10TH INTERNATIONAL COMMAND AND CONTROL RESEARCH AND TECHNOLOGY SYMPOSIUM
THE FUTURE OF C2

APPLYING THE DOMAINS OF CONFLICT TO INFORMATION OPERATIONS

INFORMATION OPERATIONS/ASSURANCE

By

Marc Romanych

JB Management, Incorporated
5500 Cherokee Avenue
Alexandria, VA 22312

703-354-6550 / 703-354-8889
FAX: 703-354-8889
mjromanych@cs.com

Applying the Domains of Conflict to Information Operations

Abstract

Military information operations (IO) are about information and its use as a means to fight an adversary. Fundamental to the use of information as a military capability, or perhaps even a weapon, is an understanding of the information environment and its utility to armed forces. However, several key concepts underpinning the conduct of military operations in the information environment are too abstract for practical application by operational and tactical level armed forces. As a result, commanders and staffs frequently relegate activities to affect the information environment to the realms of the esoteric or impractical.

Recent work conducted by the Department of Defense's (DoD) Command and Control Research Program (CCRP) provides a useful basis for visualizing the structure and characteristics of the information environment. Of particular utility is a model that describes three domains of conflict – the physical, information, and cognitive. Initially used to describe decision-making, this model, when combined with the two primary views of information – information-as-message and information-as-medium – provides a useful framework for describing how information can be used to support military operations.

To execute an information operation, a military force conducts activities to affect and protect information systems and networks in the physical domain. These actions are synchronized to affect information content, flow, and use in the information domain. The result is an information advantage that, in turn, generates effects to influence adversary and other organizations' decision-making in the cognitive domain and subsequent actions in the physical domain. In sum, these cognitive and physical effects provide an operational advantage (i.e., information superiority) at a specific time and place to the friendly force.

This paper explores the relevance of the CCRP's three-domain model to military IO. By applying the model to the doctrinal concepts of information environment, information superiority, and information operations, a view of IO emerges that field commands can use to convert doctrinal concepts into practical action. Recent experiences by ground forces during exercises and contingency operations demonstrate that this approach to understanding the information environment is understood readily by commanders and staffs.

Introduction

Although the U.S. military recognizes the existence of the information environment and its importance to armed conflict, many operational and tactical-level commands have difficulty grasping the role and use of information in defeating the adversary. The reason may very well be that several key aspects of operations in the information environment are too conceptual for commanders and staffs engaged in the immediate needs of day-to-day activities.

To employ information as an element of combat power, warfighters need a concept of information operations (IO) that fits into their doctrinal framework of the operating environment and military operations. The challenge then is to present a straight-forward view of information's utility as a resource to fight the adversary and as a medium in which military forces operate.

Information operations as currently defined by the Department of Defense are "actions taken to affect adversary information and information systems while defending one's own information and information systems."[1] In more practical terms, an information operation consists of activities to impact the content, flow, and use of information within a specific geographic area in order to gain an operational advantage over an adversary.

This paper applies the theory of the three domains of conflict as described by the Department of Defense (DoD) Command and Control Research Program (CCRP) to the concepts of information environment, information superiority, and information operations. In so doing, the paper attempts to present an explanation of IO that has practical utility to operational and tactical forces.

The Domains of Conflict

In its publications *Understanding Information Age Warfare* and *Effects Based Operations*, CCRP describes what it calls the "domains of conflict.[2] Developed primarily as a way to explain the process of decision-making, the three domains of conflict – namely the physical, information, and cognitive – can also provide a general framework for explaining how information affects the performance of military operations. In brief, CCRP's description of the domains is as follows:

- The physical domain is the real, tangible world; the environments of land, sea, air, and space. "It is the domain where strike, protect, maneuver take place across the different environments. It is the domain where physical platforms and the communication networks that connect them reside."[3]

- The information domain is "where information lives. It is the domain where information is created, manipulated, and shared. It is the domain that facilitates the communication of information."[4]

- The cognitive domain is in the mind of human beings. It is where "perceptions, awareness, understanding, beliefs and values reside and where, as a result of sensemaking, decisions are made."[5]

As pointed out by the CCRP authors, the domains of conflict can depict the relationship between physical action, information, and decisions. For the purpose of understanding how to use information as a military capability, the domains also represent aptly the structure of the information environment.

