New Network, New Roles

Exploring the roles of the military services and DISA in the Joint Information Environment using General Dominance Theory

April, 2015

Word Count: 2,788

The Challenge:

What are the appropriate roles for the military services and the Defense Information Systems Agency to establish, sustain, and operate the Joint Information Environment?

New Network, New Roles

Exploring the roles of the military services and DISA in the Joint Information Environment using General Dominance Theory

The Joint Information Environment (JIE) is the new network and the "way ahead" for the Defense Information Systems Agency (DISA). The JIE consolidates all of the disparate Department of Defense (DoD) networks in an effort to reduce cost, increase capability, improve cyber-defendability, and enable mobile or forward-deployed warfighters to access the Department of Defense Information Network (DoDIN). The JIE is also more than just a network, it aims to provide services and capabilities never before realized within the DoD. But with this new approach comes new challenges. One of these challenges is to determine the roles of the military services and of DISA in a way that will best establish, operate, and sustain the JIE. Where should DISA provide support? Where should the military participate?

Given the evolving cyber threats and the DoD's designation of cyberspace as a full-fledged domain of war in 2011 (alongside air, land, sea, and space), we cannot afford for the JIE to become "just another network." It will become our "home front" in the cyberspace domain whether we like it or not. Likewise, DISA cannot remain "just another network service provider." The military services must take a more active role - not only as a customer or stakeholder, but also as an innovator actively participating in system design, service maintenance and evolution, and cyber defense. DISA must become more than a just a "combat support agency" and evolve into a combat partner.

How can we achieve these lofty goals? Or approach cannot be haphazardly guided by the whims and allure of new technologies. It must be deliberate. It must have vision. It must philosophically align with the goals of the DoD and our nation.

Ultimately, the goal of the DoD is to win wars. To win wars, you must achieve dominance against our adversaries in every domain of war. The JIE must enable operations in the pursuit of dominance in all domains of war, and therefore we should consult applicable war theory as we establish the JIE. General Dominance Theory (GDT) provides a framework that allows us to clearly see how the JIE must contribute to our pursuit of dominance, and to discover the role of the military services and DISA within the JIE that will enable that pursuit.

When the concepts of GDT are applied, three types of relationships between the military services and DISA become clear. The first is the traditional relationship between the military services and DISA, that of the customer and provider, respectively. This is based on the fact that, at its core, JIE is designed to provide the military with an infrastructure to conduct actions that lead to success in war. The second is that the military should take an active role in the cyber defense of the JIE because of the expertise and the interest the military has in preserving its information, with DISA as support experts. The third relationship is a close integration of military intelligence personnel in the development of software and other tools designed to automate or otherwise quicken the intelligence collection and synthesis process, with DISA providing expert software/tool developers. Although the latter two relationships are untraditional, they will be critical in determining whether JIE will become the "network and enabler of tomorrow" or "just another network."

I have divided the remainder of this discussion into two parts. Part I will provide a brief overview of GDT for unfamiliar readers. In Part II, I will apply GDT's General Warfare Framework to provide clear guidance on the role of the military services and of DISA within the JIE.

Part I: A Brief Overview of General Dominance Theory

Developed in 2014, General Dominance Theory (GDT) is a high-level war theory that blends Carl von Clausewitz's theory on the nature of war with the concept of dominance. GDT ultimately derives a framework for achieving dominance in any domain based on the ideas that 1) dominance is the ability to make a desire into reality and 2) to achieve dominance you must be able to perceive and affect reality better than your adversary.

The Objectives of War, the Idea of Dominance

Clausewitz wrote, "War is … an act of force to compel our enemy to do our will." (On War. Howard translation, 1976). Stated more generally, in war our ultimate goal is to make our *desired* reality the *actual* reality. We want to change "the way things are" into "the way we want them to be." By casual inspection, this requires two things: (1) the ability to accurately perceive reality (i.e. know what is) and (2) the ability to affect reality (i.e. change what is). If we can do both of these things perfectly, then we can always achieve this goal. (Figure 1 illustrates)

Perception of Reality (POR), 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 transforming that raw information into something factual with meaning – something that accurately describes some part of reality.

