The Information Sphere Domain Increasing Understanding and Cooperation

Dr. PATRICK, D. ALLEN and Dennis P. GILBERT, Jr
Johns Hopkins University, Applied Physics Lab
Booz Allen Hamilton

Abstract. Recent discussions regarding the emerging field of cyber warfare have focused on the term "cyberspace," and have included cyberspace as being considered its own war fighting domain, much like air, land, sea, and space. In this stage of the Information Age, the international community is grappling with whether it needs to define this information realm as a domain, similar to the air, land, sea, and outer space domains that already exist. History shows that there is always an advantage in a conflict to the side that *understands and operates* within a domain better than the opponent. In this paper, the authors propose a definition of a domain, define what constitutes a domain, posit how new domains are created over time, and describe the features of what is and is not a domain. These definitions and features lead to our proposal that the "Information Sphere" should the preferred international term, and it is this "InfoSphere" that qualifies as a new domain, with features both similar to and different from the four existing physical domains.

Keywords. domain, information, cyber, cyberspace

Introduction

Since classical times, two domains of operation dominated military and civilian operations: land and sea. The advent of powered flight in 1904 initiated the opportunity for a third domain. Shortly thereafter, actions by opposing elements in this airspace began during World War I. The Army and Navy each developed its own air capabilities, and at the end of World War II, the Army Air Corps became the US Air Force—about 50 years after the first powered flight. In a similar manner, the dawn of the "space age" in 1955 encouraged each of the U.S. military services to invest in their own efforts in the space domain. By the mid to late 1980's, with the advent of then US President Ronald Reagan's Strategic Defense Initiative (SDI), the US DoD acknowledged outer space as a fourth war fighting domain.

Based on the preceding observations, the historical trends for recognizing new domains tend to follow this sequence:

- First, the *capability* to begin to operate in that domain is developed, such as the first powered flight or the first space flight.
- Second, the capabilities to operate in that domain become relatively *commonplace*, such as air travel or Shuttle launches.

- Third, the capabilities in that sphere *to affect capabilities* in that domain and in the other domains become recognized and exploited.
- Fourth, sufficient recognition of the *unique and synergistic* nature of capabilities in the domain are recognized and further developed.
- Finally, *institutional and financial support* for the domain is developed.

1. Definition of a Domain

While considerable dialogue and research has been conducted on the subject, there does not appear to be an US military definition, NATO definition, or internationally agreed upon definition for a domain. Joint Publication 1-02, the Department of Defense Dictionary of Military and Associated terms, does not define a domain. In the absence of an internationally-accepted definition, we propose a definition of a domain, and describe features or criteria that distinguish one domain from any other domain in order to help frame the discussion about whether to define the Information Sphere as its own domain.

The Webster's New Collegiate Dictionary has two relevant general definitions of a Domain:

1. A territory over which rule or control is exercised.
2. A sphere of activity, interest, or function.

Webster further defines a sphere as an area or range over or within which someone or something acts, exists, or has influence or significance, such as the public sphere.[1] Note that while the definition of a sphere does include physical environments, it also includes non-physical environments. Following this train of thought that a sphere or domain does not have to be a physical domain, it is comprehensible that a sphere can also apply to area or range in which something acts, exists, or has influence or significance.

Using these definitions as a guide, we derived the following definition for a domain for consideration by NATO countries:

> *The sphere of interest and influence in which activities, functions, and operations are undertaken to accomplish missions and exercise control over an opponent in order to achieve desired effects.*

By breaking down this definition into its component parts, we can support that each of the existing four physical domains (air, land, sea, and space) qualifies as a domain, as defined above. The key components of our proposed definition of a domain are:

- It is a sphere of interest
- It is a sphere of influence in that activities, functions, and operations can be undertaken in that sphere to accomplish missions
- It is a sphere that may include the presence of an opponent
- It is a sphere in which control can be exercised over that opponent

Based on the above components, it is clear that the four physical domains of air, land, sea, and space each qualify as a domain. Each has its own sphere of interest and sphere of influence. Aircraft fly missions, ships navigate the waterways (both surface and subsurface), ground forces take and secure terrestrial objectives, and satellites orbit the earth. In each of these physical domains an opponent can be present and can interfere with friendly operations. Moreover, the NATO members have military capabilities in each of these domains, which can be used to control and dominate potential adversaries.