A Model for the Information Environment

The information environment, in contrast to the other environments in which military forces operate – land, sea, air, and space – is largely non-physical and abstract. It is a man-made construct based on the idea that the existence and proliferation of information and information systems has created a new operating dimension or environment. However, even though a portion of the information environment is composed of physical information systems, the primary component of the information environment – information – is intangible.

Any model of the information environment must reconcile the environment's tangible and intangible parts. The model must also rationalize information's dual nature; namely its utility as a message that contains meaningful content, and its existence as a medium by which data and information are created, manipulated, and exchanged.[6] Combining the three domains of conflict with the two views of information presents a useful view of the information environment (see Figure 1).[7] Building upon the work of CCRP, the domains can be refined to describe the information environment as follows:

- The physical domain is the tangible, or material, portion of the information environment that is part of the physical environments of land, sea, air, and space. It is where information systems and networks exist; whether technology or human-based networks. It is where individuals and organizations employ information systems. For the purposes of IO, the physical domain is where information systems are attacked and defended.

- The information domain is an abstract space created by the intersection of the physical and cognitive domains.[8] This is the domain through which individuals and organizations communicate and is where the functions of physical information systems occur (i.e., information collection, processing, and dissemination). Most importantly, the information domain is where information resides. Governed by information theory, the domain has two components: information-as-message and information-as-medium. This results in a duality of information content and flow. Furthermore, without information content and flow the information domain cannot exist.

- The cognitive domain is also abstract. However, unlike the information domain which is theoretical, the cognitive domain exists in the minds of human beings and collective consciousness of groups and organizations. Yet, this domain is intangible, consisting of those elements of human thought that influence decision-making and behavior. In this domain, IO seeks to affect the interpretation and use of information by decision makers, other specific audiences, and sometimes, whole population groups.

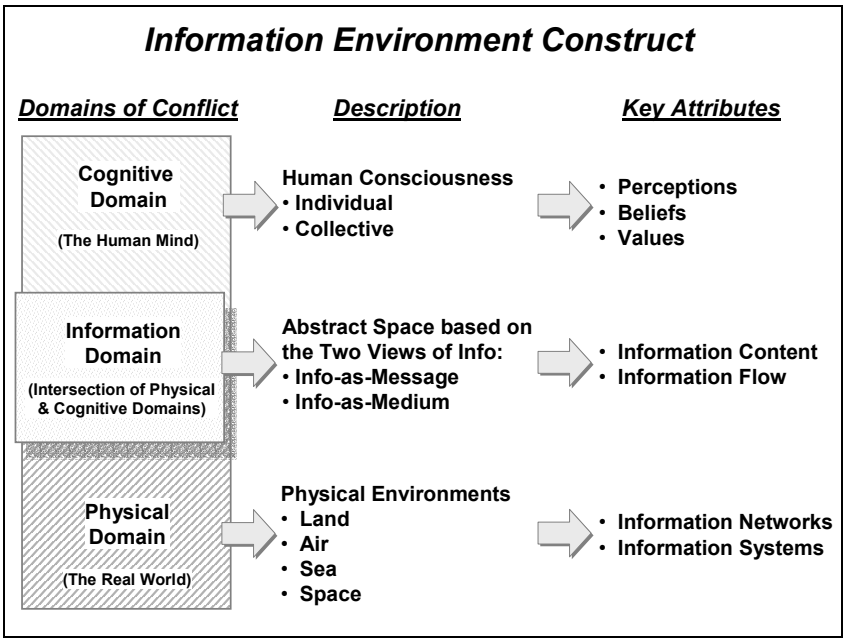

Figure 1 – The Information Environment

A Fourth Domain – Cultural or Social?

Culture is a dynamic that affects the attributes of all three domains. In the physical domain, societal hierarchy creates the social structures and human networks (i.e., organizations and institutions) that impact the use of information systems. In the information domain, language and cultural symbols impact the content and flow of information. In the cognitive domain, mental programming (i.e., values and beliefs) affects how information is used and provides structure to individual and collective decision-making.

