Operations in the Information Environment

Application of the direct and indirect approach for

by LtCol C. Travis Reese, USMC(Ret)

>LtCol Reese retired in 2016 after nearly 21 years of service as an Artillery Officer, MAGTF Planner, and Foreign Military Advisor. Upon retirement he became a strategy consultant. He is currently a Plans and Strategy Analyst for the Deputy Commandant for Information, Plans and Strategy Division.

The Marine Corps' establishment of information as a warfighting function highlights the need to comprehend military operations differently and confirms the requirement to gain and maintain an information advantage in conflict. Conducting operations in the information environment (OIE) to implement the information warfighting function does not require radical alteration to the art and science of warfare. Rather, it is entirely backward compatible with established principles, the modern iteration of which simply requires re-imagining the role of information in conflict. One principle that helps illustrate how information capabilities can be employed against an adversary is in the application of the direct or indirect approach.[1]

For this article, we will use the framework of the competition continuum applied in the *Joint Concept for Integrated Campaigning*. Competition and war are discriminated as conditions that exist above and below the threshold of traditional armed conflict.[2] Throughout this article competition and war will be referred to generically as "conflict" for ease of reference with the full knowledge that each condition has a different application of means depending on the desire to deter or defeat threats, balance conflict escalation, and achieve a strategic goal or outcome.

Historically, information capabilities have been considered asymmetric in their utility and introduced via an indirect approach.[3] Information capabilities, whether narrative or electromagnetic, have principally played a supporting role to other lethal systems as the primary tools of decisive engagement in conflict. Because of the increased use of electronic information systems vital to the employment of military forces and the operation of military capabilities in the "Information Age,"[4] OIE can now be direct and symmetric on par with the physical maneuvering of forces and the employment of explosive or kinetic munitions. Information capabilities can be applied to all domains and military activities in both competition and war. Therefore, information means increase the number of opportunities and avenues of approach to confront an adversary and can contribute as a primary defeat mechanism equivalent to, and complementary with, other physical systems. Information means, in short, provide a greater number of vectors of attack against an adversary either directly or indirectly across the conflict continuum. Rather than speak conceptually, this article will identify, in practical terms, how to maximize the benefit of information capabilities to achieve both an information and overall advantage in conflict.

Foundations

Grasping a new activity or capability in warfighting can be difficult because new tools require learning and practice. For example, adding the air domain to the repertoire of land and sea conflict took time to master and become inherent in operations. This was especially true as the rapid trajectory of aircraft development caused divergent philosophies about how best to employ planes to achieve campaign objectives.[5] Further, the debates about whether aircraft were ancillary or decisive in the conduct of war shifted as aerial-enabled combat transitioned to more routinized operations with increasingly robust means. It did not help that as the larger military was learning to integrate air forces as a matter of necessity, the community of air operations advocates was involved in robust debates about the definitions of airpower, the possibilities of airpower, and the best application of airpower. The internal divisions of air philosophies and philosophers continued through the 1990s when some advocates claimed that air power could preclude the need for ground operations and bring a decisive end to a conflict.[6]

Like the rise of airpower, every competitor or adversary (state and non-state) has developed both narrative and electromagnetic information capabilities.[7] They are actively applying these capabilities with sophistication and rapidity

guided by a more agile and experimental mindset often with little prohibition or regard to larger consequences. We, on the other hand, are wrestling with our incomplete doctrinal conclusions of how to employ them in our forces and struggle to bring them into the mainstream of operations.[8] Just as with early airpower advocates, there are challenging claims regarding the potential effects that can emerge from operations in the information environment in the conduct of conflict.[9]

Information effects are hard to model because they are focused on adversary decision making or they are produced with means that reside in layers of classification that make their contribution to military operations relatively unknown to those without the most elevated clearances and need to know.[10] Additionally, information capabilities encompass multiple disciplines, many of which once stood alone but are now collected under the information umbrella. Activities like influence operations, inform operations, electromagnetic spectrum operations, intelligence (which has its own warfighting function too), make the amorphous concept of information subject to numerous caveats and qualifications among the various communities. Information has an environment which encompasses these disciplines and, like the air domain, includes numerous forms of aviation and support activities, so too does information.

A technique that makes learning and application of a new idea easier is to determine if a new tool or concept can be applied to old principles. On that basis, one can assess if a thing changes either the nature or character of an observed phenomenon. If the phenomenon of war is identified as a violent conflict of wills,[11] and the application of information tools does not alter that violent upheaval, then the nature of war has not been changed. If adding information actions and means changes the *range of activities* that we include in conflict and has a demonstrable effect (either qualitative or quantitative), then we can safely say the character of war has changed. Ultimately, the question a Marine commander must answer is if information functions and capabilities can be introduced into the tool kit for waging conflict according to known principles of the military practice?

