General Dominance Theory

A Foundation for Information Dominance

Originally written in May 2014 for *Proceedings* (not published). Revised July 2014.

LT Jacob Foster Davis, USN

LT Davis, a native of Little Rock, Arkansas, is a former Adjunct Professor of Cyber Security at the US Naval Academy and former Surface Warfare Officer. He currently serves at Navy Information Operations Command, Maryland as an Information Warfare Officer. He holds a B.S. in Information Technology, USNA Class of 2007, and an M.S. in Systems Technology, Naval Postgraduate School, 2008.

General Dominance Theory

A Foundation for Information Dominance

In the U.S. Navy's Intelligence community, the concept of achieving "Information Dominance" is very popular. With the advent of computer and communications technology as both a tool and a weapon, we rightly see the Information Domain as the next frontier of military power. Accordingly, we work hard to gather and process information hoping to achieve a strategic advantage over our adversaries.

But there is a problem. And it is not a want of trying. Our problem is that our community has failed to properly define Information Dominance and other key terms. Consequently, we've put the cart before the horse. While we all agree that we need Information Dominance and have expended countless man-hours and resources pursuing it, we've failed to properly rein in the concept by precisely addressing what "Information Dominance" actually means. And this problem is easy to see. I would guess that if you asked 10 people in the intelligence community to define Information Dominance, you would get 15 answers.

In order to effectively strive to achieve and maintain dominance in the Information Domain we must have clear and proper definitions based on the philosophical objective of war: to make our *desired* image of reality the *actual* reality. Clear and proper definitions enable us to establish criteria that can be used to measure our progress. Additionally, these definitions will help us better allocate scarce resources (e.g., people, material, time, expertise) in tasks that support achieving dominance.

This article introduces definitions and concepts into the field of Information Dominance to add to our armamentarium. Most importantly, I propose re-defining[1]

---

[1] *U.S. Navy Information Dominance Roadmap 2013 – 2028* (March, 2013) defines Information Dominance as "… the operational advantage gained from fully integrating Navy's information capabilities, systems and resources

Information Dominance as "*the state in the battle space where a desired image of Information reality can be achieved completely despite the will of an opponent.*" Rather than an *advantage* gained in an environment *independent* of opponents, Information Dominance should be viewed as a *state* that *depends* on our ability to operate against opponents. I also propose a definition of Information Warfare: *"the pursuit of Information Dominance."*

These definitions were developed using a theory called General Dominance Theory.[2] The first part of this article serves as an introduction to that theory. The second part shows how the principles General Dominance Theory can be applied to derive these definitions and provide guidance toward pursuing Information Dominance.

The principles of General Dominance Theory, as applied to Information Dominance, support the ideas presented in the US Navy's *Navy Strategy for Achieving Information Dominance, 2013–2017* and *U.S. Navy Information Dominance Roadmap, 2013–2028.* But those documents don't discuss any of the founding principles and logic behind their conclusions. General Dominance Theory fills the resultant void that begs, "Why?" The major ideas presented by the Navy are calls to action and organization that logically flow from the principles of General Dominance Theory. Therefore, it is important that we understand and refine General Dominance Theory.

Part I: General Dominance Theory

Before we consider Information Dominance, we should step back and consider what *Dominance* means and what we need to achieve it. If we can generally define Dominance,

---

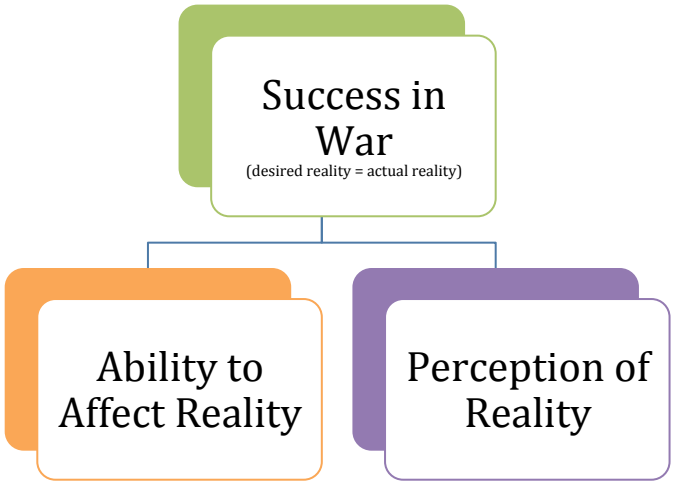
to optimize decision making and maximize warfighting effects in the complex maritime environment of the 21st Century…"

[2] This concept was first introduced in my paper *General Dominance Theory and Applications to Information Dominance: A Paradigm for Success in War*, which was published in April 2014.

then we should be able to apply those same principles to any domain, including the Information Domain.