In their works, *Understanding Information Age Warfare* and *Power to the Edge*, the authors suggest that there is a strong cultural dimension or aspect when applying the domains of conflict to an adversary.[9] What the authors loosely describe is a possible fourth domain consisting of cultural or social factors that impact the creation, processing, dissemination, and use of information. However, culture remains an amorphous and elusive concept.[10] Clearly, more work is needed to determine its place in the domain framework.

Domain Relationships

Even though the physical, information, and cognitive domains are often portrayed as separate entities, in reality they are closely connected. The interrelationship becomes clearer when a decision-making or action-reaction cycle is superimposed on the domain structure (Figure 2).

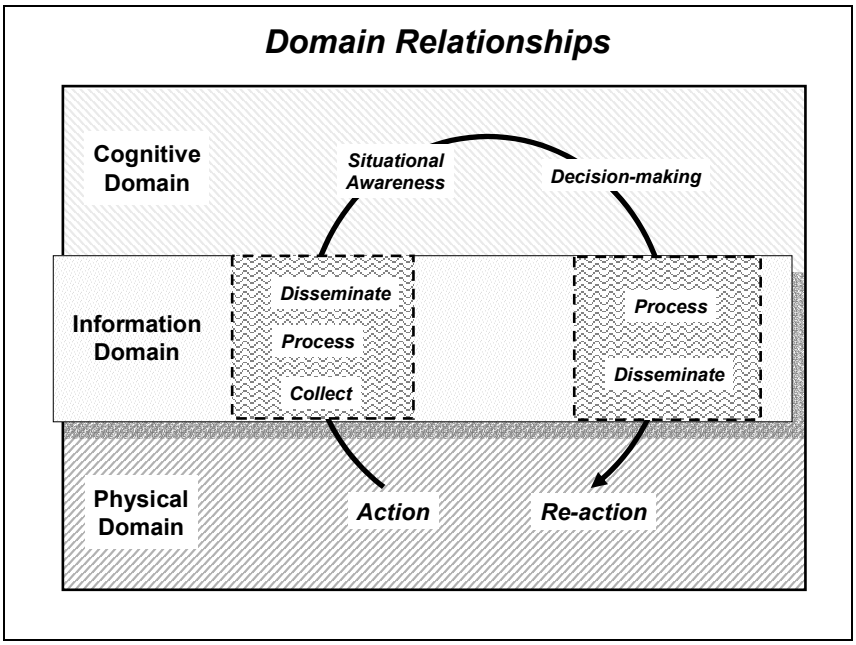

Figure 2 – Domain Relationships

Activity in the physical domain generates data which is collected by information systems. These information systems create and direct the flow of information through the information domain. In turn, the information is used by humans in the cognitive domain to form perceptions and to ultimately make decisions. These decisions are subsequently communicated through the information domain via information systems to the physical domain and then converted to into human activity. As a result, activity in one domain can produce subsequent effects in the other domains. Furthermore, because of the physical domain's connection to the rest of the rest of the physical world, information content and flow can manifest themselves in very real ways.[11] Thus, despite the information domain's intangible nature, its effects are very tangible.

The key to using information as a military capability lies in the information domain. This is because the information domain is the means by which physical domain activity and decision-making interrelate. As such, information content and flow are essential to both the formation of decisions and the execution of decisions as physical activity or behavior. As pointed out by the authors of *Understanding Information Warfare*, the information domain is "ground zero" in the battle for the use of information.[12]

Depiction of the Domains

The domains of conflict are usually depicted as a two dimensional figure consisting of three equal blocks stacked one on top of another. The physical domain is placed on the bottom, the information domain in the middle, and the cognitive domain on top, implying an equality and structural hierarchy between the domains. This is just a visual representation and should not imply anything other than the information domain's role as the linkage between the real world and the human mind. The information domain can justifiably be depicted as a line where the physical and cognitive domains meet, or perhaps as a space created by the overlap between the two domains.

In reality, the relative importance of the domains to military operations is not as a simple as a series of co-equal geometric shapes. For example, the domains' relevance can vary by echelon of operation (i.e., tactical, operational, and strategic). At the tactical level of operations, the nature of the information environment is very physical. Information content is dominated by visual observation and face-to-face human contact. Information flow is greatly impacted by terrain and physical objects. In this environment, IO uses short-range information means and the profile and posture of maneuver forces to change the immediate and short-term behavior of discrete target audiences.