To answer that question, we need to have a working definition of the information environment, and the warfighting function of information. The information environment (IE) is defined as the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information.[12] While it is not a warfighting domain, it is a space that facilitates maneuver through the established domains of land, air, maritime, space, and cyberspace. In this case, information is a noun. The function of information is performed to generate, preserve, deny, or project information to increase our advantage over the enemy.[13] In this sense, information is a verb.

In the Information Age, the concept of combat power has changed to a more inclusive definition of military power. Combat power is the total destructive force we can bring to bear on our enemy at a given time.[14] We project combat power in conflict through military instruments and regulate their use depending upon military necessity and the demands of proportionality. We also think about combat power in terms of its effects to deny, degrade, disrupt, limit, divert, etc., with accompanying operations to achieve those effects. Military information power is the total means of force or information capability we can apply against a competitor, adversary, or enemy to enhance our lethality, survivability, mobility, or influence.[15] The essence of military information power is the ability to exert one's will or influence over an opponent through the generation, preservation, denial, or projection of information. Military information power, like traditional combat power, is governed in its application by military necessity and proportionality since we are using at as an element of military force. Those principles of necessity and proportionality mean that information power elements have equivalent considerations in their use to traditional physical elements of combat power. Thus, combat power and military information power are components of overall military power able to provide effects in the relevant portion of the operating environment whether physical or informational. (See Figure 1.)

Figure 1. The relationship of combat power and military informational power to military power. *(Figure provided by author.)*

With these definitions, we now have the means to compare OIE to the first principles of our warfighting doctrine. If we can conduct OIE using the same timeless principles found in *MCDP 1, Warfighting*, that will enable synergy with other means applied against the same framework. In order to apply the capabilities of information to a direct or indirect approach in conflict, there are some inter-related concepts from *Warfighting* that must be understood. For each one of those concepts we must update our understanding of how information capabilities contribute to each element of our warfighting principles described in doctrine. As we update these principles to include information, we will be on our way to integrating the information warfighting function more completely in our conflict methodology.

Attrition and Maneuver

In conflict there are two principle ways that decisive outcomes can be achieved: attrition or maneuver. Attri-

tion warfare is defined as the pursuit of victory "through the cumulative destruction of the enemy's material assets by superior firepower."[16] Maneuver warfare is defined as a "series of rapid, focused, and unexpected attacks designed to shatter the enemy's cohesion."[17] Maneuver warfare has elements of attrition but is not focused on that as an outcome. Attrition that contributes to collapsing the adversary system in ways that cause them to fail to cope with the decision cycle is the complementary use of attrition to perform maneuver warfare.[18] Maneuver warfare is classically characterized as a conflict practice that positions forces and means by avoiding sources of strength and exploiting adversary gaps and seams. The indirect nature of maneuver warfare, as opposed to the direct nature of attrition warfare, will be discussed later. It is important to highlight that the term "maneuver" generically refers to the positioning of forces or means,[19] which is distinct from the term maneuver warfare as described above.

Information capabilities maneuver in ways that are both virtual or physical which opens more possibilities for the execution of maneuver or attrition warfare. Maneuver, through cyberspace both for cyber payloads or narrative products, is more virtual whereas other electromagnetic spectrum-enabled maneuvers, although not visible, are very physical. Physical electromagnetic maneuver has limitations, such as power and range, which must be taken into account like the employment of any weapons system. Similarly, virtual maneuver among target populations via a narrative emplaced either in military communications to influence or civil/social communications to inform is vital to commanders who want to maneuver with information in specific ways. The virtual maneuver of a narrative may be hard to quantify in terms of its overall energy on the operating environment and effect on the cognition of the chosen audience but, as we shall see, it is certainly a way we project military power. Whether we employ virtual or physical maneuver to emplace narratives products or electromagnetic means, these capabilities can be placed directly and attributably in front of an adversary or enter through a gap or seam indirectly and in some instances be unattributable to us or our partners. The point is that information capabilities can facilitate maneuver warfare and attrition warfare practices and produce maneuver and attrition effects. Because of the virtual and physical aspects of information maneuver, it is important to ensure that "conflict space" is not characterized myopically to physical "battlespace" as we think about how to incorporate OIE into maneuver or attrition warfare applications.