2. Features of a Domain

The authors offer for discussion what they consider are the six key feature of a domain:

1. Unique capabilities are required to operate in that domain
2. A domain is not fully encompassed by any other domain
3. A shared presence of friendly and opposing capabilities is possible in the domain
4. Control can be exerted over the domain
5. A domain provides the opportunity for synergy with other domains
6. A domain provides the opportunity for asymmetric actions across domains

The authors posit that if a domain has these six features, it qualifies as a domain, and if it does not have all six features, it should not qualify as a domain. This checklist of features can then be used as criteria to determine whether a new realm, such as the Information Sphere, qualifies as a domain. The following examples show how the four physical domains of air, land, sea, and space qualify as a domain according to these six features:

1. <u>Unique capabilities are required to operate in that Domain</u>. For example, aircraft are required to operate in the air domain, spacecraft for the outer space domain, ships for the sea domain, and land systems for the land domain. Note that each of these capabilities can readily differentiate themselves from capabilities in other domains.

2. <u>A Domain is not fully encompassed by any other single Domain.</u> For example, the air domain is not encompassed by the land domain, or vice versa. The capabilities, missions, and dominance techniques of the capabilities in each domain remain unique. A tank is not intended to operate in the air domain, while an airplane is not designed to operate underwater.

3. <u>A shared presence of friendly and opposing capabilities is possible.</u> Any domain can potentially be entered by opposing forces. This is not to say that every opponent is present in every domain, but that an opposing presence must be *possible* for the sphere of interest and influence to be considered a domain. *A potential shared presence* is an essential feature of a domain since dominance or control over the domain requires the possibility of an opposing presence or capability.

4. Control can be exerted. The presence of a potential opponent in the sphere of interest generates the need to influence or dominate such opponents in a domain. Since a domain is a sphere of influence as well as of interest, then it must be possible for one side's influence in a domain to dominate an opposing side's influence.

5. Provides opportunities for synergy. The capabilities in a domain must be able to provide synergistic opportunities with capabilities in other domains. The classic US Military's "Air-Land Doctrine" was an excellent example of how the capabilities of the land and air domains could be mutually supportive.

6. Provides asymmetric opportunities. Similar to synergistic opportunities are the opportunities for capabilities in a domain to gain an asymmetric advantage over opposing forces in other domains. For example, the US Army's Joint Fires Doctrine emphasizes the opportunity to use air assets as an asymmetric threat against opposing land and sea assets, while land or sea forces can be used to asymmetrically threaten enemy air assets. The principle of asymmetry must be a possibility for capabilities in a sphere of interest for it to be defined as a domain.

3. Proposed Definition for the Information Sphere's Domain

We will next address whether the Information Sphere qualifies as a domain, but first we have to provide a definition for the Information Sphere. Current DoD doctrine defines the Information Environment as "the aggregate of individuals, organizations, or systems that collect, process, or disseminate information; also included is information itself."[2] Regrettably, this definition puts the emphasis on the physical attributes of an information environment. In other publications, the Information Domain has been described as "the domain where information is created, manipulated, and shared," or "where information lives." These same authors have defined the Cognitive Domain as the "domain of the mind of the warfighter and the warfighter's supporting populace."[3] With this approach, the content, the connectivity, and the message have been segregated. We purport that these definitions diverge from the goals of the Information Operations mission area and the common understanding of Strategic Communication. Therefore, we first propose a definition of the Information Sphere, and second, for the Information Sphere's domain.

The definition we propose for the *Information Sphere* is:

The space defined by relationships among actors, information, and information systems.

