What is Military Information Power?

The post-industrial information environment

by Eric X. Schaner

Information has long been understood and employed as one of the four instruments of national power. Information, along with the diplomatic, military, and economic instruments of national power encompass the total resources available to the Nation. These resources are employed to achieve strategic objectives and the policy aims which encompass the national interest. This article draws from the classical notion of the informational instrument of national power and changes in the post-industrial information environment to derive a theory of military information power.

>Mr. Schaner, see page 14 for bio.

The Theory of Military Information Power

The global, instant, and persistent nature of information in the post-industrial era has reshaped the global security landscape. This new era, sometimes called the *Information Age*, creates opportunity for aggressors to directly target the underlying data and networks of information required for the effective functioning of societal institutions. This is possible due to the dependencies in institutions such as banking, health care, manufacturing, transportation, energy, trade and commerce, and all governmental functions now have digital data as well as advanced computing algorithms and networks to provide their services.

The Information Age also creates opportunity for aggressors to directly target individuals and groups of individuals to feed them misinformation or disinformation in order to alter their perception of reality. This is possible because of the degree to which people rely on the Internet, social media, and digital communications to socially interact, plan and coordinate activities, and receive news and information.[1]

A recent RAND study refers to the above phenomena as characteristic of a new form of conflict called *virtual societal warfare.* This form of conflict is executed by aggressors through a combination of attacks on critical societal-institutional data and targeted deceptive messaging through traditional media and social media to alter peoples' social reality and perception of truth.[2]

The growing trend of societal information dependency and the subsequent vulnerabilities is an issue shared by Information Age militaries—including the Marine Corps. During the Industrial Age, technological superiority firmly established the United States as the world's sole military superpower. A defining feature of superpower status was the assured access to and use of information to bring combat power to bear anywhere on the globe.

We can no longer assume combat power overmatch as a result of assured access to information. America's peer competitors are developing capabilities to directly target the data and underlying networks of information the United States currently relies upon to generate and employ combat power. Peer competitors are also challenging United States influence and partnerships through the employment of gradually coercive ambiguous activities, backed by aggressive

Peer competitors are also challenging United States influence and partnerships through the employment of gradually coercive ambiguoius activities. *(Photo by Cpl Nathan Reyes.)*

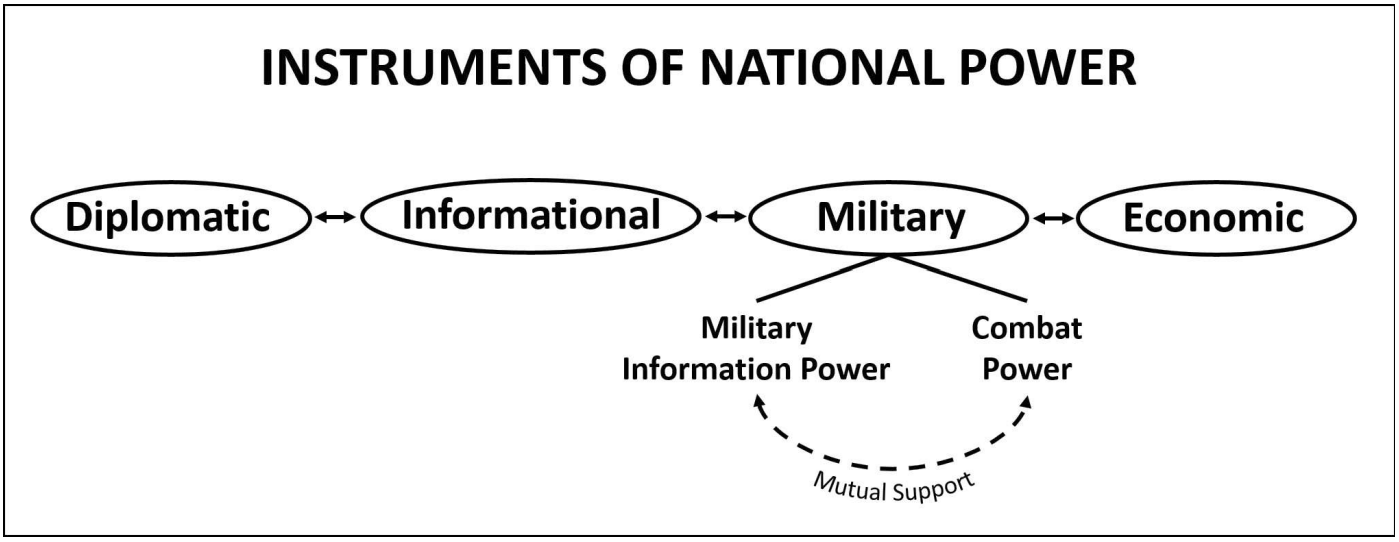

Figure 1.