Engagement of a target either through attrition or maneuver also devolves to a choice between lethal or non-lethal effects through physical and non-physical means. To understand the proper potential of information to project the kind of power that facilitates attrition, it is necessary to take a brief excursion to define lethal and non-lethal. Lethal is defined as "of, relating to, or causing death" or "gravely damaging or destructive."[20] Non-lethal is defined as:

> Weapons, devices, and munitions that are explicitly designed and primarily employed to incapacitate targeted personnel or materiel immediately, while minimizing fatalities, permanent injury to personnel, and undesired damage to property in the target area or environment. Non-lethal weapons (NLW) are intended to have reversible effects on personnel and materiel.[21]

Frequently, the inaccurate shorthand of "kinetic" is applied for lethal and physical and "non-kinetic" for non-lethal and non-physical. To illuminate the inaccuracy of those terms as they apply to military means here is an example: A slap in the face is a kinetic event using the release of stored energy in a physical entity (the pulled back hand) which is also non-lethal in effect. We must eliminate the imprecise use of the term kinetic from our lexicon when we mean lethal and non-kinetic when we mean non-lethal if we are going to appropriately synergize information-based tools with more traditional military capabilities. It is entirely possible in information capability-enabled approaches to deliver a lethal effect with a non-physical delivery mechanism.

Attrition is the elimination of an adversary's means as a straightforward test of strength and a matter of force ratios.[22] However, what is achieved is immaterial to means that produce that outcome. For example, if an adversary relies on a particular network of sensors to conduct their operations and we assess that it is critical to disrupt the network for our operations to succeed, whether we bring it down via a directed energy system, cyber-delivered payload, or missile engagement, it is still an attritive outcome. Attrition, then, is no longer a function of classical firepower as the definition insists but is a function of any power on a target that generates a destructive force. In this way we see a change to the character of conflict.

Information, as a source of power, can be applied to achieve attritive effects whether that is in support of maneuver or attrition warfare methods. The idea that a tool which uses kinetic energy to achieve its effect is more "powerful" and therefore more decisive in conflict during this Information Age is an artifact of Industrial Age thinking and that must be reconsidered in the modern era. The combination of military information power with combat power to create overall military power means that information power can be applied, as our examples show, in the same ways that combat power has been for generations and that physical battlespace alone does not account for entirety of conflict space or the associated maneuver options.

Symmetric and Asymmetric Means

The evolution of war consists of measure, countermeasures, and countercountermeasures. It is a constant pattern of symmetry and asymmetry. Symmetry is defined as two powers having comparable military power and resources. They rely on tactics and means that are similar differing only in details and execution. Asymmetry is the instance in which the resources of two belligerents differ in essence, and, in the interactive struggle, they attempt to exploit each other's characteristic weakness.[23]

As an example of symmetry of means, Carl Philipp Gottfried von Clausewitz described the Napoleonic aim of war as seeking the enemy's

army as the objective and defeating it through decisive battle or a battle of annihilation with one's own army.[24] Conversely, John Boyd, in his reading of Sun Tzu, J.F.C. Fuller, and many others, asserted asymmetry of means is achieved by choosing maneuvers that gain mental and positional advantage. Focusing on maneuver, according to the theories of Boyd, are ultimately the superior options in conflict since they incapacitate an adversary's decision making through shock and disruption. Maneuvers achieve asymmetry because they exploit a relative weakness in the enemy by placing a relative strength against it in a way that an adversary cannot compensate and causes the adversary system to collapse.[25]

As noted in the introduction, there was a time when information was considered primarily an asymmetric means to facilitate other lethal engagements that were considered more decisive. Past applications of propaganda, deception, electronic attack against radars and communications were all means to deny or project information for the purpose of facilitating delivery of lethal munitions or the maneuver of forces to emplace firepower. In the end, the application of information capabilities allowed us and our adversaries to confront each other with the symmetry of other means (tank vs tank, ship vs ship, etc.) that were considered more vital to the success of armies and navies.

To get a better sense of this, let us consider an example of information integration with a mechanical capability. At one point in time, the weaving of cloth was an interaction between weaver and loom. A human operator manipulating mechanical inputs on the loom produced the cloth. The output and activity of weaving could be eliminated in one of two ways: 1) destroy the loom or 2) maim or destroy the weaver. With the development of the Jacquard Loom in 1801,[26] fully automated and programmable weaving was introduced by encoding the pattern of the weave on a series of paper punch cards. The loom no longer functioned exclusively through direct mechanical input from the weaver but required an information interface from the punch cards. The weaver still possessed the knowledge of weaving, but the action to manipulate the loom depended on the information "stored" on the cards. Punch cards gave information to a mechanical object to automate a system once controlled by human input. In an OIE context, if the punch cards were destroyed, then the system would not operate until cards were replaced since the source of directed command was removed. Or, if the information on the cards were sabotaged—corrupting the information through an inaccurate input—the weaver would lose confidence in using the Jacquard system thus eliminating the ability to coordinate the function of the system. Finally, the loom or the operator could be destroyed, and the information would be useless or inert. All of these give examples of the relationship between information and how focusing on the source of the information, the quality of the information, or the means to fuse the information can inform a commander's choice in how they want to incorporate OIE into their choice of symmetrical or asymmetric force and maneuver.

