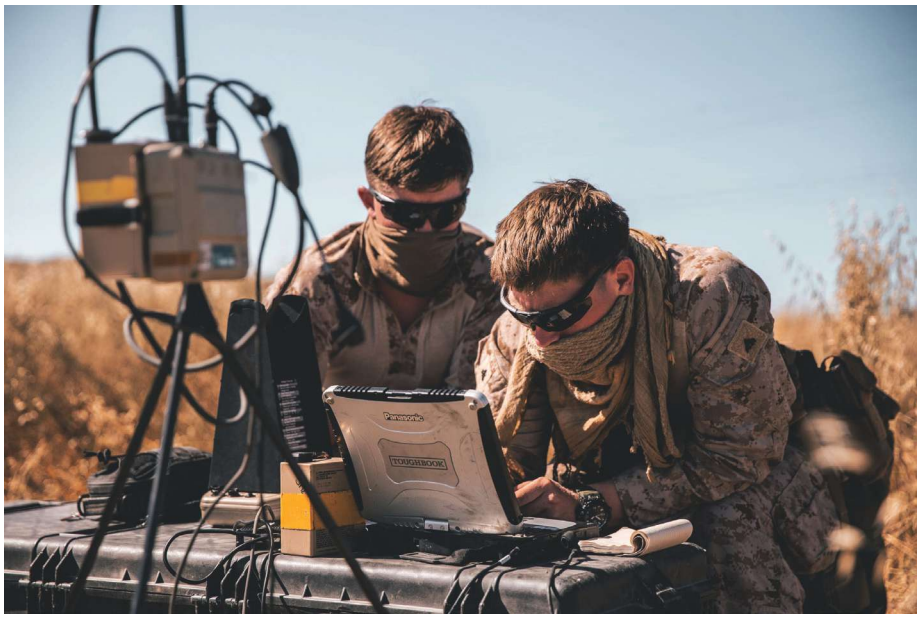
Simply put, the joint force needs a better model to explain the world.

By describing the global environment as a continuum of competition ranging from cooperation, competition below armed conflict, and competition through armed conflict, the joint force is better able to describe the integrated campaigning construct required to compete in a globally competitive setting. This ecosystem consists of activities across domains to include the creation of alliances, direction of

proxies, and objective threats of violent conflict.

Effectively campaigning through the competition continuum requires significant renovations across the joint force, particularly in the highly contested information domain. In fact, it is in the information domain where the DOD is being outmaneuvered. The Marine Corps subscribes to seven functions to enable operations in the information environment (OIE), namely: assure enterprise C2 systems, provide IE battlespace awareness, attack and exploit network systems and information, inform domestic and international audiences, influence foreign target audiences, deceive adversary target audiences, and control information capabilities.[5] Aligning the capabilities of the force to support these functions is required to compete and compensate for the delta in competency. It is a transformational endeavor currently underway.

This article provides limited examples of an adversary operating in the competition continuum, articulates one way in which operations in the IE can respond to such actions, and finally identifies how intelligence supports this effort. The goal is to provide an introduction into how operations in the IE are omnipresent throughout the competition continuum, introduce ways to conduct offensive operations in the IE, and how intelligence can best support operations. The recent joint note provides the broad framework from which to conduct operations in the information environment. We simply need to apply appropriately.



Increasing surveillance and intelligence gathering training exercises between elements of the MAGTF will be required. *(Photo by Sgt Manuel Serrano.)*

Campaigning Through Cooperation

Case Study: Chinese One Belt, One Road Initiative. Arguably the brightest example of a competitor successfully campaigning through cooperation in order to meet desired objectives is the People's Republic of China (PRC) "One Belt, One Road (OBOR) Initiative." First conceived in 2013 by President Xi Jinping, OBOR is the PRC's whole of government approach linking Chinese geopolitical ambitions to the economic influence demanded of a rising global power competing with the United States. Comprising of multiple dimensions, the OBOR initiative consists of an information component known as the "Information Silk Road." The Information Silk Road connects "regional information and communications technology networks, and lowers barriers to cross-border trade and investment in the region." Such efforts are communicated as a "win-win" propaganda message achieved through cooperation with over 70 OBOR participating nations. However, the malign aspects of OBOR is a diplomatic debt trap designed to enhance Chinese naval power abroad, exert PRC influence, and undermine U.S. geopolitical, geostrategic, and security interests in the Indo-Pacific Region.[7]