narratives and propaganda. This type of challenge deliberately remains below the threshold of armed conflict to avoid a traditional U.S. military response.

This leads to a *theory of military information power*. The theory is an expanded view of the military instrument of national power such that it comprises two mutually reinforcing elements—*combat power* and *military information power*. (See Figure 1.)

According to joint doctrine, combat power is defined as "the total means of destructive and/or disruptive force that a military unit/formation can apply against the opponent at a given time."[3] The U.S. military projects combat power in armed conflict or general warfare. To expand upon the concept of combat power, the Marine Corps recently issued a joint memorandum to define the term military information power. The memorandum was signed by the Deputy Commandant for Information and the Deputy Commandant for Combat Development and Integration in January 2020.

The memo defined military information power as:

> the total means of force or information capability that can be applied against a relevant actor to enhance lethality, survivability, mobility or influence.[4]

The memo established the term as official interim guidance to inform doctrine development. This new term underpins expanded thinking about the military instrument of national power and its applicability across the competition continuum.

Military information power is broadly applicable in competition and war, and it is a necessary mutually supporting element to combat power. The side with the ability to manipulate, deny, or destroy the information required for the decision making and basic functioning of the opposing military system, while preventing the opponent from doing the same, achieves significant advantage—including a combat power advantage. *The essence of military information power is the ability to exert one's will or influence over an opponent through the generation, preservation, denial, or projection of information.*

Information Generation

Information generation refers to the preparatory activities conducted to increase our competitive potential in the information environment, such that we may exploit this advantage to achieve some effect in any operational domain. Activities include analyzing the information environment from a threat, friendly, neutral, and physical environment perspective; planning and preparing specific courses of action; gaining the authorities to execute specific actions; and gaining access to the opponent's information environment—to include databases, communications networks, social networks, key leaders, and trusted influencers.

Information Preservation

Information preservation refers to building resiliency in the dependencies and vulnerabilities we have on information and the digital communications required to compete and win in battle.

Information preservation refers to building resiliency to the dependencies and vulnerabilities we have on information and the digital communications required to compete and win in battle.

Information preservation involves activities such as implementing strong cybersecurity measures; conducting defensive or offensive cyberspace operations, or physical attack to protect our

