The Seventh Warfighting Function

Information

by Capt Corey Klonowski

The year is 2031, and the United States is currently at the height of a great power competition with three countries around the world. The Navy and Marine Corps team is in the tenth year since implementing their expeditionary advanced based (EAB) operations. The Marine littoral regiment commander just received from higher headquarters a warning order to conduct an amphibious raid in a location within a contested area in order to establish both a sensor and fires EAB to act as a deterrent to approaching enemy naval forces. In consolidating his staff to implement the rapid response planning process (R2P2), the commander orders his S2 and S3 to incorporate the warfighting function information to shape the conditions in the landing forces favor. Drawing from the experiences gained in previous training exercises, the deuce, operations, and other supporting elements work tirelessly to identify the physical networks and dynamics of the population in order to incorporate the information in the intelligence preparation of the battlespace.

Upon landing, Littoral Combat Team 3 discovers the local populace is largely resistant to the presence of the Marines out of fear of their livelihoods becoming collateral damage. Despite numerous outreach attempts by the senior leadership of Littoral Combat Team 3, the establishment of the sensor and fires EAB's are immediately compromised as information of the Marines' presence quickly spreads through media lines and through word of mouth in the number of subcultures that exist on this particular place. Additionally, having been alerted of the Marines' presence through open-source intelligence, the enemy naval forces altered their trajectory and maneuvered around allied forces. Despite the regimental staff's best efforts to understand and impact the information environment through physical means based on the assumptions that were identified in the planning process, they were largely powerless to execute a serious information campaign with the available resources at the tactical level.

>Capt Klonowski is an 0202 Intelligence Officer. He is currently serving as the SIOC Course Director, Marine Detachment Dam Neck in Virginia Beach.

The information warfighting function is the intellectual organization of three abilities required for the application of informational power: Understanding how information impacts behavior, leveraging information to affect behavior, and facilitating shared understanding to support human and automated decision making.[1] Yet, while *information* is still relatively new to our doctrine, it is the assertion the Marine Corps does not delineate information as both a domain and a warfighting function and should be put on equal footing with other warfighting functions in order to shape the battlespace for 21st century warfare. This assertion is reinforced alone by the current absence of an information staff officer located on battalion and regimental staffs that serves in the same capacity as other staff members with their respected warfighting functions.

To successfully incorporate information as a warfighting function, Marine leaders on all levels need to better understand the information domain or how information flows in a metaphysical realm. The DOD Command and Control Research has identified and developed a model with three distinct but closely interconnected domains—physical, information, and cognitive.[2] While Marines thrive in the physical domain, I argue our inability to operate in the cognitive domain impedes our ability to leverage human behavior to our advantage. Imagine if a commander had an information staff member who, through close coordination with the national community, utilized a non-kinetic means to target the information domain that affected the moral consciousness of the local population—consequently changing the outcome of an operation.

We need to immediately address how we can realistically operate in the information environment at the tactical level across the information domain. Having a detailed understanding of our authorities is imperative because using information to alter the cognitive state of a group of individuals is accomplished through non-kinetic means with the real likelihood of garnering that information to incorporate kinetic fires. This reinforces the need for the creation of an information's staff member in battalion and regimental staffs, in addition to establishing an in-depth training pipeline with the joint and national community. In addressing this, serious questions need to be asked regarding whether battlefield commanders are also maximizing the current organic

capabilities that are required to inform the intelligence cycle. Further, are we cognizant enough of ongoing efforts by foreign and domestic actors who are effectively using information operations in open conflict in a manner we currently would view as incomprehensible and against our rules of engagement?

In order to answer the two earlier questions, we need to distinguish between offensive and defensive information operations. In recent years because of conflicts in Crimea and Georgia, we developed an appreciation of Russia's ability to shape the battlefield in their favor by effectively incorporating offensive information operations. With a more in depth look into Russia's tactics, techniques, and procedures, we now know how Russia integrated technologies from UAS platforms coupled with electronic warfare, signals intelligence, and cyber capabilities to wage an information campaign against the Ukrainians. Figures 1 and 2 depict Russia's techniques at the tactical level in finding, fixing, and incorporating information as a warfighting function to finish the enemy, achieving a desired result on the enemy within twenty minutes.[3] Employing information warfare in this case study can only be achieved through rehearsals, which begs the question as to whether we as an organization are appropriately implementing information in the planning process as we do with the other warfighting functions.