The **Ability to Affect Reality** (ATA) is achieved by the use of something in the domain. Things that we can use or manipulate in a domain to affect reality are *Domain Objects*. Domain Objects can be physical (e.g., a bullet or a submarine) or non-physical (e.g. a law or a piece of information).

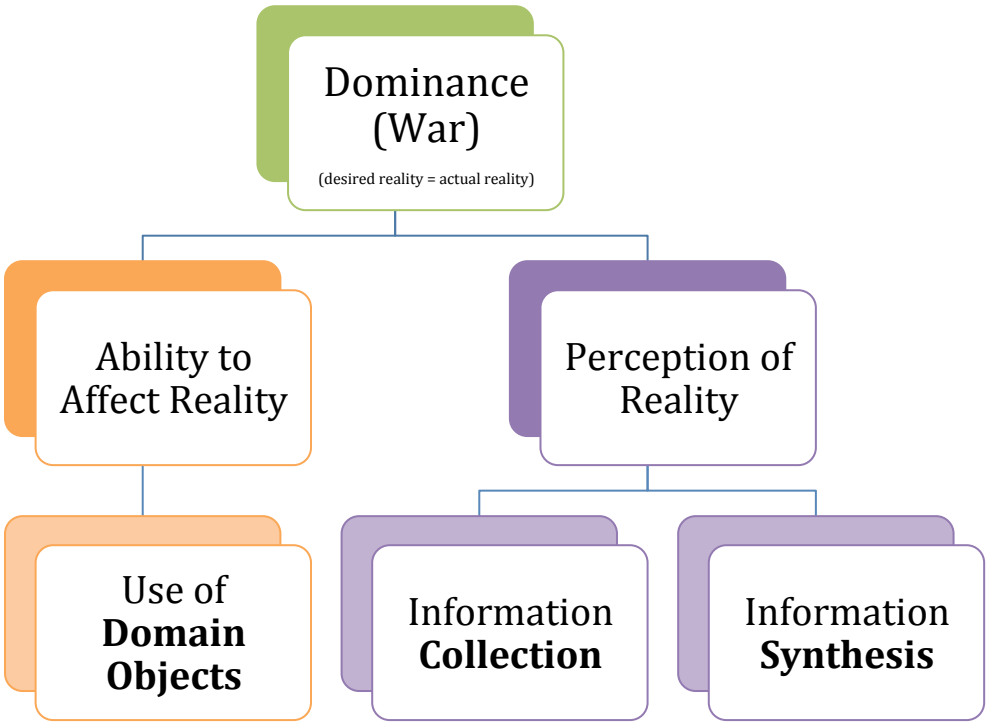

Figure 1: Our ability to achieve Dominance (the objective of war) is determined by our Ability to Affect Reality and our Perception of Reality. Ability to Affect Reality is the degree to which we can use things within the domain. Perception of Reality is determined by our Information Collection and Information Synthesis.

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 often conflicts with 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*. **Dominance** is ***the state in the battle space where a desired 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 perfectly achieved when we have a perfect POR and ATA.

In blending Clausewitz's theory on war with the concept of Dominance above, we can establish that the struggle for Dominance is war, and the actions we take to succeed in war

are all part of *Warfare*. Therefore, **Warfare** is ***the struggle against an opponent to achieve and retain ATA and POR***. In other words, **Warfare** is ***the pursuit of Dominance***.

Six Critical Controls of Dominance

Achieving Dominance requires control of our opponents and control of ourselves. Based on the requirements of Dominance (POR and ATA), these areas of control can be organized into **Six Critical Controls** (SCCs) required to achieve Dominance (Figure 2 illustrates):

