Strategy Research Project

Organizing The Army For Information Warfare

by

Colonel Maxell S. Thibodeaux
United States Army

United States Army War College
Class of 2013

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
xx-03-2013	STRATEGY RESEARCH PROJECT	

4. TITLE AND SUBTITLE
Organizing The Army For Information Warfare

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Colonel Maxell S. Thibodeaux
United States Army

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Professor Edward J. Filiberti
Department of Command Leadership and Management

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
U.S. Army War College
122 Forbes Avenue
Carlisle, PA 17013

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Distribution A: Approved for Public Release. Distribution is Unlimited.

13. SUPPLEMENTARY NOTES
Word Count: 6,147

14. ABSTRACT

This research project takes a broad look at the developing role of information in society and warfare. It develops a view of information in 21st century conflict and information as 21st century conflict. It then traces the development of the Army's information-related personnel structures to assess whether they have evolved sufficiently to address these developments. After identifying challenges with the current Army organization, the paper identifies three alternatives. The first alternative is to form a monolithic information corps, the second is to form a multi-functional information corps, and the third alternative is to outsource information warfare to the joint community while retaining traditional information-in-warfare capabilities. In light of the strategic environment and impending fiscal constraints, the author recommends consolidation of the Army's information-related branches and career fields into a monolithic information corps. This alternative best postures the Army information workforce for future growth, development, and employment.

15. SUBJECT TERMS
Information Operations

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. TELEPHONE NUMBER** *(Include area code)*
UU	UU	UU	UU	42	

USAWC STRATEGY RESEARCH PROJECT

Organizing The Army For Information Warfare

by

Colonel Maxell S. Thibodeaux
United States Army

Professor Edward J. Filiberti
Department of Command Leadership and Management
Project Adviser

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

Abstract

Title: Organizing The Army For Information Warfare

Report Date: March 2013

Page Count: 42

Word Count: 6,147

Key Terms: Information Operations

Classification: Unclassified

This research project takes a broad look at the developing role of information in society and warfare. It develops a view of information in 21st century conflict and information as 21st century conflict. It then traces the development of the Army's information-related personnel structures to assess whether they have evolved sufficiently to address these developments. After identifying challenges with the current Army organization, the paper identifies three alternatives. The first alternative is to form a monolithic information corps, the second is to form a multi-functional information corps, and the third alternative is to outsource information warfare to the joint community while retaining traditional information-in-warfare capabilities. In light of the strategic environment and impending fiscal constraints, the author recommends consolidation of the Army's information-related branches and career fields into a monolithic information corps. This alternative best postures the Army information workforce for future growth, development, and employment.

Organizing The Army For Information Warfare

Information Operations and its context need a foundational re-think.

—BG Huba Wass de Czege[1]

In 1997 the Army established the Information Operations[2] Career Field to meet the challenges of 21st Century Warfare. Bill Clinton was President. The Army's operational construct was Air-Land Battle. Microsoft was loaning Apple money to save it from bankruptcy, and the internet bubble was beginning its three-year run. The US was one year away from budget surplus, and only one in four US adults had access to the internet. A great deal has changed since 1997. Unified Land Operations is the Army's operational construct. Apple is worth more than Microsoft.[3] The government is running a 1.1 trillion dollar deficit, and nine of ten US adults have access to high speed internet.[4] The question is whether the Army has adapted itself and its people to take advantage of the growth, complexity, and ubiquity of the information age?[5]

This research project characterizes and assesses the role of information *in and as* 21st century conflict. It also directly addresses whether the current Army personnel model has evolved sufficiently, within present constraints, to produce Soldiers who are ready for information age warfare. The goal is to generate viable Army options that are suitable for the strategic environment in light of impending fiscal constraints, and to generate thoughtful consideration of the operable alternatives at senior levels of the Army. The Army needs to thoughtfully address the roles and relationships for all of its information-related capabilities and their relationship to joint capabilities. A comprehensive strategic assessment of the entire spectrum of information capabilities can help frame the necessary reforms to exploit this dynamic mission area.

Information in Society and Warfare

The first part of the 21st century has revealed an age of unprecedented information commoditization resulting in enormous wealth and prosperity. In America the basis for increasing national and personal wealth has tilted toward three industries: technology, telecommunications and publication.[6]

Information is generated, collected, organized, mined and manipulated with unprecedented levels of computer-enhanced speed and accuracy. That information is disseminated across a common global superstructure in near-real-time, traveling at light speed to billions of users and organizations. This information circulates on managed networks or is posted on servers with enabling protocols that permit secure, interactive and informed financial transactions, market trades, control of industrial equipment, and repeatable back-end business processes. Moreover, the information networks are not a closed system. The networks and the information they carry influence people in the streets, board rooms, and command centers.

Those people and organizations associated with pioneering new information production and targeted distribution are experiencing unprecedented levels of social control, and they are accruing unparalleled wealth and power.[7] It is likely that every nation's means of productivity and power is growing or shrinking in accordance with these industries and developments just as it did with industrial power during the industrial revolution. While information, along with diplomacy, economics, and military strength has always been an element of national power, in the information age it is emerging as an element of national power that sustains all others.[8]

The Army has grasped the emerging role of information in society, but whether it has sufficiently grasped information's role in the human endeavor of war is

questionable. What is irrefutable is that a vast amount of information-related activity signals the arrival of an undeniably real “information age.” Things are different. Warfare is different. The scale and character of difference profoundly affects many aspects of our society, culture, and the very foundation of power in the 21st century.