In the Information Age, electronic information systems are vital to the function of a modern military in a way that a tank or plane was considered valuable just years ago.[27] Smart munitions cannot function without information control systems and precision guidance tools which require some form of networked communications interfaces or embedded coded instructions. Many of these systems have internal defenses to protect against an attack, not from another missile or munition, but against other operating code or disruptive signals. Military capabilities now must preserve their own information and resist the generation of information from outside sources that would disrupt their essential operating components to perform a vital military task. Using a munition to destroy or disable another munition in an explosive or kinetic encounter is still an available symmetrical option. Using malicious code and disruptive or spoofing signals in a symmetrical engagement of the operating systems of that munition are options as well.

Military capabilities have more embedded networked functionality, both internal to a system and externally between unmanned systems and their human counterparts. We must expect that information, counter-information, and counter-counter-information will be the way of information power engagements. They will have symmetries and asymmetries all their own much as tanks with more armor or bigger guns were asymmetrically advantaged against their less armored counterparts. Further, information functions and capabilities will no longer simply be asymmetric means to facilitate other decisive engagements but are, and will be, vital to the parity and symmetry of forces in the future enabling the Napoleonic aim of war.

... there was a time when information was considered primarily an asymmetric means to facilitate other lethal engegements that were considered more decisive.

Finding the best avenue of approach, deciding on an attrition or maneuver process, and selecting symmetric or asymmetric informational means to achieve a decisive outcome is an essential choice for a commander today to operate in the information environment. This makes P.W. Singer's books, such as *Wired for War, Like War, Cybersecurity and Cyber War, and Ghost Fleet,*[28] read less like fiction and more like field manuals with wargaming vignettes suitable to instruct current and future commanders on the principles of information environment maneuver

to apply the information function and capabilities both symmetrically and asymmetrically.

Direct and Indirect Approach

Maneuver and attrition as well as symmetry and asymmetry ultimately evolve into the choice of how we want to approach an adversary and what means we want to apply against them. As has been shown up to this point, information capabilities conform to the same principles of maneuver/attrition and symmetry/asymmetry that has bound the use of other traditional means for centuries. That makes the criteria for applying information means the same as for other capabilities in other domains. As noted previously, information components, systems, and informational exchanges (media, communications, operator displays, etc.) are integrated in just about every capability and operation providing an additional vector of attack and aimpoint to target. Ultimately, how we position our forces and whether we apply symmetric or asymmetric means to confront components or systems is a choice between whether we want to confront the adversary directly or indirectly.

Direct and indirect are two versions of what is referred to as an approach. The *approach* is defined as the manner in which a commander chooses to contend with an adversary's center of gravity (COG).[29] The concept of a COG is also fraught with controversy in terms of how it is interpreted from Clausewitz's original definition and how we determine what it is today.[30] It is important to understand that the COG is a key element in the selection of an operational and tactical approach in accordance with our Marine Corps doctrine. For simplicity we can say that Clausewitz's conception of the strategic and operational levels of war took for granted that one would mass force against the enemy's s*chwerpunkt*, or center of gravity ('the hub of all power and movement, on which everything depends') and destroy it. In other words, a war or battle of annihilation.[31]

A direct approach attacks the enemy's COG or principal strength by applying combat power directly against it.[32] A COG is generally well protected and not vulnerable to a direct approach. If the commander's reasoned intuition and assessment of operational value makes this approach worth the risk, it represents the most direct path to victory. This has been the classical idea of war and relies typically on attrition achieved by symmetry of means and annihilating resistance.

An indirect approach attacks the enemy's COG by applying combat power against a series of decisive points that lead to the defeat of the COG while avoiding enemy strength in an erosive process.[33] B.H. Liddel-Hart, the quintessential theorist of the indirect approach, wrote that

> effective results in war have rarely been attained unless the approach has had such indirectness as to ensure the opponent's unreadiness to meet it. The indirectness has usually been physical, and always psychological. In strategy, the longest way around is often the shortest way home.[34]

The indirect approach includes a cognitive aspect, yet that is not the exclusive focus of an attack for operations in the information environment as we have highlighted in our previous examples of narrative or electromagnetic engagement options. When a modern commander chooses to engage an adversary through the information environment, direct and indirect approaches are both available for a panoply of targets than just those that affect human cognition.