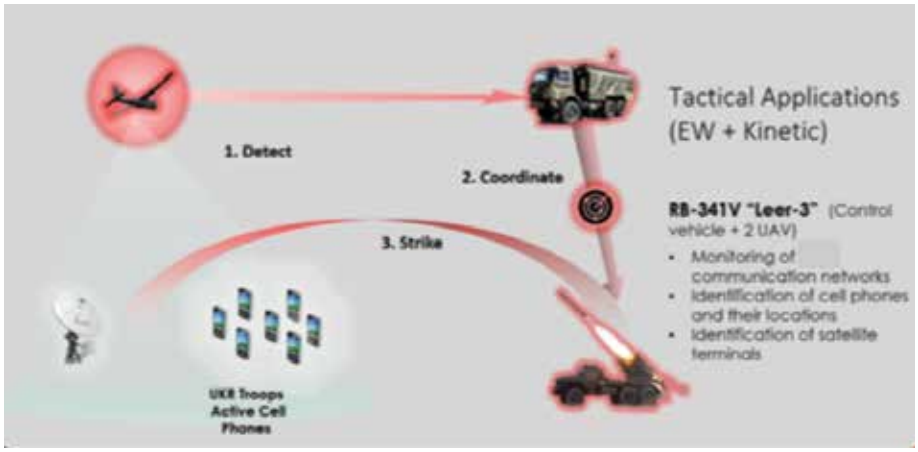

Figure 1. *(Figure provided by author.)*

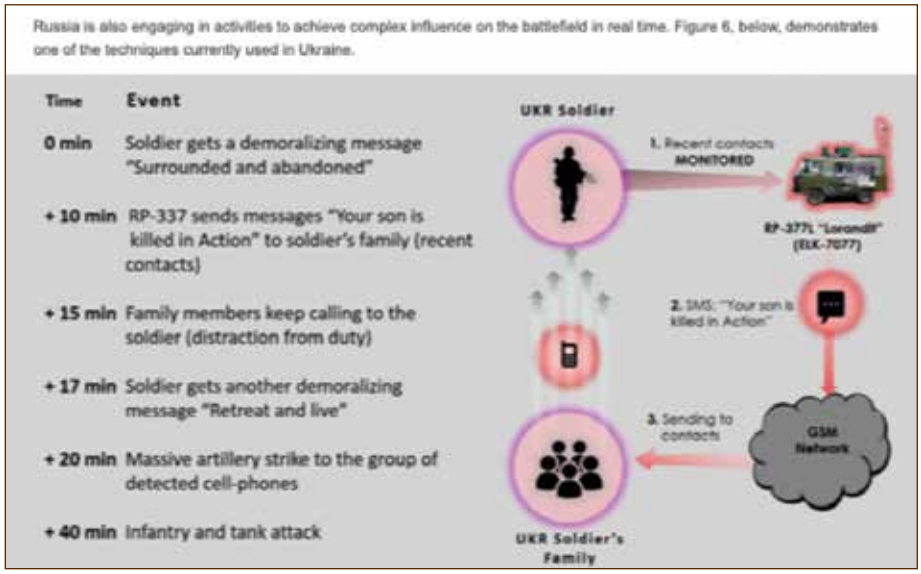

Figure 2. *(Figure provided by author.)*

small change, yet it is imperative for us to leverage organic and joint-level capabilities that gather and disseminate information at longer ranges of operations.

In a sharp contrast to one of our peer adversaries, I argue that the Marine Corps is lethargic on treating information as an actual warfighting function. We discuss operating in the information environment as a philosophical concept but fail to synchronize the other warfighting functions required to support an information campaign, none more so than intelligence and C2. In the absence of an information staff officer, the only units that are currently tasked organized with multiple intelligence disciplines equipped to analyze information are MEUs, whose area of responsibility is enormous given their broad areas of interest while afloat, and Marine Forces Special Operations Command's Direct Support Teams (DST). The DST is by far the most ideal task organized unit given their integration of intelligence disciplines at the start of their training cycle and the quality of the training environment that effectively tests their ability to operate as a true intelligence cell.