To further elaborate on this definition, we also define actors, information, and information systems:

An actor may be a sender, liaison, modifier, transferor, or recipient (either intended or unintended) of information. Information is the data being passed among actors via information systems. An information system is any information

> *perceiving system, information storage system, or communications system, (including couriers).*

Based on these definitions, we propose a new definition for the domain we call the *Information Sphere*:

> *The space of relationships among actors, information, and information systems that form a sphere of interest and influence in or through which information-related activities, functions, and operations are undertaken to accomplish missions and exercise control over an opponent in order to achieve desired effects.*

Note that the information by itself is not the domain, nor is the domain simply the information systems in which the information rides and resides. It is the space defined by the relationships among actors, information, and information systems that define the Information Sphere and allow it to qualify as a domain. We include the word “sphere” in the Information sphere to distinguish the fact that the domain we are proposing consists of more than just the information component, and calling it the “information domain” would encourage that misunderstanding. The other accepted domains do not use the term “the air sphere” or the “sea sphere,” but we use “Information Sphere” to make the distinction from just the information component completely clear.

This definition is different from the previously referenced definitions for the cognitive, information, and cyber domains because the proposed definition of the Information Sphere explicitly includes the relationship among these three components. It is the *relationships* among these three components that define the meaning, context, and value of the Information Sphere, not the three components taken in isolation.

The US Military’s Quadrennial Roles and Missions Review Report defines cyberspace as “a global domain within the information environment consisting of the interdependent network of information technology, infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.”[4] We believe that this is a good definition of cyberspace, but believe that cyberspace is still a subset of the larger Information Sphere domain. Just as naval surface actions and submarine actions are two components of the Sea domain, cyberspace, cognitive, and information are components of the more encompassing Information Sphere.

4. The Evolution of the Information Sphere as a New Domain

As mentioned above, there are five steps that capabilities in an environment tend to follow en route to becoming a new domain:

1) The *capability* to begin to operate in that domain is developed. From the advent of the PC and the birth of the public version of the Internet, communication and information capabilities have exploded. Combined with global transportations, these capabilities provide a global economy and social interactions to a degree previously unheard of.

2) The capabilities to operate in that domain become relatively *commonplace.* Fourth Generation cell phones, PCs, and Internet access are now commonly found almost everywhere in the world. Nations that have yet to develop their communications

infrastructures are jumping straight to fourth generation access that does not require the construction of expensive information infrastructures. Almost anyone in the world can achieve global communications via the Internet and cell phones.

3) The capabilities in that sphere *to affect capabilities* in that domain and in the other domains become recognized and exploited. Information has always been important to military and civilian operations. The Information Age has made the Information Sphere not only widespread but also *shared*. Opponents can reach our internet-connected networks without leaving their own country. There are few places in the world where the news media do not reach. Incidents in the remotest parts of the world often carry global implications beyond any time in previous history. As a result, conflict in the Information Sphere is becoming more prevalent and more important than even direct military action in many cases.

4) Sufficient recognition of the *unique and synergistic* nature of capabilities in the domain are recognized and further developed. As both the capabilities and threats in this sphere continue to grow, more and more resources are being allocated to the exploitation and securing of Information Sphere capabilities.

5) Sufficient *institutional and financial support* for the domain is developed. The US's efforts to create a new Sub-Unified Command for Cyber is one example of efforts toward developing the necessary institutional and financial support for operating and succeeding in the Information Sphere. The future may be an US Interagency organization, or even an international megacommunity, that represents the Information instrument of national power, along with the Diplomatic, Military, and Economic instruments. Note that the bringing together of Information Sphere capabilities from the other instruments of national power (including military) is the logical progression we would expect to see as the Information Sphere domain becomes institutionalized and supported financially.

5. What is Unique About the Information Sphere's Domain?

Now that we have described why the Information Sphere qualifies as a domain, this section will describe why the Information Sphere is also unique compared to the four physical domains. At the same time, we will describe why we believe that what makes the Information Sphere unique is yet one more reason why the Information Sphere should be treated as a new domain.

Since the definition of the Information Sphere includes actors, information, and information systems, it is evident that each of these three components must reside in a physical medium at any point in time. For example, an information server is located either on the ground, underground, in the air, in outer space, on the sea, or (potentially) under the sea.

In a similar manner, the information itself is either being stored on an information system, or is in some information conduit (including a portion of the electromagnetic spectrum) at any point in time. Finally, the human actors must be located in one of the four physical domains. Figure 1 gives an example of how one might consider the information sphere's domain with respect to the four physical domains.