Through most of the history of conflict, informational inputs to a physical military capability were largely mechanical. Think stick and rudder inputs by wire for a World War II-era aircraft wherein the only information interface existed between the operator and the control inputs, similar to the pre-Jacquard Loom from the prior example. Very little could be done in the information sphere that directly attacked a military capability and incidentally undermined the confidence of the operator not only in the system but in the cause for which they were dedicating their efforts and risking their lives. If any information activities were applied to conflict, they were largely indirect and limited to actions like sabotage (the disruption of mechanical information inputs on a capability or system), operational or tactical deception, and the attempt to influence fighters through propaganda. They were rarely directly influential in the outcomes of a conflict but did set conditions to support direct engagement by other means.[35] A pilot in a previous era could see a compatriot's plane shot down and still not succumb to the propaganda projected by the adversary insisting that said pilot was fighting a lost cause while that airman felt that sufficient means still existed to resist the enemy. Those forms of information engagement were unable to target directly, in any consequential way, that physically disrupted, degraded, or destroyed a military capability or psychologically convinced soldiers to abandon their cause while they were confident in their means to resist. Thus, information activities were considered indirect and asymmetric in their application. Despite the limited effectiveness of information actions in the past, it was still important to be persistent in that sphere and competitive in responding to adversary information.[36] With the evolution in information technology and the use of electronic control systems that intervene between the user inputs to direct mechanical systems, asymmetry of means are not the only valid way in which operations in the information environment can be conducted or maximized to disrupt a vital military capability or influence an operator.

Modern military capabilities are more integrated with informational systems and thus more subject to exploitation and disruption through information environment maneuver. Information components are indistinguishable in their importance in a system as a bolt is in a rifle or loader on a tank. They are fundamental to the operation of a system and in some cases can be disrupted if not protected. Knowing that embedded systems may be vulnerable to exploitation, many of those components and their associated operational code are undergoing a "hardening" that is akin to placing informational "armor" to protect against a likely form of information capability-enabled attack. In essence, developers now expect a form

of direct attack on a system and have set up the proverbial defense along the most "likely avenue of approach" to defend the system so that it can continue to perform its function to allow for the total operation of a capability. Directly engaging a capability's hardened information system with an electromagnetic spectrum action is effectively a "symmetric" attack no different than engaging a physical armor system with a traditional conventional weapons system. This realization is causing the DOD to identify the information vulnerabilities in our own systems and create hardening standards against electromagnetic attacks.[37] This is the proverbial information version of siting a machine gun with a principle direction of fire down an likely avenue of approach. Engaging in such a manner is certainly a direct approach and may collapse an adversary capability, but it comes with the high possibility that the "information terrain" is heavily defended and the attack will be contested. A condition like this would lead any commander to think of alternatives to attrition warfare and seek maneuver warfare solutions to this challenge.

Many capabilities also rely on an external family of support systems that have embedded control systems that, when attacked, can disrupt or eliminate their ability to provide a service or function to the primary capability. Leveraging a supporting system's vulnerability creates an "indirect" attack option and applies "asymmetric" information means to disrupt or degrade the use of a primary adversary capability. An example case may be attacking a fuel pump with a networked industrial control system that manages the valves for the pump. That pump system may be how the enemy chooses to refuel their tanks. If the tanks cannot get any fuel from a tactical supply system, then a weakness was exploited via an indirect approach and with a means asymmetric to the adversary defense of their networks and capabilities. Additionally, many control systems are connected to an operator display making it feasible to disrupt both the operation of the system and post a message to the user warning them of the futility of their cause. In the case it supports Liddell-Hart's observation that the indirect approach may include the psychological as much as the physical through literal messages amplifying the inability to cognitively cope with compounding erosive physical effects.

The variety of ways in which information transmission and sharing occurs gives the Marine Corps multiple ways to maneuver against the adversary, exploit gaps and seams in their *systems* or *networks*, and attack at the time and place of our choosing to corrupt that information. This is done in order that the adversary act or operate in ways that keep them from achieving their objectives or disrupting ours. This can be done either through a direct or indirect approach and with symmetric or asymmetric means as an integrated function of our targeting and fires efforts with the capabilities of the OIE in a dynamic and expanding conflict space.

OIE

OIE is emerging as the maneuver doctrine of the information environment and provides a methodology for how to perform a direct or indirect approach. Yet, like the air combat philosophers of a century ago, we are still coming to terms with the best way to approach this practice.[38] In addition to that, the means of conducting either narrative or electromagnetic maneuver are changing exponentially, making progress on the methodology of OIE iterative and non-linear as we assess how to engage and respond to every new form of attack and defense daily in both the narrative and electromagnetic space.