Objectives of War

In war, our ultimate goal is to make a *desired image* of reality the *actual* reality. We want to change "the way things are" into "the way we want them to be." This requires two things: (1) the ability to accurately perceive reality and (2) the ability to affect reality. If we can do both of these things perfectly, then we can always achieve this goal, and we can always achieve success in war.



Defining Domain

In war, we speak of *Domains* - we want to achieve dominance in a set of Domains. A Domain is a container. A Domain is an environment. Within a Domain, things happen in a certain way. A **Domain** is *an environment where things exist and where those things are bound by laws and patterns of existence, movement, destruction, propagation, and other environmental factors – the combination of which is either unique of other Domains, or distinct enough to warrant special consideration.*

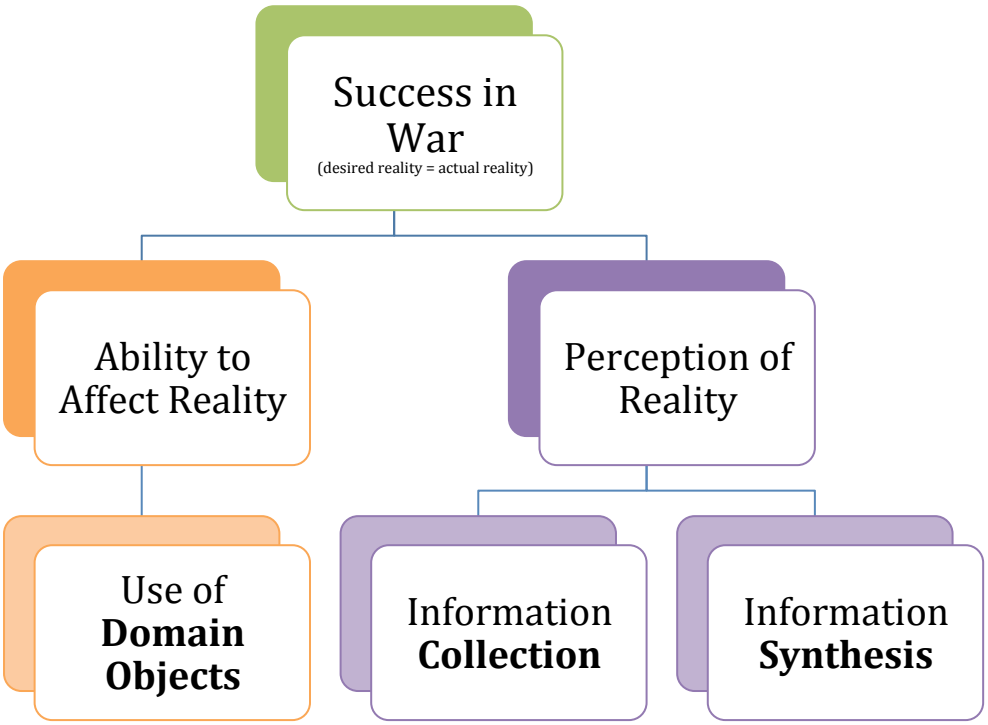
For example, the Air Domain includes all things that exist and move through the air. These things follow laws and rules such as buoyancy, Bernoulli's principle, and gravity.

Things are surrounded by nitrogen, oxygen, and carbon dioxide in weather phenomena. Properties of this Domain cause things to move and propagate in certain ways. The behavior of things in this Domain is significantly different from other Domains.