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

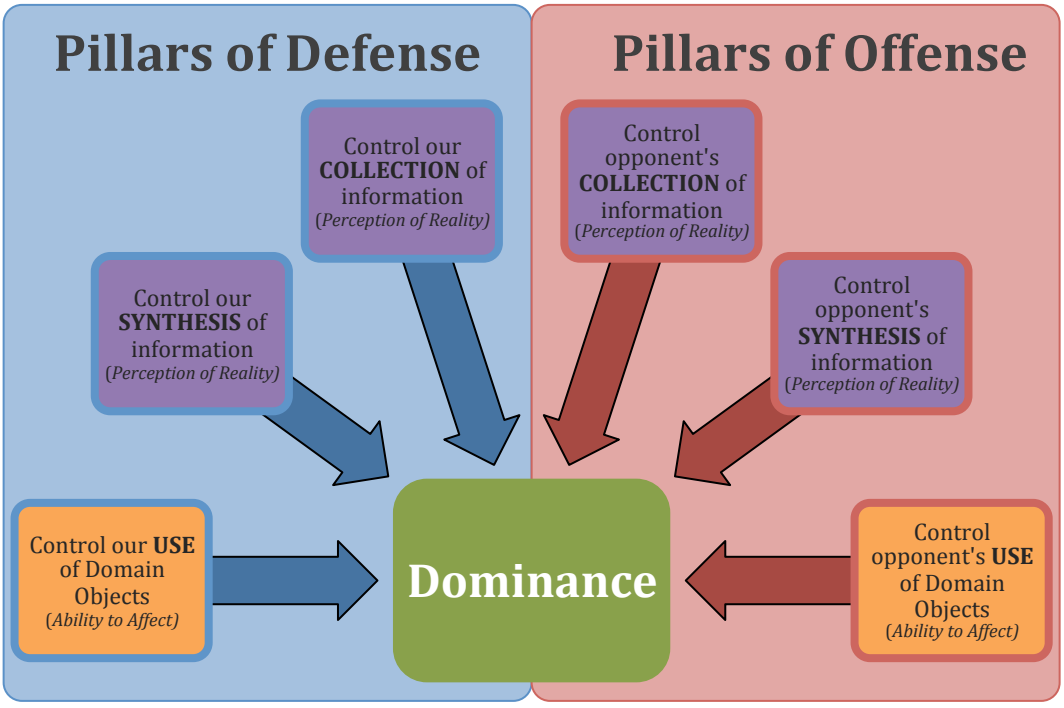

Figure 2: The Six Critical Controls of Dominance puts our desires in direct competition with our opponents. The Pillars of Defense illustrate our need to protect our POR and ATA, while the Pillars of Offense illustrate our need to degrade our opponent's POR and ATA. By achieving all of the Pillars of Defense while successfully achieving any of the Pillars of Offense, we can achieve Dominance while preventing our opponent from achieving Dominance.

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 controls will preclude us from achieving Dominance. Reciprocally, if we *achieve any* of the controls 4 – 6 then we can prevent our opponent from achieving Dominance.

General Warfare Framework

It is not enough to know what we need in order to achieve Dominance, we must organize ourselves in a way that will maximize our ability to pursue Dominance. Properly allocating our 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 organization, we can take the Six Critical Controls of Dominance and form a **General Warfare Framework** (GWF). This framework can help ensure that each task we undertake can be traced back to one of the SCCs and, ultimately, back to the concept that perfect Dominance requires perfect POR and ATA.