OIE is defined as actions taken to generate, preserve, or apply military information power in order to increase and protect competitive advantage or combat power potential within all domains of the operational environment.[39] OIE engages sources of information transmission, information inputs, and information processing to facilitate the overall Information warfighting function and the practical realization of military information power. The Marine Corps has foregone the terms such as information operations or information warfare in favor of OIE. Information operations is defined as

> the integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own.[40]

Information warfare has no official U.S. government definition yet, "it is typically conceptualized as the use and management of information to pursue a competitive advantage, including offensive and defensive efforts."[41] The focus on adversary decision making alone is insufficient to describe the purpose for actions in the information environment, thus information operations is not a useful framing for the totality of information actions. Additionally, the stipulation of warfare alone is too limiting to the idea of when to apply information means in an age of continuous conflict. The information environment is virtual and physical with means that can produce both lethal and non-lethal effects, approached directly or indirectly, and applied to either in an attritive or maneuver warfare design. In many ways, operations in the information environment is the best expression of a multi-domain conflict, wherein information capabilities can maneuver through a virtual environment to produce a physical effect or vice versa in accordance with existing warfighting principles.

The Marine Corps' ability to perform OIE is broken into seven functions supported by six capability areas. The functions are: 1) assure enterprise command and control (C2) and critical systems; 2) provide IE battlespace awareness; 3) attack and exploit networks, systems and information; 4) inform domestic and international audiences; 5) influence foreign target audiences; 6) deceive foreign target audiences; 7) control OIE capabilities, resources, and activities. Like the six functions of Marine aviation or the six functions of tactical combat service support, these seven functions characterize the "what" of OIE. The six capability areas are: 1) electromagnetic spectrum operations; 2) cyberspace operations; 3) space op-

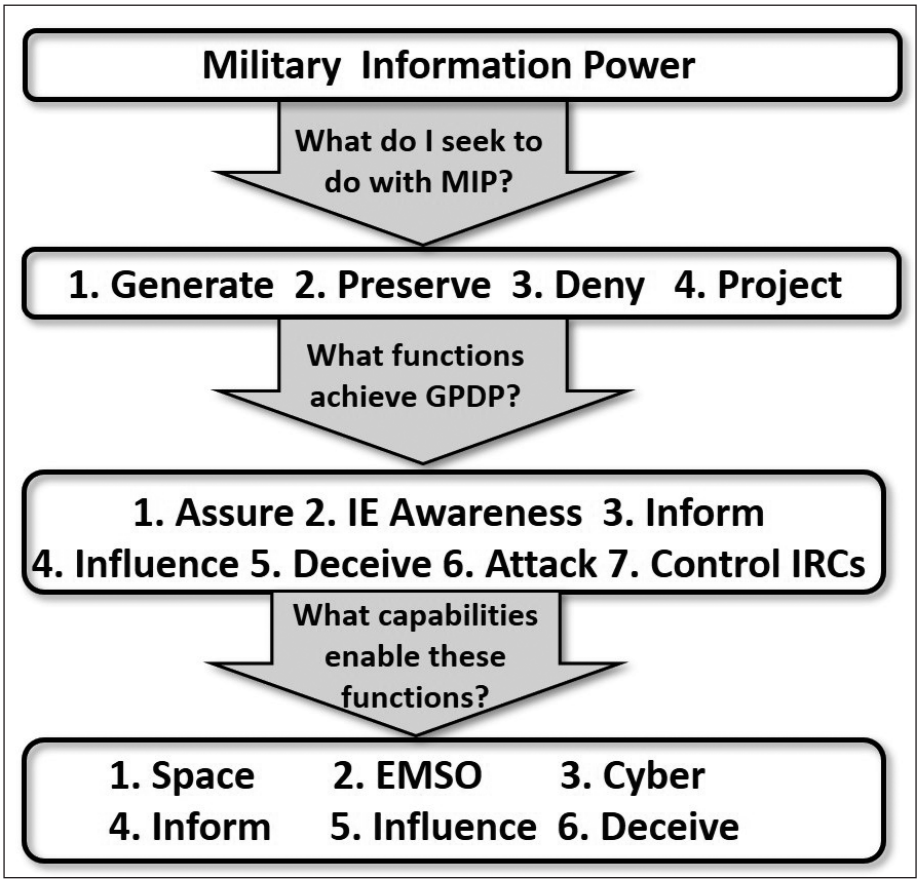

Figure 2: The logical flow of military information power to the information capabilities. *(Fifure provided by author.)*

erations; 4) influence operations; 5) deception operations; and 6) inform operations. These six capability areas characterize the "how" of OIE. Suffice it to say, each one of these functions and capabilities is a lesson unto itself.[42] Their mention here is simply to stipulate that when we are referring to OIE these are the functions and capabilities applied. The essence of this article is to confirm that these elements can be integrated into overall operations and that information as a function can be used to engage an adversary according to the principles of direct and indirect approach. These functions and capabilities just highlight how that is done and is the subject of a deeper study for Marines today. (See Figure 2.)

