A Theory-Based View of IO

By Marc J. Romanych, MAJ, USA (Retired)

Editorial Abstract: *The military operates in the information environment for the same reason it operates in the physical environments of land, sea, air, and space – to reduce the adversary's effectiveness and will to fight. IO is distinguished from other operations by its purpose – to create and sustain an information advantage that can be turned into an operational advantage over the adversary. Retired Army Major Marc Romanych gives us a better understanding of the nature and character of the information environment, the dynamics of the information domain, and military operations to affect the content and flow of information.*

At its very core, military information operations (IO) are about information and its utility as a capability to wage war. Without a doubt, our adversaries use information to further their goals and to thwart our national interests and objectives. If this situation was not noticeable prior to the events of September 11, 2001, it is certainly obvious now. Information has become a commodity for use by armed forces, and the information environment is now a critical part of the military operating environment.

Today, the information environment exists everywhere in the world. Even in the remotest of areas, activity in the information environment significantly impacts civilian populations, government and private organizations, and the armed forces. Additionally, all organizations, not just modern armies, use and share the information environment. In fact, in most cases, any group or organization that uses the information environment must also compete with other entities for access to, and use of, information.

The information environment is interwoven with the physical environments of land, sea, air, and space. The degree and complexity of these connections vary from place to place, but in general are ever increasing. Thus, to be successful, today's military forces must now treat the information environment as part of the battlespace. Ignored, or mishandled, the information environment can present a serious threat to our mission.

This article presents a view of IO based on the application of the theory behind the concepts of information environment, information superiority, and information operations. It attempts to present a rational explanation of IO that can be used to develop actionable doctrinal concepts.

Information Environment

The information environment is abstract. It is a man-made construct that describes and characterizes an operating environment based on the existence and proliferation of information and information systems. Although a portion of the information environment is composed of material objects, information systems and networks, the primary component of the information environment – information – is intangible. Therefore, unlike the land, sea, air, and space environments, the information environment has minimal physical presence. Yet, despite its predominantly nonphysical nature, the information environment can manifest itself in very real ways.

There are several factors that must be considered by any model of the information environment. The first, as discussed in the previous paragraph, are the information environment's tangible and intangible parts. Second, is a duality resulting from the two primary views of information - *information-as-message*, which regards information as a message or signal that contains meaningful content, and *information-as-medium*, which considers information as a system, or perhaps means, by which data and information are created, manipulated, and exchanged.[1] This duality of message and medium reveals itself within the information environment as information content and flow.

To understand information's effects on military operations, it is useful to visualize the structure of the information environment and the relationship between its components. For this purpose, the information environment can be thought of having three distinct, but closely interconnected domains – physical, information, and cognitive (see Figure 1):[2]

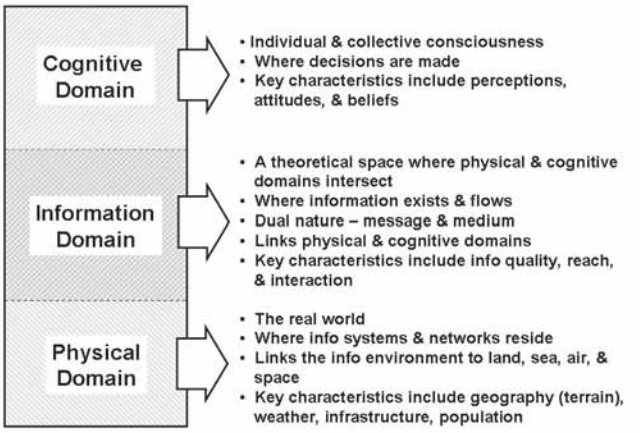

Figure 1. Information Environment Construct.

- Physical Domain. The real, or material, part of the information environment that coexists with the physical environments of land, sea, air, and space. It is the domain of maneuver and combat operations. It is where the physical elements of information systems and networks reside, and for the purposes of IO, where information systems are attacked and defended.

- Information Domain. The abstract space where information exists and flows. The information domain consists of information itself, but is also the medium in which the functions of information systems (i.e., information collection, processing, and dissemination) occur. The information domain links the reality of the physical domain to the human consciousness of the cognitive domain and therefore is critical to the command and control of military forces. In this domain IO manipulates information content and flow.

- Cognitive Domain. The individual and collective consciousness that exists in the minds of human beings. The cognitive domain is where perceptions are formed and decisions are made. In this domain, IO seeks to have an effect on the interpretation and use of information by decision makers, other specific audiences, and sometimes, whole population groups.