At the operational and strategic levels, the information environment becomes more conceptual – an exchange of broad competing ideas and ideologies. At these echelons, IO uses mass communication means to change mid- and long-term beliefs and attitudes of broad target audiences.

Furthermore, the importance of each domain to military forces may change according to mission and area of operation. During conventional combat operations, the destruction of enemy information systems and networks may dominate non-lethal measures to influence adversary will and decision-making. At the opposite end of the operational spectrum, during peace operations, key leader and populace group perceptions and attitudes may be more important than physical world reality.

Clearly, the two dimensional depiction of the domains has its limitations. To increase its utility, the model can be expanded to three dimensions and scaled to a map for commanders and staffs to use in the planning and execution of operations.

Visualization of the Information Environment

Unlike land, sea, air, and space, the information environment has minimal physical presence. Yet, it is possible to visualize information's effects on military operations by portraying the structure of the information environment in a manner similar to how commanders and staff visualize the physical environments of their operational area.

With the domains of conflict as a framework, the information environment can be analyzed and "mapped" using the military's intelligence preparation of the battlespace (IPB) methodology.[13] This is done by first identifying existing and projected characteristics of the operating environment that are of possible significance to the content and flow of information. Typically, these are aspects of the environment associated with geography, populace, communications infrastructure, media, societal organizations, and third party entities.

Once the significant characteristics are identified, each is then individually evaluated using the three-domain model as a guide. The result is a determination of what each characteristic's affects are on the employment of information systems and networks (the physical domain), the use of information for decision-making (cognitive domain), and information content and flow (the information domain). The individual impacts are then combined to develop an aggregate description of the information environment and plotted on a map of the geographic area to depict where and how information content and flow will affect military operations.[14] (See Figure 3)

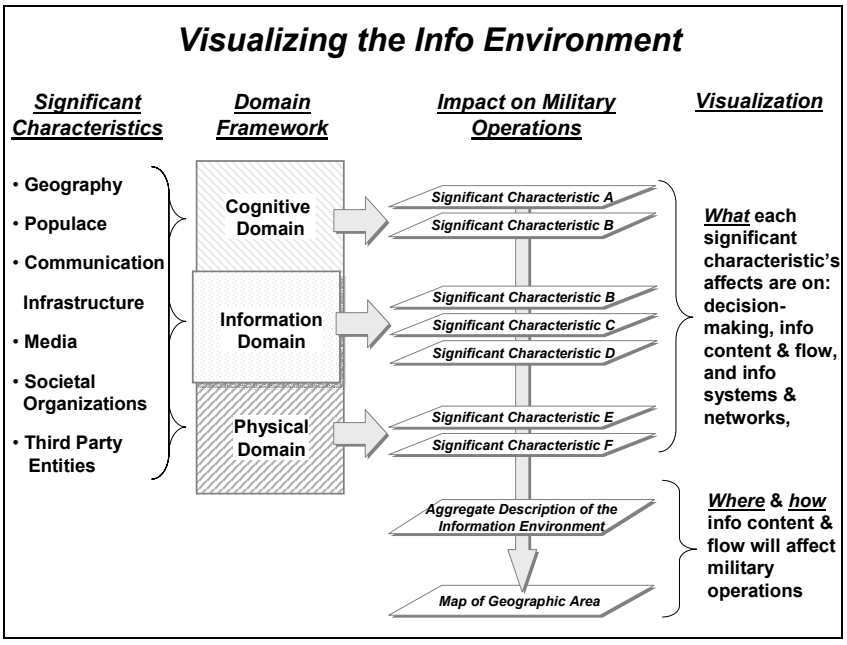

Figure 3 – Visualizing the Information Environment

Depending on the operational area, level of war, and mission, the significant characteristics of the information environment will differ. This is because the information environment is not uniform. Like terrain, the characteristics and impacts of the information environment vary within and between geographic regions. Furthermore, as previously discussed, the relative importance of each domain changes by echelon of operation; becoming less tangible and more conceptual as the level of operations move from the tactical to the strategic. Finally, the assigned mission (i.e., combat, peacekeeping, humanitarian assistance, etc.) determines a military force's relationship to the operating environment and establishes the relative importance of the environment's features to the conduct of operations.