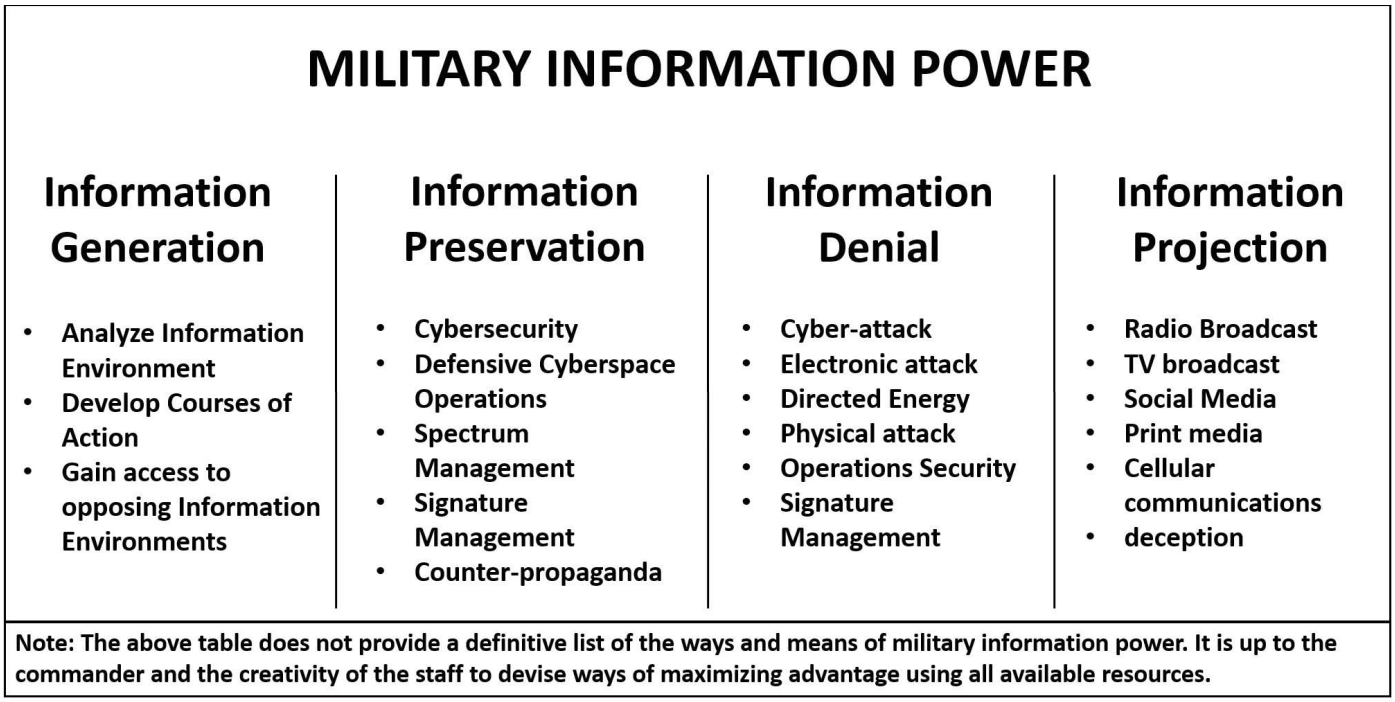

Figure 2.

networks; effectively managing the use of the electromagnetic spectrum; and exercising effective operations security and signature management. It also involves building resiliency to negative news, propaganda, and narratives—to include social media narratives—that work against our mission and objectives. This requirement is increasingly a primary concern for commanders at all echelons.

Information Denial

Information denial describes the use of any means available to gain advantage over an opponent by denying them vital information. This may include manipulating, disrupting, or destroying the information needed by the opponent to sense, make sense, and act. Active information denial involves activities such as cyberattack, electronic attack, directed energy attacks, and physical attack to name a few. Passive means of denying the opponent vital information may include selectively altering or suppressing the physical and digital signatures emanating from friendly forces. This may also include implementing operational security measures, communications discipline, camouflage, and strong cybersecurity measures.

Information Projection

Information projection refers to transmitting information of any type to inform, influence, or deceive an observer—such as the people, government, or military of a competitor or enemy nation. The Marine Corps may project information in many ways to include direct communications such as radio, television broadcast, print media, cellular communications, and social media. Information may also be projected by taking physical actions knowing they are observable, and by knowing what informational impact such actions may create. The methods and objectives of information projection should always be considered with information denial.

Figure 2 depicts and summarizes the elements of military information power as combination of information *generation*, *preservation*, *denial*, and *projection* based on the discussion above.

Conclusion

The theory of military information power provides the theoretical foundation for a more practical discussion of how the Marine Corps generates, preserves, denies, and projects information to gain advantage and achieve objectives. To accomplish this, the Marine Corps has been advancing the concept of operations in the information environment through the establishment of the MEF Information Group. The MEF Information Group is a formation at the tip of the spear in operationalizing the theory above into practice across the whole of the MAGTF.

Notes

1. Michael J. Mazarr, Ryan Michael Bauer, Abigail Casey, Sarah Anita Heintz, and Luke J. Matthews, *The Emerging Risk of Virtual Societal Warfare: Social Manipulation in a Changing Information Environment,* (Santa Monica, CA: RAND, 2019).

2. Ibid.

3. Joint Staff, *Joint Publication 3-0, Joint Operations, incorporating Change 1,* (Washington, DC: October 2018).

4. Joint Staff Joint Memorandum, *Definitions for Information Related Terms,* (Washington, DC: HQMC, January 2020).