The domains are closely interconnected. Information systems in the physical domain create and direct the flow of information in the information domain, which in turn affect human perceptions, attitudes, and ultimately decision-making in the cognitive domain. Thus, activity in any one domain can produce consequent effects in the other two domains, and because the physical domain connects the information environment to the rest of the physical world, the effects of information may be felt in other parts of the battlespace.

For the purposes of IO, it is important to note the information domain's role as the linkage between

"activity in any one domain can produce consequent effects in the other two domains"

decision-making and action. Armed forces use the information environment to collect, process, and disseminate information for situational awareness and decision-making, and once decisions are made, to process and disseminate information so that it can be turned into action. The information domain, then, is the means physical domain activity and decision-making interrelate, and as such, is critical to both the formation and the execution of decisions.

Information Domain

Of the three domains, the information domain is the key to using information as a military capability. By manipulating information content and flow, a specific effect can be created that will impact other organizations that share the battlespace. To this end, the information domain can be thought of as having three primary attributes that characterize the utility of information to civilian and military organizations – information quality, reach, and interaction.[3] The discussion of information quality, reach, and interaction is an abbreviated summary of the work described in Understanding Information Age Warfare. According to the authors, the information domain can be expressed in terms of richness, reach, and quality of interaction.

For the purpose of applying the concepts to IO, minor modifications were made to the terminology.

These attributes, or characteristics, can be summarized as follows:

- Information Quality. The value, or worth, of information to an organization in terms of accuracy, relevancy, and timeliness.[4] Organizations require information that is useful to their mission and current situation.

- Information Reach. The degree to which an organization shares and distributes information. To collaborate or synchronize activity, an organization must exchange information both internally and with the rest of the information environment.

- Information Interaction. The quality of information exchange (e.g., face-to-face discussion, radio, print, telephone, computer network) available to an organization for the collection, processing, and distribution of information. The employment of information technology and process affects an organization's ability to use information and interface with the information domain.

The relationships between information quality, reach, and interaction, can be portrayed as a three-dimensional model with each axis representing a specific attribute (see Figure 2).

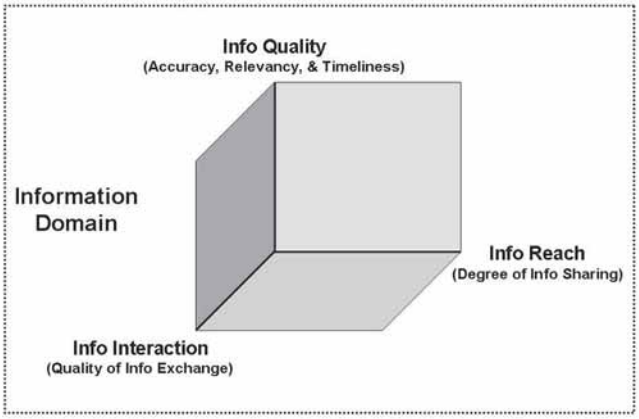

Figure 2. Attributes of the Information Domain.

Information Needs, Position, and Situation

All organizations require information to operate. However, information is not benign. Organizations create and disseminate information to gain an advantage over their competitors. To understand how a military force can achieve an advantage over its opponents in the information domain, it is necessary to address the concepts of information needs, position, and situation.[5]

To operate successfully, an organization must meet its information needs. Information needs is defined as the set of information required to plan and execute a mission or task. Every organization has unique information needs as predicated by factors such as the structure of the organization, type of activities, and available technology. Information needs can be articulated in terms of the three previously discussed key attributes of the information domain (i.e., quality, reach, and interaction) and then visually portrayed as a three-dimensional volume (see figure 3).

To meet its information needs, an organization requires a steady flow of quality information. Information position is an organization's information state at any given point in time. It is a summation of how much information an organization possesses. Information position changes as an organization improves its information quality, distribution, and means. Conversely, an information position can diminish if there is a decrease in information quality, distribution, or means.

An organization's information needs and position vary with mission and time – neither is fixed or static. The disparity between the organization's information needs and position is its information situation. If the availability of information exceeds an organization's needs, then it is in a positive information situation. If information availability is less than the organization's needs, then the organization is in a negative, or deficit, information situation. In general, it should be expected that organizations will almost always be at an information deficit, especially military forces engaged in combat operations. Furthermore, no two military formations are likely to have the same information needs, position, and situation, even though they occupy the same battlespace.

Joint Combat Camera Photo

Information advantage is important in the war against terrorists, especially considering the dangerously close proximity of the enemy with the civilian population.