Analysis of the information environment will, in all probability, identify distinct sub-information environments; areas in which the information environment's characteristics and effects are notably different from those in adjacent areas. These sub-information environments, with their unique composition and character affect friendly and adversary military operations in different ways – perhaps favoring one side over another.

The Information Domain

The information domain is the least tangible part of the information environment. Existing at the intersection of the physical and cognitive domains, it is an abstract, non-physical space. Yet, despite its lack of physical presence, the domain, as described by CCRP, can be characterized as having three primary attributes – information quality, reach, and interaction.[15]

Information quality, reach, and interaction are the elements that connect the information domain to the physical and cognitive domains. However, more importantly, the three attributes form the

basis of information's utility to civilian and military organizations. From this perspective, the attributes can be loosely described as follows:

- Information Quality. The value, or worth, of information to an organization in terms of accuracy, relevancy, and timeliness.[16] Organizations require information that is useful to their mission and current situation.

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

- Information Interaction. The quality of information exchange (e.g., face-to-face discussion, radio, print, telephone, computer network. etc.) 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.

Information Needs, Position, and Situation

All organizations need a constant flow of relevant, accurate information to operate successfully.[17] An organization's information needs are defined as "the measurable set of information required to plan and/or execute a mission or task."[18] The information an organization possesses at any point in time is its information position. Needs and position can both be expressed in terms of information quality, reach, and interaction, and depicted as a three-dimensional volume (see Figure 4).

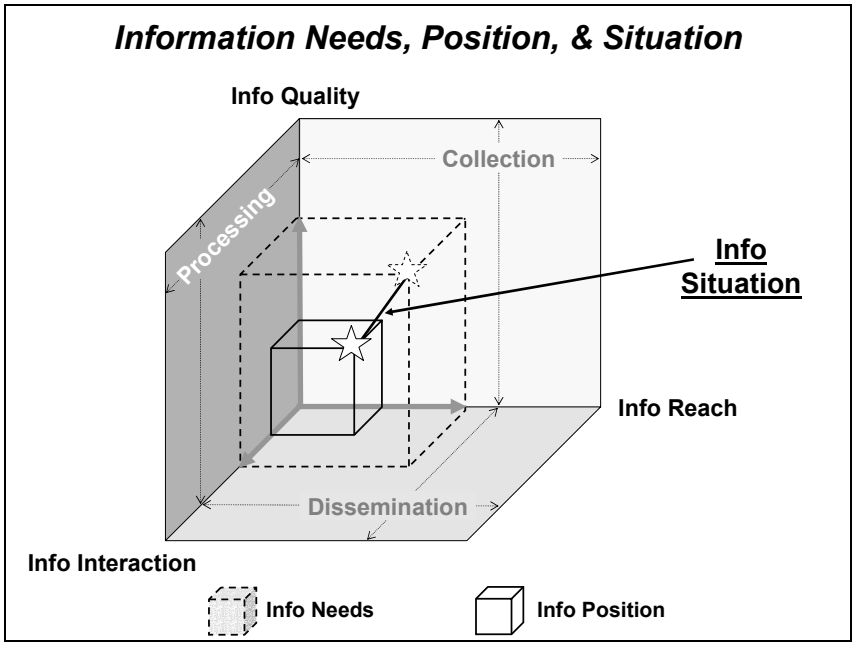

Figure 4 – Information Needs, Position, and Situation

Because an organization is unlikely to possess all the information it requires to operate, there will always be a disparity between its information needs and position. This gap is its information situation. Information situation constantly fluctuates because needs and position change with each mission and over time. Generally, organizations will be in a deficit information situation, especially military forces engaged in combat operations. The challenge for an organization is to reduce the disparity between information needs and position as much as possible.

Although information needs, position, and situation may aptly describe information's utility to organizations, it does not explain what an organization does to maintain or improve its information situation. To change focus from the possession of information to how organizations operate in the information domain, it is necessary to consider the planes formed by the three axes (i.e., information quality, reach, and interaction). To this end, the three planes can represent information system functions: information collection = quality and reach; information processing = quality and interaction; and information dissemination = reach and interaction. Together, these functions can represent how an organization maintains or improves its information situation.