Campaigning through cooperation is usually an enduring activity with no discrete start or end point; the relationship with the ally or partner is in place and will continue for the foreseeable future.[6]

OIE Response to campaigning through cooperation: Inform and influence domestic and foreign audiences. The *38th Commandant's Planning Guidance* states,

> I will continue to advocate for the continued forward deployment of our forces globally to compete against the malign activities of China, Russia, Iran and their proxies—with a prioritized focus on China's One Belt, One Road Initiatives.[8]

Forward deployed units conducting operations, exercises, and investments compete in the IE by *informing foreign and domestic audiences* of U.S. presence and engagement. An aggressive forward posture delivers positive force-ratio contributions to the joint force.

> The Marine Corps defines inform foreign and domestic audiences as "actions taken to truthfully communicate with domestic and foreign audiences in order to build understanding and support for operational and institutional objectives.[9]

This information function seeks to assure regional partners and allies while deterring and dissuading adversaries. Informing foreign and domestic audiences enhances the ability of forward

The refrain "train, train, and train some more" will be heard repeatedly. *(Photo by LCpl Isaac Velasco.)*

deployed MAGTFs to synchronize effectively in coordination with interagency partners in order to expose PRC propaganda and misinformation. The end state of such an approach is to ensure the United States emerges as the key partner of choice while undermining PRC malign influence.

Intelligence support to campaigning through cooperation: Inform and influence domestic and foreign audiences. Intelligence support begins as it always has—with a constantly evolving intelligence preparation of the battlespace (IPB) product. The IPB, however, must be relevant across the full continuum and encompassing of the seven functions of OIE. Opposed to focusing solely on military capabilities, IPB support to the IE integrates evolving subjective concepts of projecting and protecting state power. Intelligence support to cooperation in the competition continuum is not solely adversary focused, otherwise stresses the needs of individual partner nations. Those "on the fence" actors who require persuading to side with the United States in this enduring competition for access and influence. Proper intelligence support includes a detailed understanding of host nation current capabilities, perceived threats, and desired growth. The IPB articulates both objective and subjective notions of third-party interests, as well as U.S. policy vis-à-vis the country and the region. It is in this realm where intelligence support frames future operations not only by explaining the actions of the competitor (in this case PRC) but also identifying impacts on the target nation. Enhanced cooperation with U.S. Embassy country teams facilitates access to detailed databases of U.S. programs, weapons sales, and security assistance. From this foundation, unified and recommended talking points based on projected impact on targeted audiences are created. Good intelligence work can even micro-target based on population clusters and nuance interpretations of interests.

Good intelligence work can even micro-target based on population clusters and nuance interpretations of interests.

Campaigning Through Competition Below Armed Conflict

Case Study: Iranian gray zone operations in the Middle East and beyond. The *Twilight War* between the United States and Iran that began in 1979 is a powerful example of enduring competition below armed conflict.[10] Iran uses its geopolitical influence as a regional hegemon in the information domain to counter the United States but not merit a harsh response. A contemporary example is Iran's response to the U.S. unilateral withdrawal from the Joint Comprehensive Plan of Action. In May of 2019, Iran used asymmetric capabilities to mine four commercial ships off the coast of Fujairah. In September of the same year, Iran employed drones to attack two major oil installations in the Kingdom of Saudi Arabia. Both of these escalatory actions orchestrated by the Islamic Revolutionary Guard Corps occurred without triggering an armed conflict against the Iranian Regime. All the while, the Islamic Republic continued to fund and modernize its robust ballistic missile arsenal.[12] In the gray zone fight, Iran uses religious fundamentalism, terrorism, plausible deniability attacks, surrogates, proxy networks, and malign activities to compete against the United States, its partners, and allies below the threshold of conflict.