Information Advantage

Information advantage is the ability to use information better than one's opponent. By definition, having such an advantage means being in a superior information situation relative to the opposition. Such an advantage is determined by comparing the difference between each side's own information situations (for a simple example, see Figure 4).

Information advantage is relative. Even though two organizations exist in the same information environment, their information needs and positions (and hence situation) will be dissimilar. Therefore, information advantage must be considered in terms of each organization's own information situation relative to that of their opponent. Furthermore, relativity extends to how the information environment affects each force. Since no military formations are likely to possess the same capabilities, specific characteristics of the information environment will impact them in different ways. Thus, information advantage not only results from the ability to use information better than the adversary, but it can also be a consequence of leveraging the information environment to one's own advantage.

It should be noted that reducing an adversary's information position is not the only way to achieve an information advantage. Activities that improve or maintain one's own information situation are also critical to improving and maintaining one's own situation relative to the adversary. However, these activities are unlikely to unilaterally result in an exploitable information advantage. For military forces, attacking the adversary in the information environment and manipulating the information environment are often the best ways to gain an advantage.

The worth of information advantage is "derived from the military outcomes it can enable."[6] As an operational or tactical capability, information is unlikely to unilaterally achieve decisive results. The real contribution of an information

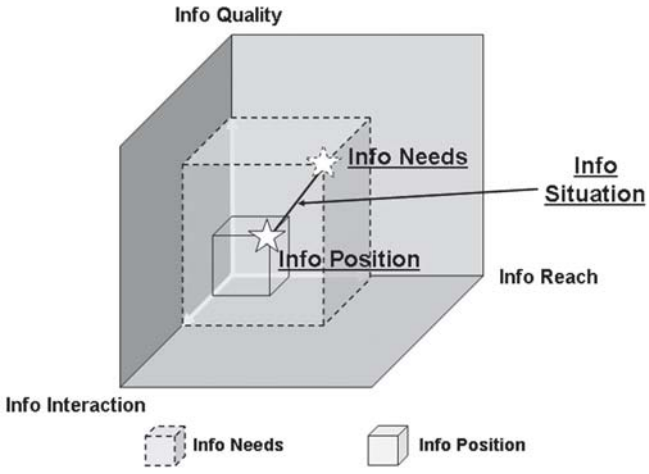

Figure 3. Information, Needs, Position, and Situation.

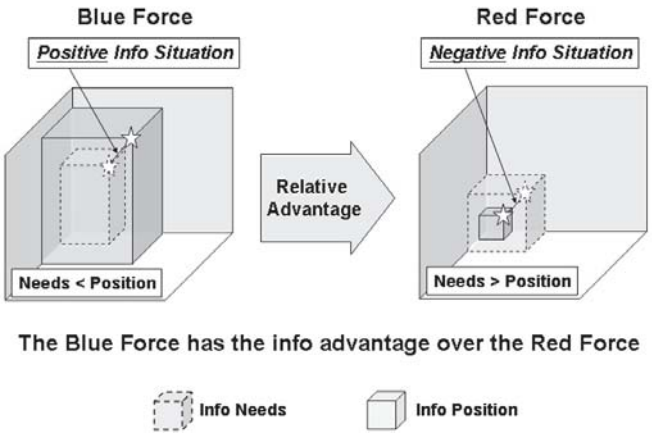

Figure 4. Information Advantage.

advantage is the subsequent outcomes in the physical and cognitive domains. However, an advantage in the information environment does not automatically equate to an exploitable result elsewhere in the battlespace – that is information superiority.

Information Superiority

Information superiority is the least understood term associated with IO. Information superiority is an operational advantage derived from having an information advantage over the opposing force.[77] Definitions of information superiority abound and the terms "information advantage" and "information superiority" are often used interchangeably.

This operational advantage is the product of manipulating the use, content, and flow of information.

An operational advantage can manifest itself in two general ways - as a force or position advantage in the physical domain, or a decision-making advantage in the cognitive domain. It should be noted that operational advantages (i.e., information superiority) are not achieved in the information domain.[8] This is because the information domain is abstract - it does not really exist. Information advantage describes a theoretical concept in an abstract part of the battlespace. Any type of advantage is only useful to the military if it occurs where the military operates – in the physical world (i.e., domain) of fire and maneuver or in the cognitive domain where decisions are made to employ military forces and weapons.

Both information superiority and information advantage are localized and transitory phenomenon. This is because battlespace information content and flow are in continual flux, and the information situations of opposing forces will constantly change. Therefore, both information superiority and advantage must be sought at a particular time and place in the battlespace – normally in association with the decisive and decisions point of an operation.[9]

Information Operations

So then, what is IO? In practical terms, it is synchronized activities that impact the use, content, and flow of information in the battlespace. The broad purpose of IO is to gain and maintain an information advantage over the adversary. This is achieved by creating and sustaining a gap between the adversary's information needs and position through the manipulation of information in the battlespace.