Information Advantage

Information and the information environment are not benign. The possession and use of information can provide a marked advantage to an organization relative to its opponents. Therefore, organizations not only collect, process, and disseminate information to meet their own information needs, but also, when in a competitive situation, to gain and maintain an advantage over an opponent.

CCRP defines information advantage as the ability to use information better than one's opponent. A non-doctrinal term, information advantage means being in a superior information situation relative to another, perhaps opposing, organization. Information advantage is determined by comparing the disparity between each side's information situations. As pointed out by CCRP, "information situation can be described in terms of the volumetric difference between needs and position."[19] For a simple illustration, see Figure 5.

Information advantage is relative. Even though two organizations may occupy the same operating environment, they are unlikely to have the same information needs, position, and situation, or the even the same capabilities to use the information domain. Therefore, information advantage is measured in terms of one's own information situation relative to that of the opponent. Furthermore, because characteristics of the operating environment impact different organizations in different ways, relativity extends to how the information environment affects opposing organizations.

An information advantage can be created by the ability to use information better than one's adversary, the reduction of the adversary's information position, and the leveraging of the information environment for one's own purposes. Which ever methods are used to produce an information advantage, both the content and flow of information must be addressed if an exploitable information advantage is to be realized.

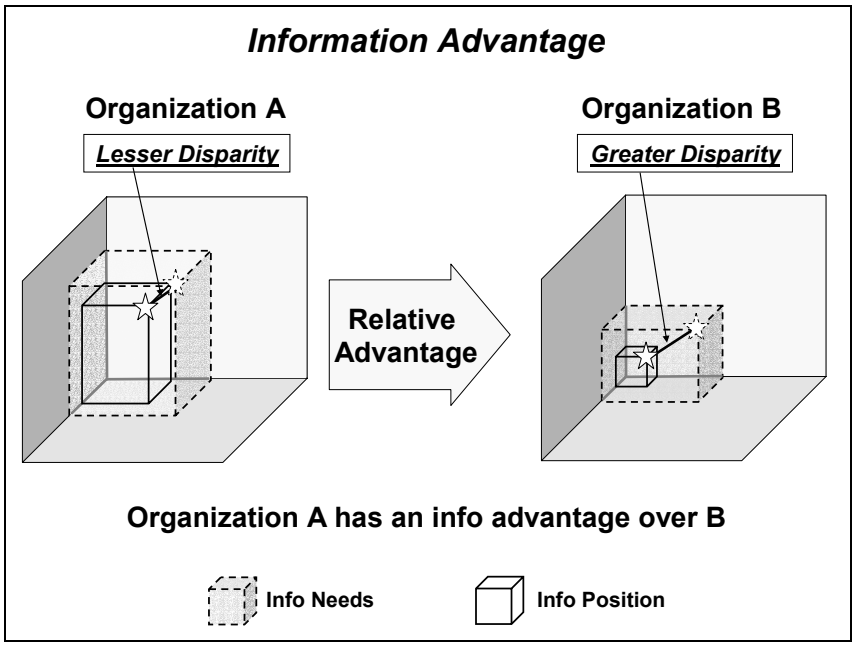

Figure 5 – Information Advantage

Information Superiority

Information superiority is the least understood term associated with IO.[20] Definitions and differing perspectives abound. A useful definition in use by the U.S. Army is "the operational advantage gained by the ability to collect, process, and disseminate an uninterrupted flow of information while denying an adversary's ability to do the same."[21] Therefore, information superiority results from an information advantage.

Conceptually, this relationship between information advantage and superiority fits well with the three domains of conflict. Affecting information content, flow, and use leads to the ability of one force to use the information domain better than its opponent – an information advantage. As a consequence of this advantage, that force can then gain an exploitable result – information superiority.

The operational advantage resulting from information superiority can manifest itself in two general ways – in the physical domain as a force or position advantage, or in the cognitive domain as decision-making advantage (see Figure 6).[22] However, an advantage in the information environment does not automatically equate to information superiority. An operational advantage will only result from information advantage if it is achieved for a specific purpose.