Members and qualities of one Domain (e.g., people, things, and rules of movement) can usually be found in other Domains, and members and qualities of one Domain can have an impact on another. It isn't the individual members and qualities of a Domain that make it distinct; rather, it is the *combination* of those members and qualities. For example, aircraft, vehicles typically thought of as operating in the Air Domain, are used in the Subsurface Domain for reconnaissance. Submarines, a vehicle typically thought of as operating in the Subsurface Domain, are used in the Land Domain for submarine-based missile strikes. These vehicles are a part of multiple Domains because they operate or have an impact on multiple Domains.

Defining Dominance and Warfare

Perception of Reality ("POR"), a component of Success in War, is determined by two factors: (1) our ability to *collect* information and (2) our ability to *synthesize* information. Collection is the process of completely receiving (both actively and passively) information from the battle space. Synthesis is the process of correctly changing that raw sensory information into something factual with meaning – something that accurately describes some part of reality.



The **Ability to Affect Reality** ("ATA") is the other component of Success in War. It is achieved by the use of something in the Domain. Things that we can use in a Domain to affect reality (e.g., our opponent or the environment) are *Domain Objects*. Domain Objects can be physical (e.g., a bullet or a submarine) or non-physical (e.g. a war plan or a piece of information).

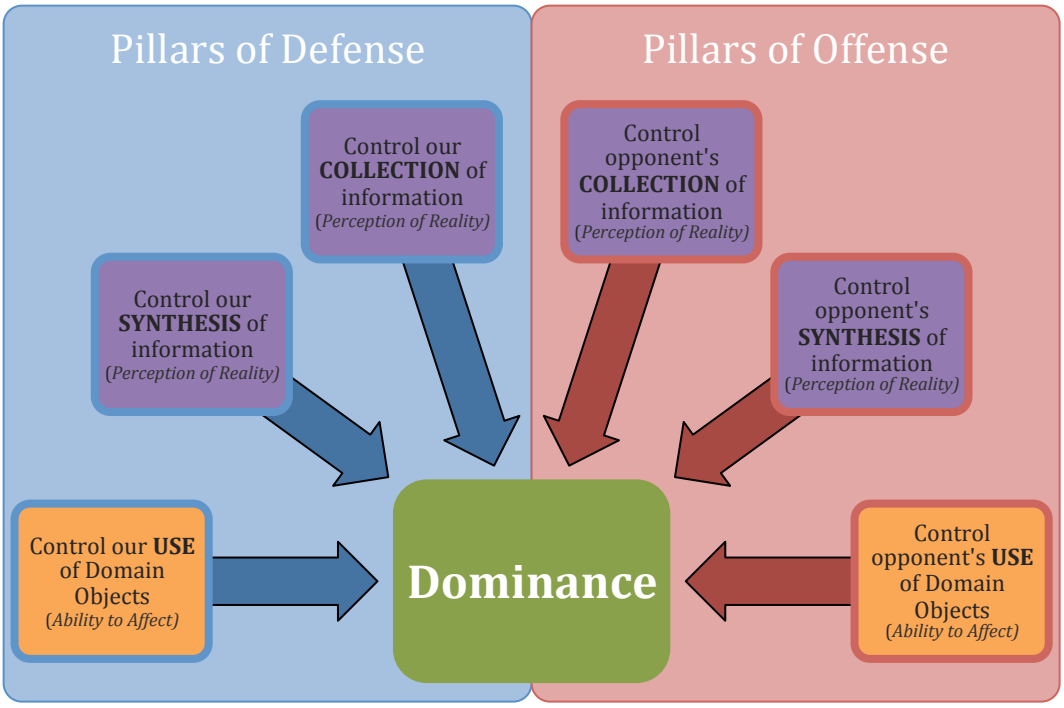
The actions we take both in our pursuit of POR and ATA are performed under competitive circumstances against an opponent – and that opponent's desired reality is often not the same as our desired reality. Therefore, our opponent may take actions that prevent us from achieving perfect POR and perfect ATA. In this struggle, we must achieve our desired reality at the expense of our opponent's desired reality. In other words, we want to be *dominant*. Therefore, **Dominance** is ***the state in the battle space where a desired image of reality can be achieved completely despite the will of an opponent.*** The better our POR and ATA, the closer to Dominance we come. Dominance is achieved when we have a perfect POR and ATA.