Note that this figure shows that the Information Sphere is separate from each of the four physical domains, but is also accessible by, and provides access to, all four. Information may enter or exit via a physical medium, but that may or may not be relevant. For example, if an intruder is seeking an entry point into a network, the physical location of the entry point may matter to the intruder. However, once the intruder is in the network, the physical location of the entry point and any informational areas of interest are of less importance due to the degree of access provided by the network. What is important in this case is the relationship between security elements of the network (including people), the targeted information, and the intruder, rather than the physical location of the assets.

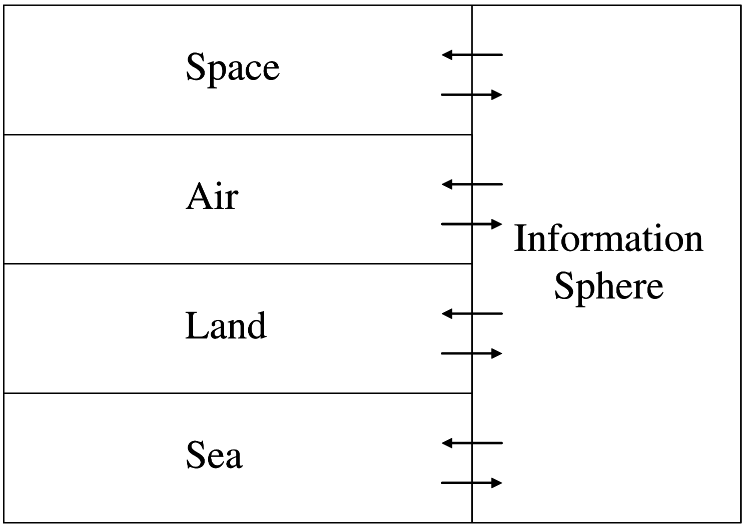

Figure 1. Information Sphere is a Unique Type of Domain[5]

Note that the concept of entry and exit points from one domain to another is prevalent in all domains. Aircraft and spacecraft land on the ground or at sea. Ships dock at land-based ports. The same is true for the Information Sphere. There will always be entry and exit points from the Information Sphere to and from the other domains, as the purpose of most activity in the Information Sphere is to affect something in the physical world. However, there are also actions and desired end states associated with operations *within* the Information sphere that are unique to the Information Sphere, irrelevant to and unaffected by the physical space in which the actors, information, or information systems actually reside.

Each domain has actions that are dependent and independent of each of the other domains. Similarly, *the Information Sphere is not completely encompassed by any physical domain*. For example, a distributed database that has elements either residing or in transit on land, in the air, on the sea and/or in outer space is not contained or fully encompassed by any of the four media in which it is located or passes through.

Moreover, *even the union of air, land, sea, and space physical environments does not fully encompass the Information Sphere*. The interactions we described for the Information Sphere often occur in a space of relationships where the physical location of the actual components is irrelevant once access has been achieved. For example, the ability for two actors to interact in some way does not depend on the medium or media within which the information exchange occurs. What matters are the interaction and the relationship between the actors, information, and information systems? Moreover, shared presence within all four physical domains does not equate to dominance in the Information Sphere, either in the control of information access, information systems, or in the beliefs and perceptions of groups of interest within those four domains.

It is these relationships between actors, information, and information systems that define the interest and influence mechanisms in the Information Sphere. Since these relationships can be satisfied by a wide range of paths into, out of, and through various physical media, the value, benefit, and vulnerability of elements within the Information Sphere are relatively independent from the four physical domains.

Another important distinction is that the *desired effects* of an information activity *eventually* reside in one or more of the four physical domains. For example, the information activity may be to bring down an enemy air defense system, which opens the way for the air operations, which shapes the upcoming ground or sea battles. However, there may be a significant delay between the initial information activity and any effect in one or more physical domains. For example, the placement of a back door on a target server does not have an immediate effect other than the opportunity for access at a later date. Until that access is exploited, there is no physical manifestation of a desired effect.