Both information advantage and superiority are localized and transitory conditions. This is because the respective information situations of opposing forces, as well as information content and flow in, and through, a specific geographic area are not static. Therefore, to have value to a military force, information advantage and superiority are sought at certain places and times in the operational area.[23]

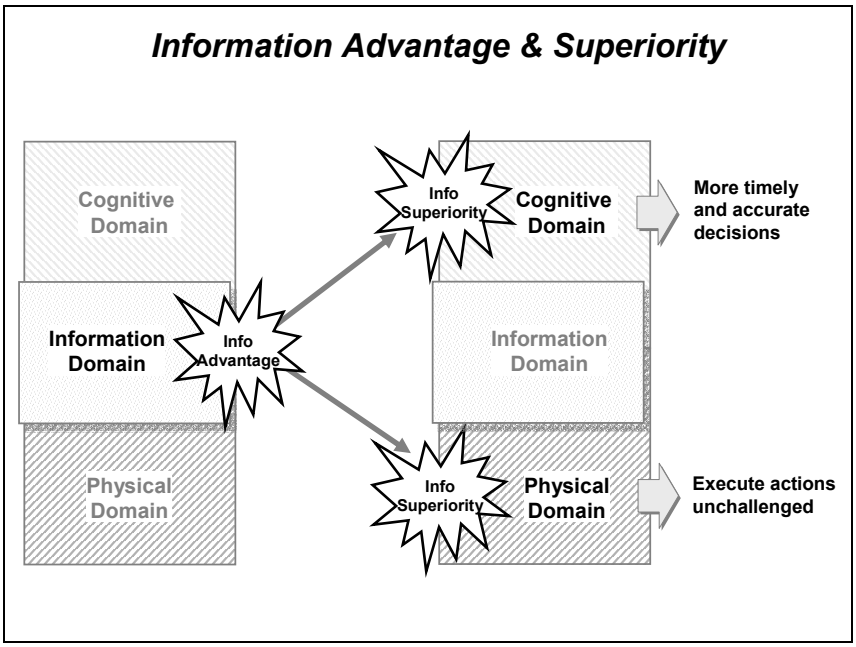

Figure 6 – Relationship between Information Advantage and Superiority

Conclusion – What are Information Operations?

As mentioned in the introduction, IO can be described as activities to impact the content, flow, and use of information within a specific geographic area in order to gain an operational advantage over an adversary. The purpose of any information operation is information superiority – an operational advantage resulting from the use of information that supports mission achievement. While IO operates in all three domains of the information environment, to be effective it must focus on the information domain where an information advantage is achieved. Thus, the broad objective of IO is information advantage.

The creation of an information advantage is linked to specific activities in the physical world. IO is conducted by affecting and protecting the means of information content and flow in the physical domain (i.e., information systems and networks). These actions are directed at impacting information content and flow, and affecting the adversary's functions in the information domain (i.e., information collection, processing, and dissemination). This manipulation of the information domain and attacking of adversary information capabilities creates an information advantage, that when synchronized to other military operations provides information superiority at a specific place and time in either the cognitive (i.e., a decision-making advantage) and physical domains (i.e., a force advantage).

To produce an information advantage, IO must impact both the content and flow of information critical to the adversary forces and any other entities in the operational area. Activities that address information content while ignoring how that content flows will fail to attain an information advantage. Likewise, impacting the way information flows without regard to its content will not yield an exploitable information advantage.

While IO is not the sole contributor to information advantage and superiority, it is the means by which a military force actively uses information to reduce an adversary's information position and creates effects that leverage the characteristics of the information environment to the forces' own advantage. In a military context, this duality of operations is analogous to "fires and maneuver," where *fires* equates to a direct engagement of an opponent's information position in order to reduce its ability to meet its information needs, and *maneuver* consists of activities to affect information content and flow with the information domain for the purpose of achieving a positional advantage in the information environment.