The struggle for Dominance is war, and the actions we take to win the war are all part of *Warfare*. In the context of this paradigm, therefore, **Warfare** is ***the struggle against an opponent to achieve and retain a perfect ATA and POR***. In other words, **Warfare** is ***the pursuit of Dominance***.

Six Critical Requirements of Dominance

Achieving Dominance requires control of our opponents and of ourselves. Based on the components of Success in War (POR and ATA), this control can be broken down into six types of control required to achieve Dominance:

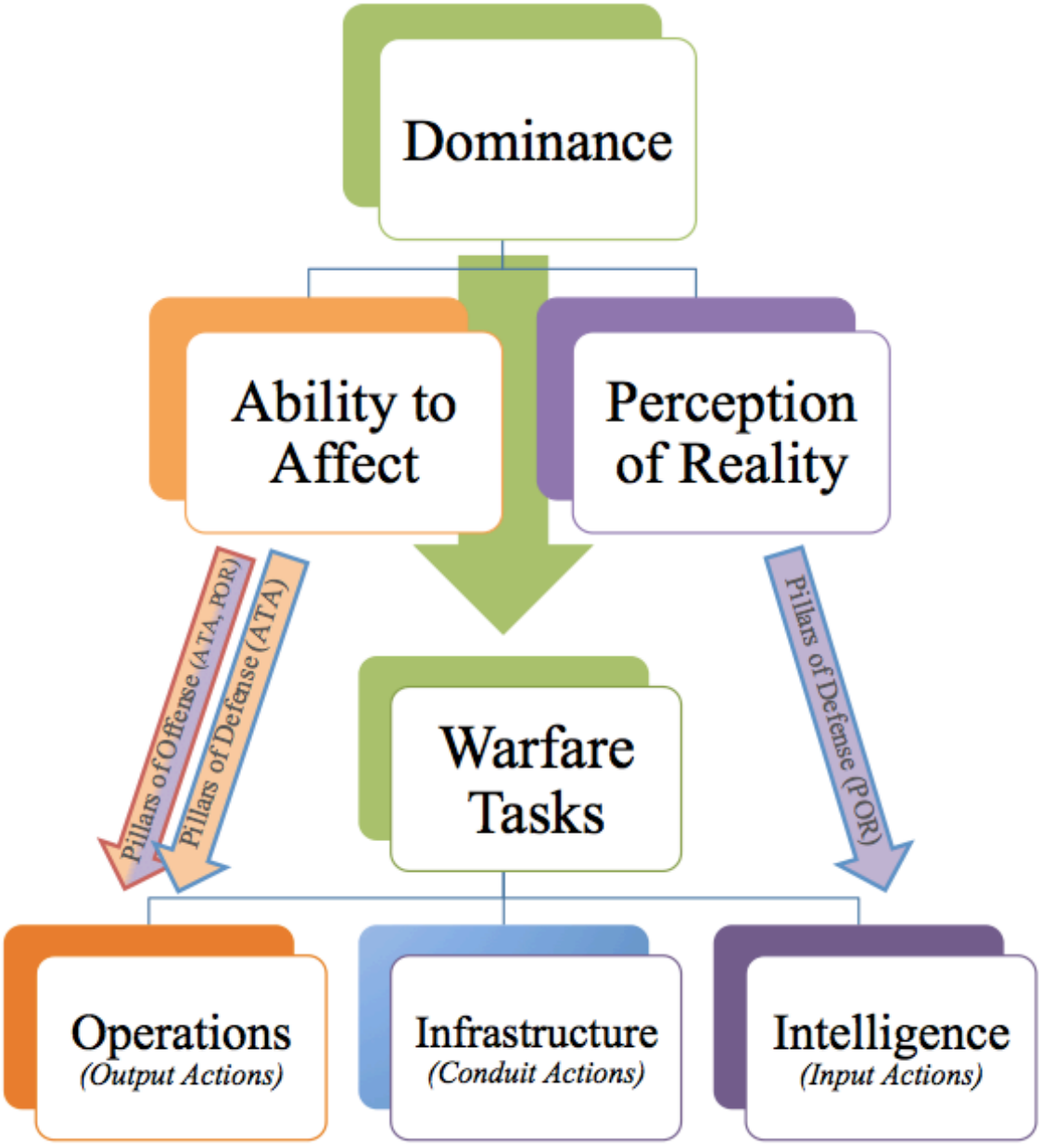
1. Control our collection of information
2. Control our synthesis of information
3. Control our ability to use Domain Objects
4. Control the opponent's collection of information
5. Control the opponent's synthesis of information
6. Control the opponent's use of Domain Objects