Gaining information superiority over the adversary should always be the underlying premise of OIE. Now, more than any time in history, military capabilities rely on informational systems. Those systems, if successfully attacked can negate the capacity of the adversary to perform their intended operations and incidentally undermine the confidence of the operators not only in the systems they have been given to use, but in the cause for which they were dedicating their efforts and risking their lives.

Conclusion

In the past, information actions and physical engagements were at unique ends of the spectrum:

> The inherent assumption during the Industrial Age was that information contained within intelligence, command and control, communications, and weapons systems was largely secure, accurate, and trusted. The Information Age has fundamentally undermined this assumption and thus altered the technological and combat power advantages the United States experienced during the Industrial Age.[43]

As more capabilities operate with embedded programming and more communications rely on integrated networks of information, the connection between capability and information is less distinctly separated. OIE forms the maneuver methodology that takes into account this newer synergy of information with traditional military capability and amplifies the opportunities to engage an adversary either directly or indirectly across the spectrum of conflict.

The evolution in terms between information operations, information warfare, and OIE makes one looking from the outside question whether those on the inside are actually are actually having a substantive or a semantic debate that makes a difference to improving the practice.[44] Regardless of the practical challenges and philosophical divides, delivering effects in the information environment will be, if it is not already, as vital to a military operation as eliminating radars to blind air defense was in the past in order to achieve freedom of action and maneuver in the air domain. Strangely, this gives way to the idea that information properly applied may even preclude the need for the traditional use of airpower in certain instances in much the same way that airpower advocates once claimed that airpower may limit the need for ground operations. That is certainly a testable conclusion and we should resolve to determine if military information power enables, or simply facilitates, the other warfighting functions. The answer likely rests on the balance between the two positions.

This places the force in an quandary: institutional information forces and capability placeholders must exist in advance of a coherent maneuver philosophy because if they do not, our security may be placed at unnecessary risk by those nations or actors who have a more defined appreciation of an information-based military approach. However, investment in information-based means cannot reside on fear and uncertainty alone. No, it is a requirement of the entire Marine Corps by virtue of the information warfighting function to realize the use of information capabilities more fully and understand how to perform information-based maneuver as

a universal discipline like air, land, and maritime maneuver is for any competent military professional. There are institutional learning pains to define what constitutes elements of information, what means are considered information capabilities, what the functions of information are, and what activities are conducted to operationalize and realize those functions in a coherent form for military operations.[45] In essence, how and with what do we exercise the components of information through an operational model to benefit the military discipline in the art and science of war? However, we answer the question, OIE synchronizes with established principles but its unique characteristics bring new dimension to the selection of a direct or indirect approach.

Notes

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

2. Office of the Chairman of the Joint Chiefs of Staff, *Joint Concept for Integrated Campaigning*, (Washington DC: March 2018), available at https://www.jcs.mil; and Department of Defense, *Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge*, (Washington DC: January 2018), available at https://dod.defense.gov.

3. Catherine A. Theohary, *Information Warfare: Issues for Congress (R45142)*, Congressional Research Service, (March 2018), available at https://crsreports.congress.gov.

4. Information Age defined in https://www.merriam-webster.com: "the modern age regarded as a time in which information has become a commodity that is quickly and widely disseminated and easily available especially through the use of computer technology."

5. Nathan K. Finneyand Amanda M Hemmingsen, *On Strategy: A Primer*, Combat Studies Institute Press, (Fort Leavenworth, KS: The Army University Press, 2020).

6. Ibid.

7. Mark Pomerleau, "What Cyber Command's ISIS Operations Means for the Future of Information Warfare," *C4ISRNET*, (June 2020), available at https://www.c4isrnet.com.

8. Brian Kerg, et al., "Call to Action: Operations in the Information Environment." *Marine Corps Gazette*, (Quantico, VA: May 2020), available at https://mca-marines.org.

9. Herb Lin, "Doctrinal Confusion and Cultural Dysfunction in the Pentagon Over Information and Cyber Operations." *Lawfare*, (March 2020), available at https://www.lawfareblog.com.

10. One may say that intelligence capabilities operate in the same way. That is not a suitable comparison since the reason for preserving the secrecy of the means is to protect a source or method That is why we decouple the intelligence products from the means as much as feasible and in varying grades of detail to enable the greatest use of the outputs to facilitate making sense of the operating environment. Information outcomes and means are often conflated in operational applications making it difficult to visualize their contribution to conflict outside of select circles.

11. *MCDP 1.*

12. Office of the Chairman of the Joint Chiefs of Staff, *DOD Dictionary of Military and Associated Terms*, (Washington DC: January 2020), available at https://www.jcs.mil.