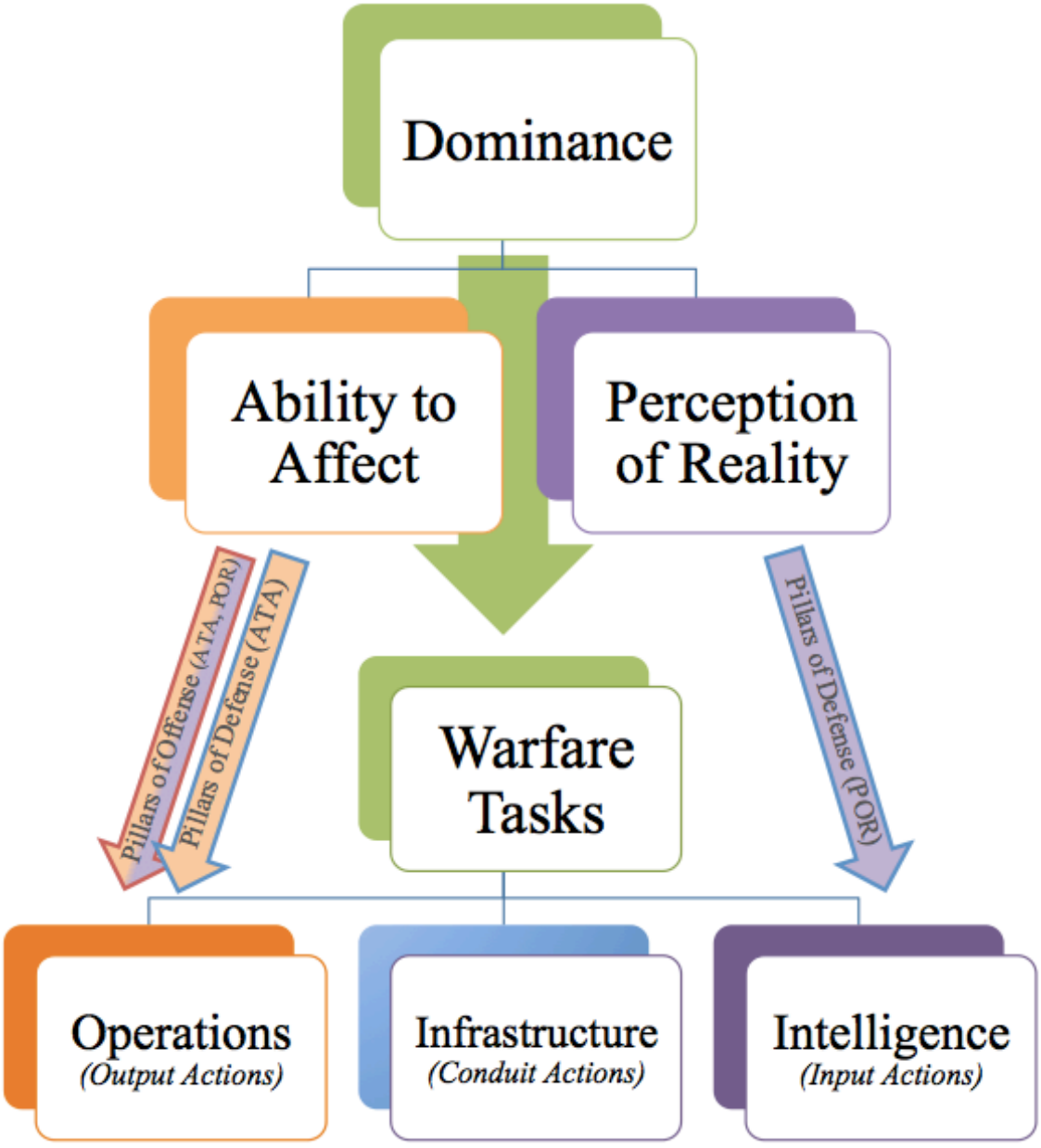

Figure 3: The General Warfare Framework is the translation of the Six Critical Controls into a practical framework that ensures that all tasks performed in the pursuit of Dominance (Warfare Tasks) actually contribute to achieving Dominance. Operations are actions that aim to achieve the Pillars of Offense and the ATA Pillar of Defense. Intelligence actions aim to achieve the POR Pillars of Defense. Infrastructure actions enable Operations and Intelligence actions.

Each of the SCCs can be divided into one of two categories: (1) *Operations* and (2) *Intelligence* actions. Intelligence actions satisfy SCCs 1 and 2 and are the actions we take to increase our Perception of Reality (POR). Operations satisfy SCCs 3-6 and are things we do to affect our opponent or the environment to or protect ourselves.

The translation of the SCCs into this General Warfare Framework is where we pass from the theoretical into the practical. In practice, we must perform actions to enable Intelligence and Operations actions. These actions are *Infrastructure* actions.

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 our objective of Dominance: *the state in the battle space where a desired reality can be achieved completely despite the will of an opponent*.

Part II: Using General Dominance Theory to Guide the JIE

The major takeaway from GDT is the establishment of the General Warfare Framework (GWF) (Figure 3), a guide to determining what actions to take in the pursuit of Dominance. Any action we take must fit into the GWF. If actions don't fit into the GWF, they are wasteful or counterproductive.