Critical Requirements 1-3 are the ***Pillars of Defense***. Critical Requirements 4-6 are the ***Pillars of Offense***. Requirements 1 – 3 are defensive because *loss of any* one of these requirements will preclude us from achieving Dominance. Reciprocally, if we *achieve any* of the requirements 4 – 6 then we can prevent our opponent from achieving Dominance.

General Warfare Framework

Properly allocating scarce resources is essential to achieving and maintaining Dominance, so we must ensure that everything we do has a reason that supports that objective. To guide this pursuit of Dominance, we can take the Six Critical Requirements of Dominance and form a *General Warfare Framework*. This framework can help ensure that each task we undertake can be traced back to one of these six requirements.



Each of the Six Critical Requirements of Dominance can be divided into one of two categories: (1) Inputs and (2) Outputs. Inputs satisfy Critical Requirements 1 and 2 and are the actions we take to increase our Perception of Reality (POR). Inputs can also be described as *Intelligence*. Outputs satisfy Critical Requirements 3-6 and are things we do to affect our opponent or protect ourselves. Outputs can also be described as *Operations*.

Tasks that enable Input and Output actions are Conduits. They provide the *Infrastructure* for Intelligence and Operations. These actions don't directly contribute to

achieving Dominance because they don't directly address a Critical Requirement, but they can be essential to Operations and Intelligence actions.

Task Purpose	Description	Applicable Critical Requirements	Task Category
Inputs	Tasks that achieve Perception of Reality	1 & 2	**Intelligence**
Outputs	Tasks that achieve and maintain Ability to Affect	3, 4, 5, & 6	**Operations**
Conduits	Tasks that enable Input and Output actions	All (indirectly)	**Infrastructure**

If every task we perform can fit into one of these three categories, we can have a high degree of confidence that we are working towards the philosophical objective of Dominance: *the state in the battle space where a desired image of reality can be achieved completely despite the will of an opponent.*

Part II: Applying General Dominance Theory to Information Dominance

Now that we have defined Dominance in general terms, we can easily apply the definitions and methods of General Dominance Theory to the Information Domain. To develop definitions, measurable goals, and tasks in the pursuit of Information Dominance, we simply apply the fundamentals of General Dominance Theory to the Information Domain using the following 6 steps:

Translation Step	Concept from General Domain	→	Resultant Concept in Information Domain
1	Domain	→	Information Domain
2	Domain Object	→	Information Domain Object
3	Dominance	→	Information Dominance
4	Warfare	→	Information Warfare
5	Six Critical Requirements of Dominance	→	Six Critical Requirements of Information Dominance
6	General Warfare Framework	→	Information Warfare Framework

Step 1: The Information Domain

The Information Domain[3] is a distinct warfare Domain that is not necessarily bound by physical dimensions and includes all information. By its nature, it includes the information used in other warfare Domains and information that may *not* be found in other Domains. The **Information Domain** can be described as: *a special case of a Domain whose members are bound by the laws and patterns of existence, movement, destruction, propagation, and the other environmental factors of information. The Domain that includes all information and things that can affect information.*

Step 2: Information Domain Objects

In the Information Domain, information pieces not only make up our Perception of Reality (POR), they can also be used as objects of force that enable on our Ability to Affect Reality (ATA). This is because physical objects are not the only causes of force in this Domain. Information is a force that can have an affect on an opponent. Instead of tanks, pieces of information (Information Domain Objects) can affect our opponent. For example, information describing illegal activity of high-ranking officials could be used to defame. Therefore we should define **Information Domain Object** as: *a special case of a Domain Object that resides in the Information Domain. A physical or non-physical entity whose use has an Ability to Affect an opponent or the environment in the Information Domain.*

---

[3] In my work, *General Dominance Theory and Applications to Information Dominance: A Paradigm for Success in War*, I explain how what is popularly called the Information Domain is more accurately described as the Composite Information Domain, a collection of Domains that are significantly related to information. In that construct, the Computer Network (Cyber) Domain is a special segment of the Electronic Domain, which is a special segment of the Electromagnetic Domain. Those Domains along with the Information and Political Domains (and possibly others) comprise the Composite Information Domain. For what most people intend to describe, it is more accurate to use the term *Composite Information Dominance* than the term *Information Dominance*. For the purpose of this article, the term *Information Domain* is used interchangeably with *Composite Information Domain* and includes Electronic Warfare and Cyber Warfare.