13 Eric X. Schaner, "What is Military Information Power?" *Marine Corps Gazette*, (Quantico, VA: April 2020).

14. Ibid, *MCDP 1.*

15. Joint Memorandum, Deputy Commandant for Combat Development and Integration and Deputy Commandant for Information, "Definitions for Information Related Terms," (Washington, DC: January 2020).

16. Ibid, *MCDP1.*

17. Ibid, *MCDP 1.*

18. Ibid, *MCDP 1.*

19. *DOD Dictionary of Military and Associated Terms.*

20. *Merrian-Webster*, s.v. "Lethal," available at https://www.merriam-webster.com.

21. Department of Defense Directive, *DoDD 3000.03E, DoD Executive Agent for Non-Lethal Weapons (NLW), and NLW Policy*, (August 2018), available at https://www.esd.whs.mil.

22. Ibid, *MCDP 1.*

23.Robert Tomes, "Relearning Counterinsurgency Warfare" *Parameters,* (Carlisle, PA: U.S. Army War College, Spring 2004).

24. Ibid, *On Strategy: A Primer.*

25. John Boyd, "John Boyd: Patterns of Conflict Presentation and Biography." *GeekBoss*, (November 2019), available at https://geekboss.com

26. Emmanuel Anthony, Posselt, "The Jacquard Machine Analyzed and Explained: with an Appendix on the Preparation of Jacquard Cards: Posselt, Emanuel Anthony, 1858- [from Old Catalog]: Free Download, Borrow, and Streaming." *Internet Archive*, (Philadelphia, PA: Pennsylvania Museum and School of Industrial Art, January 1887), available at https://archive.org.

27. Malte von Spreckelsen, "Electronic Warfare–The Forgotten Discipline." *Joint Air Power Competence Centre*, (Kalkar, DE: NATO Joint Air Power Competence Centre, December 2018), available at https://www.japcc.org.

28. Information on P.W. Singer available at https://www.amazon.com.

29. Office of the Chairman of the Joint Chiefs of Staff, *JP 5-, Joint Operation Planning*, (Washington DC: June 2017).

30. Dale C. Eikmeier, "Let's Fix or Kill the Center of Gravity Concept," National Defense University, (Washington, DC: National Defense University Press, October 2016), available at https://ndupress.ndu.edu.

31. Ibid, *On Strategy: A Primer,* quoting *On War*, Peter Paret translation.

32. Ibid, *JP 5-0.*

33. Ibid, *JP 5-0.*

34. Basil Henry Liddell-Hart, *Strategy,* second revised editions, (New York, NY: Plume, 1991).

35. Ibid, *Information Warfare: Issues for Congress (R45142).* The CRS report describes several historical examples to amplify this point.

36. Although not directly related to this specific example, the condition of being operationally persistent and maintaining competitive interaction is identified in the cited Lawfare article regarding the current state of cyber activities by nations in competition below the threshold of traditional armed conflict. It cogently describes the dynamic in any era where information exchange had to be maintained in conflict if only to limit adversary freedom of action in that realm. Persistence is a requirement to be

competitive. Once cannot drift in and out of the conversation, as it were, and expect to keep one's place or be better advantaged than when one left. See Michael P. Fischerkeller and Harknett J Harknett, "A Response on Persistent Engagement and Agreed Competition." *Lawfare*, (October 2019), available at https://www.lawfareblog.com.

37. Government Accountability Office, Report to the Committee on Armed Services, U.S. Senate, "Weapon Systems Cybersecurity: DOD Just Beginning to Grapple with Scale of Vulnerabilities," (Washington DC: October 2018), available at https://www.gao.gov.

38. Ian T. Brown, "OIE And MCDP-1: Boyd's Foundation." *Marine Corps Association and Foundation Blog*, (April 2020), available at https://mca-marines.org.

39. Ibid, *Joint Memorandum, Definitions for Information Related Terms*.

40. *DOD Dictionary of Military and Associated Terms*.

41. *Information Warfare: Issues for Congress (R45142)*.

42. See Eric Schaner, "What are OIE?" *Marine Corps Gazette*, (Quantico, VA: April 2020).

43. Eric X. Schaner, "Information and Uncertainty," *Marine Corps Gazette*, (Quantico, VA: April 2020).

44. Ibid. "Doctrinal Confusion and Cultural Dysfunction in the Pentagon Over Information and Cyber Operations."

45. For insights into the most recent discussion on foundational terms discussed in this article please see the April edition of the *Marine Corps Gazette*. This article specifically builds on and references the definitions identified in that edition of the *Gazette* to evolve the integration of OIE into the principles of conflict in established and tested doctrine. If those definitions are false or inaccurate as tested in wargames and experiments, then this discussion will need iterative improvement