As another example, competition between opposing thoughts or beliefs frequently has a delayed reaction. The concept of freedom, for example, is often dormant until the opportunity to be free, or to achieve increased freedoms, becomes available. In the conflict among beliefs, a thought that is planted may blossom many years later after additional thoughts and physical events have occurred.

Therefore, the fact that the actors, information systems, and information that comprise the Information Sphere must reside at any instant in one of the four physical domains is either secondary or irrelevant to the functioning of the abstract relationships within the Information Sphere. Information easily transcends the barriers between the physical domains. The Information Sphere is a space where the understanding of relationships in that space can lead to dominance over opponents in that space.

6. The Information Sphere's Qualifications as a Domain

We argue that the Information Sphere qualifies as a domain according to our preceding definition for the following reasons:

- The space of relationships among actors, information, and information systems forms a sphere of interest
- It is a sphere of influence in that activities, functions, and operations can be undertaken in that sphere to accomplish missions
- An opponent to friendly operations may function in that sphere
- Control can be exercised over that opponent in or through that sphere

Besides meeting the four preceding criteria described above, the Information Sphere also meets each of the six features required of a domain.

1. Unique capabilities are required to operate in that Domain. Information capabilities are required to operate in the information realm. The Information Sphere requires unique equipment and personnel skills to function effectively, accomplish missions, and dominate any enemy presence. Information capabilities operating in the Information Sphere are both unique and differentiable from the capabilities designed to operate in other domains. For example, a computer system (and associated software/code) optimized for hacking into enemy computer networks is a unique asset different from air, land, sea, and space platforms. Hacking skills are unique from the more traditional set of pilot, sailor, soldier, and astronaut**.**

As information capabilities become more specialized, the uniqueness and differentiability of these capabilities will continue to grow. For example, the Information Sphere now has a set of unique equipment (materiel) and personnel skills required to effectively operate in, defend, and attempt to dominate the domain. With these new capabilities comes a range of unique support structures, such as doctrine, organization, training, leadership development, facilities, and policy.

2. A Domain is not fully encompassed by any other single Domain. The Information Sphere is not fully encompassed by any combination of land, sea, air, or space domains. The Information Sphere has capabilities and functions that are meaningful only in this information environment.

3. A shared presence of friendly and opposing capabilities is possible. Until recently, the Information Sphere rarely allowed for *a shared presence*. A shared presence was not feasible primarily due to physical and geographical separation and the inherent time delays. With the birth of the Information Age, however, the Information Sphere is frequently shared. Examples of this sharing include the range of information media, including the Internet, local and wide area networks, television, radio, print media, video and audio recordings, and other capabilities. Due to the explosion of information and information capabilities, the Information Sphere allows for a shared presence more than ever before. As a result, dominance and control in this domain have become much more important than in the past.

4. Control can be exerted. For the Information Sphere, control can refer to the control of the information systems in a region of the information sphere, control to the access of the information in that information sphere, or even the dominance of one belief over another in a region of the information sphere. As an example, air-to-air radars on fighter aircraft may try to jam or spoof the radars of opposing forces in the air domain, thereby attempting to control the information sphere. The recent spate of alleged nation-state sponsored hacks into sensitive but unclassified US military and contractor information systems is an example of the type of temporary but useful control our opponents can undertake in the Information Sphere.[6] Influence over population groups is a constant competition in the Idea Battlespace among ideas vying for dominance over other ideas.[7]

5. Provides opportunities for synergy. The Information Sphere provides synergistic support to all the other domains, and vice versa. The ability to gather information directly from an enemy information source can assist air, land, sea, and space operations. Conversely, the ability to take out an enemy information system from the

air can force the enemy to use an information system already compromised by our side.[8]

6. Provides asymmetric opportunities. Information capabilities can provide an asymmetric threat against enemy capabilities in other domains. In his book, *The Next World War*, James Adams[9] describes a case where a computer virus was entered into a printer that was supposed to be delivered to an enemy site in order to neutralize an enemy air defense system. In a similar manner, physical assets can be used to disrupt and destroy opposing information systems.