Step 3: Information Dominance

Just as we defined Dominance generally, we can apply the principles of General Dominance to the Information Domain. Information Dominance is simply a special case of Dominance in the Information Domain. **Information Dominance** is *the state in the battle space where a desired image of Information reality can be achieved completely despite the will of an opponent.*

Step 4: Information Warfare

Using the definition of warfare from General Dominance Theory, Information Warfare is simply a special case of Warfare in the Information Domain. **Information Warfare** is: *the struggle against an opponent to retain an Ability to Affect the Information Domain and maintain an accurate Perception of Information Reality; the pursuit of Information Dominance.*

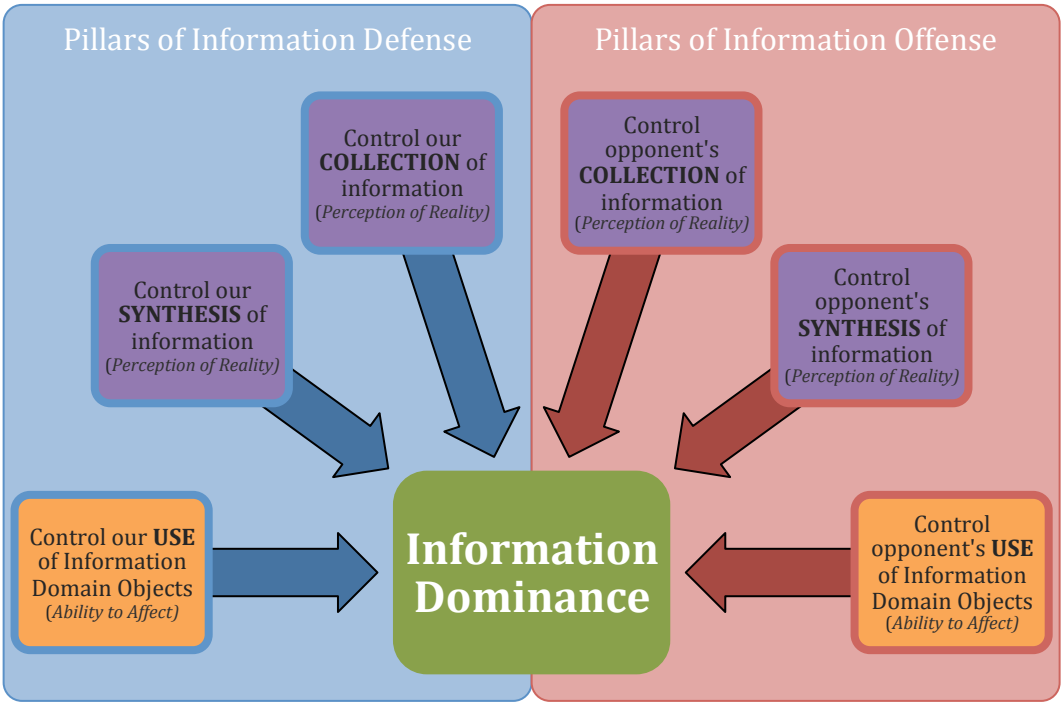
Step 5: Six Critical Requirements of Information Dominance

The Six Critical Requirements of Information Dominance can be defined using the Six Critical Requirements of Dominance from General Dominance Theory applied to the Information Domain. Specifically:

1. Control our collection of information
2. Control our synthesis of information
3. Control our use of Information Domain Objects
4. Control the opponent's collection of information