In 2017, the 37th Commandant, Gen Robert Neller, recognized this as a major weakness and took steps by reorganizing each MEF Headquarters Group's to the MEF Information Group to specifically address improving our readiness in information warfare.[4] As

part of this new focus, radio battalion's underwent two critical changes with the creation of electronic warfare platoons and mandating in their mission statement to conduct "limited cyberspace operations." While I argue we took steps in the right direction, serious flaws continue to exist in the task organization and our inability to bridge the other intelligence functions that are necessary for a successful offensive information campaign. Further, our training environments are largely designed to find, fix, and finish the enemy on simplistic communication capabilities, which has largely shaped how today's ground commanders seek to employ singular capabilities like electronic warfare.

Over the course of multiple training exercises with ground units, an apparent theme became apparent as units were learning how to integrate ground electronic warfare capabilities. While the electronic warfare platoons are admirable in the advancements of our understanding of electronic warfare, the candid assessment is that this capability is a simplistic approach to acquiring and jamming frequencies at a reduced range. I am not dismissing the importance of ground electronic warfare as a capability we need in our arsenal; rather, our training should also be directed at consolidating the different intelligence disciplines to produce information from both simple and complex technological infrastructures that, in turn, can also be used for offensive and defensive purposes. Further, the Marine Corps needs to develop a realistic foundation as to how cyber operations will be managed and executed at the tactical level. This should include a training pipeline, providing the tools and resources at the tactical level, and identify the parameters of the cyber authorities. By addressing these issues, commanders will be better armed with the attributes of an information campaign.

The Marine Corps needs to take dramatic approaches to incorporate offensive operations in the information environment among all three levels of war. To succeed, I argue this starts with the intelligence cycle, where information is collected and eventually produced as an intelligence product that feeds a commander's decision. As mentioned above, training environments must be compatible in order to support multiple disciplines of intelligence. To this day, the revered Integrated Training Exercise still lacks a signals environment and script for a signals intelligence platoon to operate. We need to integrate early and often across the different intelligence disciplines to work collect, analyze, and publish accurate reports during training evolutions to develop understandings of the informational, physical, and cognitive aspects in a simulated battlespace.

The Marine Corps needs to take dramatic approaches to incorporate offensive operations in the information environment among all three levels of war.

To put this in better context, we need to have a better understanding of the technological advances in cellular technologies around the world and how people access their information. In 2020, 3.81 billion people used social media with a shocking 98.68 percent of this demographic reporting they have access to websites or apps through a mobile device. This has nearly doubled in five years as companies like Facebook (2.6 billion users), YouTube (2 billion users), and WhatsApp (1.6 billion users) have reached populations in every country, with notable exceptions to countries like Iran, Syria, and North Korea.[5] The Marine Corps needs to adapt to the ever-changing landscape of technological advances if we are going to achieve a strategy that impacts human behavior to our advantage. This requires a change to our approach on how we are incorporating information warfare in the planning process by specifically addressing how we are reaching demographics that have access to advanced technologies.

To achieve this, ground commanders and their supporting staff sections need to be more integrated at the national and strategic levels than ever before, well before the first Marines are inserted into contested areas. In order to understand and define the battlefield environment, the intelligence preparation of battlefields need to factor in the technologies that are prevalent and how the demographics receive information and over what services. In turn, close coordination is required with the national entities to obtain the methods at the tactical level to conduct successful offensive information operations. We already have some of this infrastructure in place as radio battalions are presently designed to conduct higher level coordination with the national intelligence community. But this will be insufficient when detachments from radio battalions typically are designated under different command relationships, and these detachments are operating in forward contested environments. This eventuality could be offset by organizing the intelligence disciplines into a DST-like element and/or an information staff officer that is capable of conducting national-level coordination as it relates to their specific operational environment.

Given the enormity of the task of reaching targeted populations in an information campaign, the Marine Corps needs to think boldly in fielding the appropriate technologies and synchronizing the force with the joint and national community. It is an understatement that if my proposal on fielding teams fused with the different intelligence disciplines were to go into effect, the intelligence team would be overwhelmed with the task of coordinating an information campaign, not to mention their more traditional duties of focusing on the enemy. *MCDP 1, Warfighting*, references the hierarchy of the three levels of war, specifically how the tactical level includes the *technical* application of combat power.[6] My assumption is when *Warfighting* was modified by Gen Krulak in 1997, employing cyber capabilities or using organic technical intelligence gather-

ing capabilities to influence targeted populations in the potential billions was not even a factor at the time. Further, if our tactics and techniques are supposed to overlap, what exactly are our tactics and authorities in employing capabilities such as cyber operations at the tactical level?