Now let us consider the appropriate roles of the military services and of DISA should be within the JIE. All we have to do is determine where the JIE belongs within the GWF. It is surely Infrastructure, but does it also have a role in Operations or Intelligence actions? (Figure 4 illustrates)

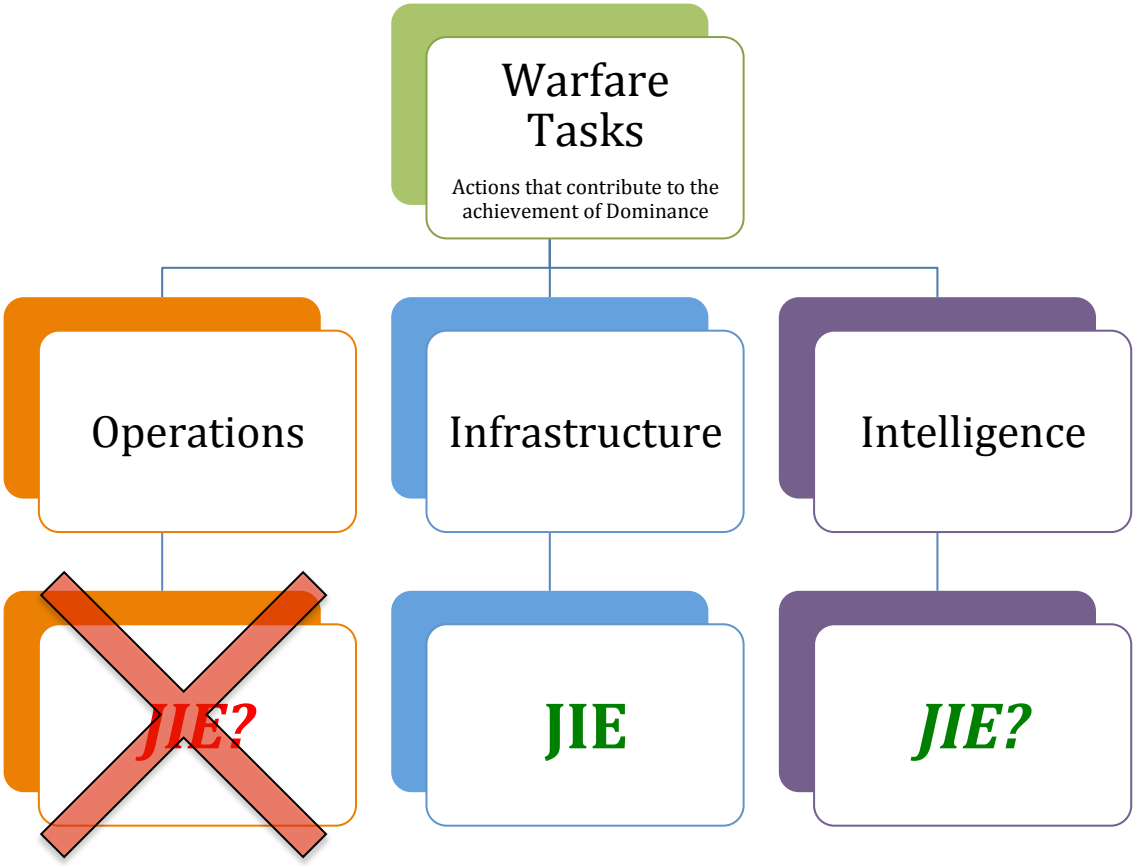

Figure 4: Because of its aim to become the "new" DoDIN, JIE is performing an Infrastructure action - it enables Operations and Intelligence actions. But is the JIE also a part of Operations or Intelligence actions? JIE will perform Intelligence actions based on its cyber defense requirements and also by conducting actions that aid in the collection and synthesis of information for the warfighter.

The JIE Performing Infrastructure Actions

Infrastructure actions are those actions that enable Operations or Intelligence actions. Clearly, as the "new" DoDIN, JIE is performing Infrastructure actions. JIE will provide our warfighters access to information we have collected and/or synthesized and will allow them to perform further synthesis and integration into their Operations actions.

Given the role of JIE in Infrastructure actions, the role of military services and DISA follows in a traditional customer/provider relationship. DISA should act as a service provider and the military services as a customer that provides useful feedback and coordination to DISA.

In the Navy, our Information Professional (IP) officers and Information Systems Technicians (ITs) conduct Infrastructure actions on a daily basis. They ensure secure and reliable communications and network paths are established and available for use. In the same way, our IPs and ITs should represent the Navy as a customer and stakeholder. As with any good team, **DISA and the Infrastructure personnel from each of the services should have a collaborative relationship from design to implementation and maintenance**.