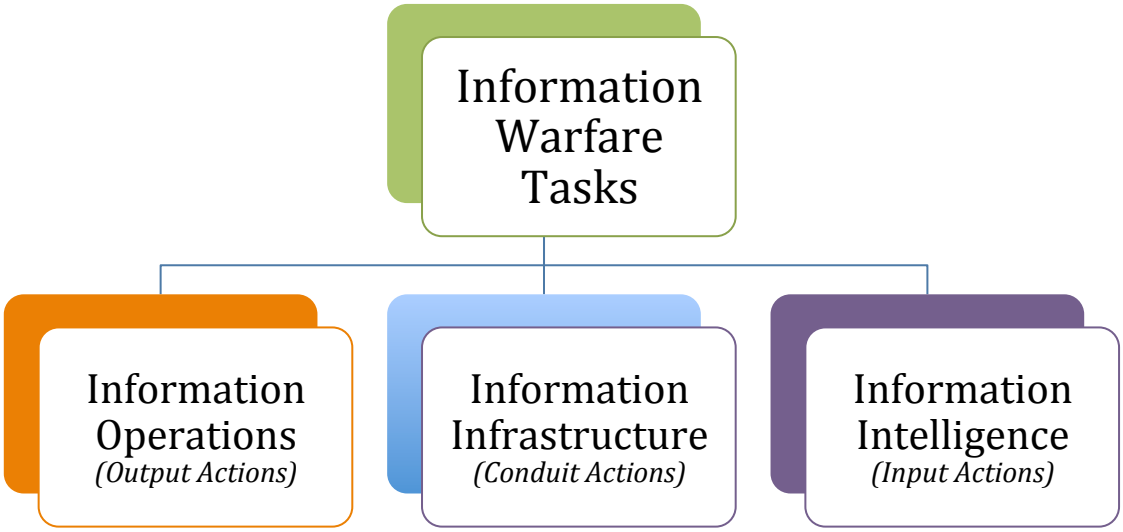
5. Control the opponent's synthesis of information

6. Control the opponent's use of Information Domain Objects



Step 6: Information Warfare Framework

In General Dominance Theory, the General Warfare Framework organizes the tasks required to achieve Dominance. In the Information Domain, the Information Warfare Framework organizes tasks into Information Operations, Information Infrastructure, and Information Intelligence.



In Information Warfare, **Information Operations** (IO) are: *output actions that (1) degrade an opponent's ability to collect, synthesize, or use information and (2) prevent our opponent from degrading our ability to collect, synthesize, or use information.* IO actions prevent our opponent from affecting our ability to collect, synthesize, and use information and degrade our opponent's POR and ATA.

Information Intelligence (Intel) actions provide decision-making intelligence to the commander based on information present in the battle space. These input actions work to meet Critical Requirements 1 and 2 (Collection and Synthesis) and inform Information Operations.

Information Infrastructure (II) actions provide commanders the conduit to conduct IO and Intel actions and to translate Intel into IO capabilities. II actions can also improve actions we take to increase our POR and ATA. Without II actions, our IO and Intel actions may be significantly degraded.

Application to the Navy's Information Dominance Corps

The Information Warfare Framework can be easily applied and integrated with the Navy's Information Dominance Corps (IDC). The IDC currently organizes people into the following groups:

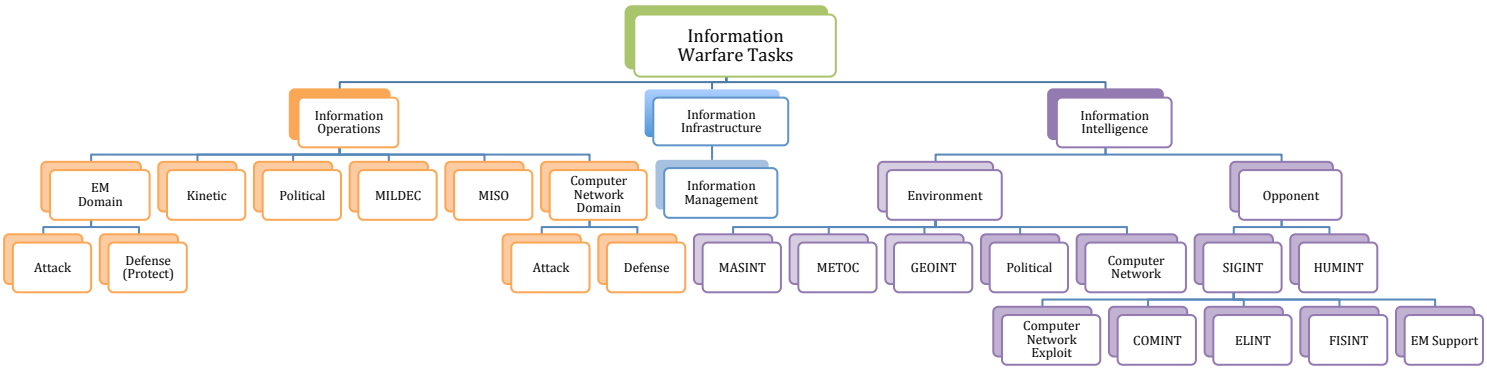
- Information Professional
- Intelligence
- Meteorological/Oceanography (METOC/OCEANO)
- Information Warfare