OIE Response in support to competition below armed conflict: Increase IE battlespace situational awareness. As gray zone operations occur throughout the battlespace, a primary task in the information environment should be governed by the information function IE battlespace situational awareness.

Competition below armed conflict tends to occur over extended periods of time. In comparison to armed conflict, actions are often more indirect and the expenditure of resources less intense, thus allowing for a more protracted effort.[11]

This information function is designed to provide

> information flows that comprise the IE running estimate integrating intelligence and other information which characterize the physical, informational, and cognitive dimensions of the information environment in order to identify threats, vulnerabilities, and opportunities.[13]

The running estimate is a visualization and decision-making tool for sensing and making sense of the noise floor in a gray zone fight: critical to ensuring a faster, more accurate, and efficient decision-making cycle for the Commander. By maintaining a keen edge on IE battlespace situational awareness, the MAGTF commander is able to maintain multi-domain awareness, understand the threat space, and manage risks while exploiting opportunities against adversarial critical vulnerabilities across all domains. This function leverages disruptive technologies, namely: artificial intelligence, machine learning, and other high-end computing algorithms to predict threats, vulnerabilities, and opportunities in the information environment.

Intelligence support to competition below armed conflict: Increase IE battlespace situational awareness. Gray zone activities that leverage proxies, exercise diplomacy, coerce economically, interfere electronically, and control resources all while remaining deniable serve a difficult challenge for the intelligence community. Identifying and describing the battlespace to increase clarity for the commander regarding the scope of adversarial actions traditionally begins during step one of the IPB process, *define the battlespace environment*. Intel support to battlespace awareness in the competition continuum is fundamentally unchanged, albeit more complex. As enemy activities remain below the threshold of armed conflict, indicators of enemy presence and actions are less distinct. Successful intelligence efforts identify key indicators of enemy activities below armed conflict through a targeted collection plan focusing on adversarial public statements, financial support to proxy groups, trade negotiations to garner favor with partners, activities in cyber space, and attempts to influence a broader public narrative. Such a collection effort maintains multi-domain awareness of confrontational actions and provides the commander a broad appreciation of the battlespace to consider a range of responses and force protection measures.

Rarely do wars end with a complete end of armed conflict. Wars disrupt political, social, and economic structures, networks, and institutions to the point it is often impossible to simply return to a pre-conflict state.[14]

Campaigning Through Armed Conflict

Case Study: Russian Federation in the Ukraine. Russian aggression in Georgia and Ukraine over the past dozen years has changed global borders and displaced hundreds of thousands. Unified employment of information capabilities had effects at the strategic, operational, and tactical levels of each effort. In August 2014, Russian conventional and unconventional troops surged into southeast Ukraine in the name of a "humanitarian convoy" to protect ethnic Russians. Since then, Russian forces have employed a highly sophisticated cocktail of cyber and electronic warfare capabilities to gain effects at the tactical level.[15] The employment of tactical-level information operations include well-timed jamming of counter battery radars, intercepted communications, disrupted command and control nodes, electronic targeting of Ukrainian positions, spoofed GPS receivers, hacked personal cell phones, and even sending individualized and personalized text messages to shocked front line troops. This tactical employment of information warfare proves highly effective and is an example of how our Nation's adversaries are successfully integrating information as part of a combined arms effort.[16]

OIE response during armed conflict: Attack and exploit network systems and information. In an armed conflict against a peer competitor, the MAGTF will prioritize the information function of *conduct attack and exploit adversaries' networks systems*. The Marine Corps defines this information function as

> those actions conducted to exploit or attack enemy networks systems, signatures and information in order to create advantage for the MAGTF ... This function also includes non-lethal actions occurring in and through the information environment as well as fires and maneuver.[17]

Using the attack and exploit network systems and information function is effective when force ratios and relative combat power assessments disfavor

friendly forces during the onset of combat operations. Furthermore, as highly networked opposition forces disperse across a broad front of battlespace, employing information-related capabilities across multiple domains to include electromagnetic spectrum and cyber isolates and fixes the enemy. By employing this information function, the ability to dislodge, degrade, or destroy enemy forces in detail is greatly enhanced.