The JIE Performing Intelligence Actions

Actions we take to improve or protect our Perception of Reality (POR) are Intelligence actions. The JIE has several goals that can be considered Intelligence actions.

One of the stated goals of the JIE is to provide a system "more secure against cyber threats." By taking action to protect the information that we store and access, the JIE is conducting Intelligence actions. Specifically, if JIE were to not take actions to protect information, an adversary could deny, degrade, or destroy our information in a way that reduces our POR. By denying, degrading, or destroying our networks and systems, the adversary could reduce our ability to collect information, which would also reduce our POR.

Another stated goal of the JIE is to introduce "DoD Core Enterprise Services" which includes better Email capabilities, directory and cloud computing services, and ways to acquire specialized software tools on demand. All of these efforts increase the efficiency of each user and, arguably, increase the ability of any given user to synthesize and collect information. In many cases perhaps new services will actually be able to synthesize information on behalf of users, thereby directly contributing to POR.

With the JIE actively taking actions to protect our information and POR, and with the possibility of the JIE automatically collecting or synthesizing information on behalf of the warfighter, we can classify some of the actions of the JIE as Intelligence actions.

We should expect DISA and the military services to assume roles and relationships that promote these Intelligence actions. The military services have a considerable capability to conduct Computer Network Defense (CND). As the principle architects of JIE, DISA will have considerable knowledge of the inner structure and network boundary requirements of the JIE. Therefore, **the military services should lead the CND efforts of the JIE, enabled by DISA experts.**

The military also understands best what collection and synthesis is required to increase their POR within a given domain or geographic area. DISA will have (or should acquire) the expertise needed to develop systems and JIE services that can contribute to collection and synthesis of information. Therefore, **the military services should actively drive the development of Information collection and synthesis systems and DISA should provide the capability to develop such systems.** For example, Navy Intelligence (Intel) officers and Intelligence Specialists (ISes) can work with DISA software developers to find ways to take the enormous troves of data and deliver actionable information to JIE users.

The JIE Performing Operations Actions

Actions we take to affect our opponents' Ability to Affect Reality (ATA) or POR or to defend our own ATA are Operations actions. The JIE does not have any advertised capability to conduct these types of actions.

However, if the JIE were to engage in actions intended to "trick" or deceive adversaries (i.e. to directly affect an adversary's POR), these could be considered Operations actions. For example, if the JIE architecture physically or logically "changed shape" or changed appearance periodically to deceive an opponent.

In this case where the JIE is conducting Operation actions, it might again be appropriate for the military services, with their full-spectrum cyber expertise, to take the lead while being facilitated by DISA JIE experts.

Conclusion and Recommendations for Action

When determining the roles of the military services and DISA in establishing, operating, and sustaining the Joint Information Environment, we need a framework to guide our decisions. The General Warfare Framework provides this guide leads us to results that contribute to our ultimate goal in war: the state where we can make our desired reality the actual reality. By using the GWF, we can ensure that every action we take directly supports one of the two requirements for achieving Dominance, our Ability to Affect Reality and/or our Perception of Reality.

By applying the GWF, it is clear that the JIE will engage in Infrastructure actions, which dictates a traditional customer/provider relationship between the military services and DISA. It is also clear that the JIE will be conducting Intelligence actions, which will require military services to provide Computer Network Defense expertise enabled by DISA JIE experts. The JIE will conduct Intelligence actions that will increase our ability to collect and synthesize information and therefore our military intelligence personnel should lead the development of these specialized tools and capabilities while DISA provides the means to create such tools and capabilities. It is likely that the JIE will not be involved in Operations actions, but the GWF provides an easy way to determine if Operations actions are being taken, and could therefore provide a way to determine the role of the military services and DISA to conduct such actions.

Given the importance of the cyber domain and the fact that our adversaries can affect our POR by attacking the JIE, and the fact that we can greatly improve our own POR by creating tools that help collect and synthesize information on behalf of warfighters, we must consider adopting non-traditional roles between the military services and DISA. Now, in the early stages of JIE implementation, is the time to set a new standard for a new age.

As JIE evolves to meet our needs over the next decades, we should periodically assess its actions to ensure alignment with the GWF. By doing this, we can ensure that JIE is not only a force-multiplier and a "great system," but something that directly contributes to our goal: Dominance.