7. Benefits of Treating the Information Sphere as a Domain

First, there is always an advantage in a conflict to the side that *understands and operates* within a domain better than the opponent. This is true on land, air, sea, and space, and can also be true in the Information Sphere. Obtaining dominance in the Information Sphere will likely lead to continued dominance in the four physical domains via asymmetric effects. By defining the Information Sphere as a domain, a body of knowledge or military science of operating in the Information Sphere will be more thoroughly developed to improve understanding and consensus on the subject.

Second, *representing* the relationships of information among actors and information systems in a manner useful to planners and decision makers will help improve the effectiveness and efficiency of operations in and through the Information Sphere. For example, the ability to readily visualize relationships in a common format will facilitate a unity of effort and common understanding of objectives and constraints. Defining the Information Sphere as a domain should lead to an investigation and experimentation on a number of methods to represent these relationships, and the best-of-breed methods should emerge to enhance our capabilities in this domain.

Third, focusing and *preparing enhanced capabilities* in the Information Sphere will enable superior *influence and control* in this domain. The side with better personnel, equipment, doctrine, organizations, and leadership will have a significant advantage over the opposition. If the military departments of NATO countries choose to define the Information Sphere as a formal war fighting domain, then the resourcing to more effectively and efficiently function in that domain should follow.

Fourth, defining the Information Sphere as a domain allows for increased emphasis on *planning and employing* all instruments of national power—diplomatic, informational, military, and economic—in a common, coordinated endeavor. Since information is a common element in the use of all instruments of national power, the ability to function effectively in this domain will encourage the coordination and synchronization of effects among all these instruments.

Fifth, defining the Information Sphere as a domain will help increase the emphasis on improved *information assurance and cyber security*, which can and should lead to improved economic and national security. Defining the Information Sphere as a domain will help define the common areas of interest between these sectors, and eventually lead to common, or at least coordinafted, resourcing in the areas of information security.

Finally, defining the Information Sphere as a domain can help *focus international efforts* on the important conflicts already ongoing in this domain. In addition to the skirmishes in cyberspace, the battle for the hearts and minds of many groups of actors worldwide has been raging since the birth of philosophies and political systems. In a battle of the minds, the physical location of the people believing in something is less important than the dominance of that belief over other competing beliefs. Defining the Information Sphere as a domain will help highlight the need for renewed effort and capabilities in this cognitive realm.

8. Summary

This paper presented the definition and features of a domain, a definition for the Information Sphere, and why the Information Sphere qualifies as a domain along with the four physical domains of air, land, sea, and space. The paper also presented why the Information Sphere has some distinct differences from the four physical domains, and the benefits of treating the Information Sphere (which includes cyberspace) as its own domain. Lastly, the paper describes why the Information Sphere is a comprehensive domain that encompasses the areas of cyberspace, cognition, personnel, and information itself, which is why we include the term “sphere” in the definition. Referring to this new area as the “Information Domain” would imply that the focus of this domain is focused just on the information component, which does not adequately capture the full scope of the new proposed domain: the “Information Sphere Domain.”

References

[1] http://www.merriam-webster.com/dictionary/sphere; accessed 14 January 2009.

[2] Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms (Washington D.C.: U.S. Government Printing Office, 12 April 2001), page 203.

[3] Alberts, David S., Gartska, John J., Stein, Frederick P., Net-Centric Warfare-Developing and Leveraging Information Superiority (DoD C4ISR Cooperative Research Program, 2nd Edition (Revised) August 1999.)

[4] Gates, Robert M., Quadrennial Roles and Missions Review Report, Department of Defense, January 2009, http://www.defenselink.mil/news/Jan2009/QRMFinalReport_v26Jan.pdf, accessed 1 February 2009.

[5] Allen, Patrick D., Information Operations Planning (Artech House, New York, 2007), p. 298

[6] Wortzel, Larry M.,Chairman, et al., 2008 Report to Congress (U.S.-China Economic and Security Review Commission, Washington, 27 October 2008), http://www.uscc.gov, accessed 25 November 2008.

[7] Allen, op cit., p. 114

[8] Koch, Andrew, Information warfare tools rolled out in Iraq, (Janes’ Defense Weekly, Washington, 6 August 2003)

[9] Adams, James, The Next War, Simon and Schuster, New York, 1998.