Intelligence support during armed conflict: Attack and exploit network systems and information. Intelligence support during armed conflict provides clarity on how to get to, and persist, inside the enemy engagement area. Armed conflict in the information contested environment recognizes that to be sensed is to be targeted. Alternatively, to sense the enemy is to enable targeting. What this means is that good intelligence support to attacking and exploiting enemy network systems and information is twofold. First, the identification of enemy networks and systems is identified and expanded upon during the IPB process. Understanding the enemy's ability to sense through electronic and other technical means supports force protection efforts in the information domain. Detailed network analysis identifies critical vulnerabilities in the system, which leads to coverage gaps as specific enemy assets are identified.

Secondly, persisting inside the enemy's engagement zone means effectively fighting back. A tireless intelligence, surveillance, and reconnaissance effort to locate enemy networks that lead to command and control, collections capabilities, and weapons systems feeds the targeting effort. Locating and remaining in contact with these systems demands modern sensing capabilities and an adept decentralized effort to fully exploit and disseminate all that is collected. Although intelligence support to OIE during armed conflict spans all warfighting domains and functions, it is still rooted in the basics of good intelligence work.

This article offers tactical insight on operations in the information environment and required intelligence support using the competition continuum as a framing device. Admittedly, it is limited in scope and does not address all seven functions of OIE. Otherwise, the brief examples of adversary activities in each stage of the competition continuum and how responses in the IE can produce concrete effects highlights how the integration of information related capabilities into a combined arms effort cannot be delayed.

... naval sea power is tightly linked to a nation's overseas commerce and economic well-being.

As stated at the outset, naval sea power is tightly linked to a nation's overseas commerce and economic well-being. America's founding documents identified this key relationship. In 1890, Alfred Thayer Mahan published the most influential book on naval strategy, entitled *The Influence of Sea Power Upon History 1660–1783*.[18] This seminal publication detailed the introductory elements required to achieve sea power and enable power projection. *Based on its omnipotence, information power is the new sea power*. As the resurgence of great power competition defines the 21st century security environment, what will be the influence of information power upon our history? How will the MAGTF posture and operate across the competition continuum to shape that history?

Notes

1. Alexander Hamilton, "The Utility of the Union in Respect to Commercial Relations and a Navy," *The Federalist Papers*, (London, UK: Phoenix Press Paperback, 2000), available at https://avalon.law.yale.edu.

2. Robert Strassler ed, *The Landmark Thucydides: A Comprehensive Guide to the Peloponnesian War*, (Free Press, Touchstone edition, 1998).

3. Joint Chiefs of Staff, *Joint Doctrine Note 1-19 (JDN 1-19): Competition Continuum*, (Washington, DC: June 2019).

4. Ibid.

5. Deputy Commandant for Information, "Functions of IE Operations," (Washington, DC), available at https://www.candp.marines.mil.

6. *JDN 1-19*.

7. Scott Kennedy, "Building China's One Belt, One Road," Center for Strategic and International Studies, (Washington, DC: April 2015), available at https://www.csis.org.

8. Gen David H. Berger, *38th Commandants Planning Guidance*, (Washington, DC: July 2019),

9. "Functions of IE Operations."

10. David Crist, *The Twilight War, The Secret History of America's Thirty-Year Conflict with Iran*, (New York, NY: Penguin Books, July 2013).

11. *JDN 1-19*.

12. Defense Intelligence Agency, "Iran Military Power: Ensuring Regime Survival and Securing Regional Dominance," (Washington, DC: 2019).

13. "Functions of IE Operations."

14. *JDN 1-19*.

15. Defense Intelligence Agency, "Russia Military Power: Building a Military to Support Great Power Aspirations," (Washington, DC: 2017).

16. Joseph Trevithick, "Ukrainian Officer Details Russian Electronic Warfare Tactics Including Radio Virus," *The Drive*, (October, 2019), available at https://www.thedrive.com.

17. "Functions of IE Operations."

18. Alfred Thayer Mahan, *The Influence of Sea Power Upon History 1660–1783*, (Boston, MA: Little Brown and Company, 1925).