It must be recognized that the three domain model is not exclusive to the information environment. All military operations, not just information operations, occur within the framework of these domains. Every military action has the potential to convert information into a military capability, and any asset or capability that can affect content and flow of information is a possible contributor, or even detractor, to an information operation. For this reason, IO should not be viewed as a stand-alone operation or finite, discrete set of assets and capabilities. Therefore, at a minimum, IO should represent all methods and means that can impact the information environment. At its maximum, it is an approach to conducting military operations.

---

[1] Joint Publication 1-02, *DOD Dictionary of Military and Associated Terms*, 30 November 2004, available on-line at the Joint Electronic Library: www.dtic.mil/doctrine.

[2] The two CCRP works are *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., 2001) and *Effects Based Operations: Applying Network Centric Warfare in Peace, Conflict, and War* by Edward R. Smith (Washington, D.C.: DoD Command and Control Research Program, 2002). For an earlier, but comparable, discussion of the need for a model for IO, see *Toward a Functional Model of Information Warfare* by L. Scott Johnson (*Studies in Intelligence*, Volume 1, Number 1, 1997).

[3] *Understanding Information Age Warfare*, page 12.

[4] Ibid.

[5] Ibid.

[6] The nature of information is often explained by three views of information – information as message, medium, and matter. As a concept, *information-as-message* regards information as a message or signal that contains meaningful content. *Information-as-medium* views information as a system, or perhaps means, by which data and information are created, manipulated, and exchanged. The third view – *information as physical matter* – is an emerging concept that is not as yet widely accepted. For a 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.

[7] The discussion of the three domains and the figure of information environment are adapted from previous work in the articles "Visualizing the Information Environment" by Marc J. Romanych (*Military Intelligence Professional*

Bulletin, Volume 29, Number 3, pages 5-8) and "A Theory-Based View of Information Operations" by Marc J. Romanych (*IO Sphere*, Spring 2005), pages 12-16.

[8] For further discussion of the information domain's existence at the intersection between the physical and cognitive domains see Bryan N. Sparling's *Information Theory as a Foundation for Military Operations* (Fort Leavenworth, Kansas: Scholl of Advanced Military Studies, US Army Command and Staff College, 2002), pages 12-19.

[9] Alberts et al states that "all contents of the cognitive domain pass through a filter or lens we have labeled human perception. This filter consists of the individual's world view, the body of personal knowledge the person brings to the situation, their experience, training, values, and individual capabilities" (*Understanding Information Age Warfare*, page 13). In *Power to the Edge*, (DoD Command and Control Research Program, Washington D.C., 2003), authors David Alberts and Richard Hayes briefly introduce a social domain into the model, but only briefly discuss the domain in the context of command and control and interoperability of allied forces.

[10] Possible broad elements of culture that are relevant to military operations are language, religion, ethnicity, and nationality.

[11] This discussion is adapted from "A Theory-Based View of Information Operations" by Marc J. Romanych.

[12] *Understanding Information Age Warfare*, page 12.

[13] This discussion is based on "Visualizing the Information Environment" by Marc J. Romanych (*Military Intelligence Professional Bulletin*, Volume 29, Number 3) and "Mapping the Information Environment" by Robert Cordray III and Marc Romanych (an article under consideration for publication with *IO Sphere*).

[14] This product is analogous to the graphic products, such as a Modified Combined Obstacle Overlay (MCOO), produced by the intelligence staff to help the commander visualize the militarily significant aspects of the physical environment.

[15] The discussion of information quality, reach, and interaction is a summation 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 military operations, these terms were modified.

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

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

[18] *Understanding Information Age Warfare*, p. 103.

[19] Ibid, p. 107.

[20] Numerous definitions of information superiority are in use and the terms "information advantage," "information superiority," and "information dominance" are frequently interchanged.

[21] FM 1-02, *Operational Terms and Graphics*, (Headquarters, Department of the Army, Washington, D.C., 21 September 2004). The Army definition was selected over the DoD definition – "That degree of dominance in the information domain which permits the conduct of operations without effective opposition." – because of its inclusion of a vague definition for an information advantage.

[22] An operational advantage only has utility if it occurs where military forces exist – in the physical domain of combat operations or in the cognitive domain of military decision-making.

[23] Because information superiority is not sought everywhere or all the time, the different characteristics of the operational area's sub-information environments must be recognized and considered in order to accurately focus the information operation.