Based on the Information Warfare Framework and the historical focus of each of these groups, each group within the IDC could be focused according to the following:[4]

[4] Those familiar with IDC will notice, however, that this organization is very similar to current practice. Also, this addresses IDC community **focuses**, and does not imply that focus should be to the exclusion of other actions.

- **Information Professionals** should specialize in the Information Infrastructure. This would include (but not be limited to) information systems, information management, and human-machine interfaces. Anything that enables Information Operations and Intelligence actions falls into this category.
- **Intelligence** personnel are concerned with Intelligence actions. This could be about our opponent or the Domain environment. They should specialize in leading the collection of information and synthesis, and ensuring it can be used in Information Operations. They should work closely with those conducting Information Operations actions.
- **METOC/OCEANO** personnel are a special case of intelligence personnel. They should specialize in MASINT, METOC, OCEANO, and GEOINT. Their specialty is Intelligence (including prediction) about the physical environment, as opposed to Intelligence about our opponent.
- **Information Warfare** personnel should specialize in Information Operations.[5] They are the sword and shield of the IDC. They also have a natural interest and expertise in time-sensitive Intelligence based on the speed of war. They should work closely with those conducting Intelligence actions.

Using the Information Warfare Framework, popular tasks of the IDC would be categorized according to the following:



[5] As defined herein.

Conclusion and Recommendations for Action

I have given an introduction to General Dominance Theory, which provides definitions for Dominance and Warfare that can be applied to the Information Domain. In applying General Dominance Theory to the Information Domain, I established core definitions that can guide our efforts as we pursue Information Dominance. I also derived two sets of criteria (The Six Critical Requirements of Information Dominance and the Information Warfare Framework) that can help us determine actions that contribute to our desired end state: success in the Information Domain.

Applying General Dominance Theory to the Information Domain gives simple, unifying mantras for those fighting for Information Dominance: (1) *Information Dominance is the state in the battle space where a desired image of Information reality can be achieved completely despite the will of an opponent* and (2) *Information Warfare is the pursuit of Information Dominance.* These simple definitions can help each member of the Navy's Information Dominance Corps realize their part in achieving Information Dominance.

These definitions:

- provide the Information Warfare Framework, in which the concept of Information Operations is given more definition and relevance,
- give tasks currently performed by the Information Professional community are a name (Information Infrastructure), and
- provide these benefits without altering the concept of Intelligence.

In other words, this approach to defining Information Dominance does not destroy the great strides the Intelligence community has made in the last 100 years. Rather, it helps refine time-tested concepts and applies them to modern, more complex challenges. As long as the actions we take in pursuit of Information Dominance fit into the Information Warfare

Framework, those actions will contribute to achieving Information Dominance. On the other hand, actions that do not fit into this framework are wasteful or counterproductive and should be stopped or refocused.

We cannot afford to stumble into Information Dominance through "brute force" and luck. We will lose to faster, more organized, and more focused adversaries. By using General Dominance Theory, we can use the objective of war (*to make our desired image of reality the actual reality*) as the basis for our organization and focus. Instead of stumbling, we can now use clearly established goals, definitions, and frameworks to assess our current efforts and align them in a way that allows us to achieve Information Dominance more quickly.

General Dominance Theory, as applied to Information Dominance, should be refined and subsequently adopted by the US Navy as the underlying theory that provides direction to the Information Dominance Corps and guides strategy and tactics in the Information Domain.