Although IO operates in all three domains of the information environment, it must focus its effort on the information domain where an information advantage can be achieved. To create an information advantage IO must impact both the content and flow of information critical to adversaries and any entities in the battlespace. Activities that only address information content will fail to attain an information advantage. Likewise, impacting the way information flows without regard for its content will not yield an exploitable information advantage.

"Information superiority is the least understood term associated with IO."

Information operations are not stand-alone operations. All military action has the potential to alter information content and flow, and possibly create an effect in the information environment. Furthermore, any asset or capability whose activities can affect the content and flow of information is a potential contributor, or even detractor, to an information operation. Therefore, IO is really more than a set of finite, discrete capabilities – it is an approach to planning and conducting military operations. As an integrated operation, IO should represent all methods and means that can affect information present in the battlespace.

To execute an information operation, a military force synchronizes activities to affect and protect the means of information content and flow in the physical domain. In sum, these actions impact information content and flow and how the adversary force uses that information. This manipulation of the information domain and adversary information capabilities results in an information advantage. In turn, the information advantage affects the actions and decision-making of adversary forces and other organizations that share the information environment; that is, it provides an operational advantage (i.e., information superiority) to the friendly force.

Conclusion

The military operates in the information environment for the same reason it operates in the physical environments of land, sea, air, and space – to reduce the adversary's effectiveness and will to fight. IO is distinguished from other operations by its purpose – to create and sustain an information advantage that can be turned into an operational advantage over the adversary, and its means – affecting the content and flow of information.

The lesson is clear – IO must go beyond activities to affect information systems and networks. It must concentrate on information in the battlespace. There are many ways and means to impact the information domain,

The Associated Press

IO may be used to influence an adversarial leader's decision-making and populace perceptions to gain advantage.

and IO should represent all these capabilities. However, while IO's ultimate objective may be to influence leader's decision-making and populace perceptions, these effects in the cognitive domain are not the sole provenance of IO.

This article just scratches the surface of a complex and evolving subject.[10] Our understanding of the nature and character of the information environment, the dynamics of information domain, and military operations to affect information content and flow is limited. No doubt with more theoretical work and practical experience, our view and employment of information as a military capability will change.

End Notes

[1] There is a third view of information – information as physical matter – that is a little understood concept. It has the potential to fill the gaps in the other two views and possibly even reconcile dual nature of information. For a good discussion of the three views of information see *In Athena's Camp: Preparing for Conflict in the Information Age* by John Arquilla and David Ronfeldt (Santa Monica, California: RAND, 1997), pages 144-149.

[2] The three domain model is an adaptation of work by the DoD Command and Control Research Program (CCRP) presented in *Understanding Information Age Warfare,* by David S. Alberts., John J. Garstka, Richard E. Hayes, and David A. Signori (DoD Command and Control Research Program, Washington D.C., August 2001), pages 10-14. The text and diagram of the three domains is adapted from "Visualizing the Information Environment" by Marc J. Romanych (*Military Intelligence Professional Bulletin,* Volume 29, Number 3).

[3] The discussion of information quality, reach, and interaction is an abbreviated summary of the work described in *Understanding Information Age Warfare*. According to the authors, the information domain can be expressed in terms of richness, reach, and quality of interaction. For the purpose of applying the concepts to IO, minor modifications were made to the terminology.

[4] This description is another simplification of the text in *Understanding Information Age Warfare*, which describes eight attributes for information quality: completeness, correctness, currency, accuracy, consistency, relevance, timeliness, and information assurance.

[5] The discussion of these concepts is another distillation of the work of Albert et al in *Understanding Information Age Warfare*.

[6] *Network Centric Warfare: Developing and Leveraging Information Superiority* by David S. Alberts, John J. Garstka, and Frederick P. Stein, (DoD Command and Control Research Program, Washington D.C., 1999), page 55. Actually, the authors were referring to information superiority. Subsequent work indicates that this idea is better applied to the concept of information advantage.

[7] Definitions of information superiority abound and the terms "information advantage" and "information superiority" are often used interchangeably.

[8] An operational advantage in the information domain is really just an information advantage.

[9] Decisive and decision points are that time and place in the operation when friendly and adversary forces must fulfill their information needs in order to successfully execute their respective missions.

[10] For further information on current theory behind the information environment, particularly the information domain, see *Understanding Information Age Warfare*.