Significant overlap of the three levels of war need to occur for this type of campaign to be carried out successfully. Our success is dependent on our efforts to coordinate with the joint community to harness information collection capabilities when operating in the same battlespace. The complexities in this kind of coordination on the information flow cannot be underestimated, especially in a denied or degraded communications environment. Only multiple opportunities in adequate training environments can reduce the friction in joint-level operations at the tactical level. In addition, serious investments in program-of-record gear that is smaller with fewer SL-3 components are necessary in disaggregated environments, which will require smaller physical and signature footprints. The Marine Corps also needs to expand investment in automation for computer programs that will reduce the amount of hours of analytics and delivery of information required in a massive information campaign. Not only will this be necessary for offensive information operations but for defense as well.

We as an organization need to focus on defensive information operations, probably more so than for offensive purposes. Due largely in part to our cherished freedoms, our military is more susceptible in garrison and competition to misinformation campaigns which occur regularly due to this generation's social media and technology dependence. A lot of attention in today's political climate in America is centered on false news. In a study published by the Massachusetts Institute of Technology Sloan School, the authors discovered falsehoods are 70 percent more likely to be retweeted on Twitter than the truth and reach their first 1,500 people six times faster.[7] Our adversaries target specific demographics who in turn willingly or unwillingly help spread information that draws divisions in our society. The military is not exempt from this, which seriously threatens C2 and a unified force to achieve our objectives. We need realistic procedures in place to address and identify to all paygrades of the military when a country with no moral authority employs sophisticated methods of information operations by targeting the emotions of an individual.

In order to deter misinformation from infiltrating and dividing our forces, we need to identify the means on which that information is delivered. I was encouraged by the administrative message recently published addressing the use of technologies with geo-location capabilities. One handset by an unwilling participant can expose an entire unit, which has second and third order effects to the strategic success of a mission. In a successful information campaign, defensive-minded commanders need to think beyond the content and understand the metadata that could expose his or her force via cyberattacks or by other means. Our first impulse is to look at our internal communication methods over single channel radios. Yet while this is one aspect and something we absolutely need to pay attention to, we need to re-approach everything that encompasses the entire infrastructure and networks required to run combat operation centers and subsequently our ground tactics.

Our critical vulnerability in understanding the application of information in the operating environment ...

Our critical vulnerability in understanding the application of information in the operating environment is the successes the Marine Corps has enjoyed in fighting a counter-terrorism fight. I mentioned earlier we are good at operating in the physical domain, such as providing security, money, and resources to a local populace in an attempt to win their "hearts and minds." In an ever-changing technological landscape, our credibility as an organization will be determined on how we adapt to the technologies from both an offensive and defensive mindset, in addition to our ability to serve as forward sensors in contested areas that feed information as part of the larger joint strategy. These are issues that need to be addressed immediately, as our ability to levy a successful information campaign will allow the Marine Corps to shape the battlefield in our favor.

Notes

1. Expeditionary Warfare School Distance Education Program, *The Information Environment*, Academic Year 2021, Functional Employment of the MAGTF Coursebook and Readings.

2. Robert Cordray III and Maj Marc Romanych, "Mapping the Information Environment," (Fort Sam Houston, TX: Joint Information Operations Center, 2005).

3. *The Information Environment.*

4. I MEF Expeditionary Force, *Marine Corps Creates First Information Group to Prepare for Modern Battlefield*, (July 2017), available at https://www.imef.marines.mil.

5. Brian Dean, "Social Network Usage & Growth Statistics: How Many People Use Social Media in 2020," *Backlinko,* (August 2020), available at https://backlinko.com.

6. Headquarters Marine Corps, *MCDP 1, Warfighting*, (Washington, DC: 1997).

7. Soroush Vosoughi, Deb Ro, and Sinan Aral, "The Spread of True and False News Online," (Cambridge, MA: MIT Initiative of the Digital Economy, March 2018).