Business is going beyond the delivery of goods and services across land, oceans, and air aided by new information technology. Now business is delivering new goods such as software, web services, and information via electro-magnetic spectrum, satellites, and undersea fiber optic cables.[9] As the mode for production and delivery changes, business operations change. As business operations change and adapt in the commercial sector, the security sector must likewise change and adapt. The issue is not simply adapting to *information in business*, but adapting to *information as the business* of technology platforms, publication, transmission, and ultimately influence and power.

Information-In-Warfare

As General Martin Dempsey once remarked, “War is discovery—we must continue to out-think and out-adapt our adversaries. Only by remaining alert to the weak signals of change can we preserve the initiative and provide options for our civilian leaders.”[10]

Increasing challenges from state and non-state actors have prompted military leaders to emphasize a new *domain* within the global commons.[11] The cyber domain has joined the air, land, maritime, and space domains as essential for joint mission accomplishment.[12] Dominance within these domains help commanders fight conventional wars. At the same time, US political leaders have argued that information wars have already begun.[13] Is there such a thing as an information war separate and distinct from a major conflict that requires dominance in all domains? If the political

leaders think so, then it is up to the military leaders to adapt and prepare to fight an information war. At the very least, competing nations are vying for a competitive advantage in the information environment, not only by diminishing the US's reputation in the global community, but by pilfering intellectual property, foiling industrial controls, and 'hacking' into secured networks to intimidate or exploit sensitive information.[14] This is evidence that the military may need to adapt to this kind of conflict by devising stratagems and organizing for them.

After all, wherever there is conflict there is the need for well organized, trained, and equipped military personnel. The problem is that conflicts within the newly emphasized cyber domain are not clearly within the purview of established US Services or service-like entities such as the Army, Navy, Air Force, Marines, or Special Forces. Now that world powers are preparing for the potential of information warfare—to include cyber warfare,[15] how can the US effectively protect and wield that kind of national power? How can the Army and other joint forces divide and fulfill their responsibility for guardianship in this environment?

The role of *information-in-warfare* has developed rapidly since the mechanization of armed forces first required wireless radios at the tactical level and the doctrine of AirLand Battle acknowledged the importance of the electromagnetic spectrum as a combat enabler.[16] Over the last two decades, the US has made great strides in bringing an information-empowered force to bear with such key enablers as: the global positioning system for precise navigation and bombing; communications and surveillance systems; biometric systems; and lethal, remotely linked aerial systems.[17] The list goes on.

At the same time, these same information technologies are empowering better coordinated and capable adversaries. For example, the Mumbai terror bombers were able to navigate, communicate, and gather intelligence from commercially available systems resulting in 174 deaths.[18] The smart phone, satellite communications, GPS, and real time social media are all information-related technologies that enabled the lethality and effectiveness of their operation.[19] The terrorists integrated key information technologies, including social media, to employ previously unattainable command and control capabilities.

At the same time, Mumbai's security forces had a difficult time depriving their adversaries of these combat enablers. Indian authorities could not completely shut down voice communications and social media that terrorists used to co-opt and monitor the authorities. This kind of situation poses a challenge for future engagements. It is unclear whether the US could respond to this type of incident either at tactical or strategic levels. If one views this kind of action as warfare, then the use of information-in-warfare has become more difficult and complex.

Information-As-Warfare

As bad as the situation in Mumbai, there are larger problems. *Information-in-warfare* is not only increasing in complexity, but *information-as-warfare* is emerging. New systems of nation-to-nation coercion via rapid, mass publication, unlimited computing power, and ubiquitous connectivity are threatening the old division of labor among organizations that handle this kind of threat at a national level. The goal is not just to more effectively harness information to shoot, move, and communicate in the traditional sense (using *information-in-warfare),* rather it is to harness *information-as-warfare* to impose one's will on adversaries.

For example, a number of nations are attempting to counter nuclear proliferation in Iran as a matter of policy. Unidentified political entities are pursuing these political goals via coercive means such as introducing the stuxnet virus into Iranian networks. The virus, which is information in the form of computer logic, effectively interfered with the Iranian uranium enrichment program.[20] When information becomes a means, in and of itself, to enforce an external policy decision, then information outstrips its traditional role of enabling battle on land, air, and sea. It becomes *information-as-warfare* or information warfare.[21] Whether or not stuxnet was produced by a military organization or even a nation state is irrelevant. The fact is that it represents a coercive means to a political end, which is the traditional role of the military in conflicts. Thus it is now possible for military organizations to harness *information-as-warfare*.[22]

Already, near peer competitors are pursuing this approach in the military sphere.[23] For example, China's conception of Information Warfare focuses on information well beyond the machine and network-based portion of the information environment.[24] Their targeting extends across the information environment to include "dumping information garbage; disseminating propaganda; applying information deception; releasing clone information; and establishing network spy stations" for espionage while concurrently defending themselves against such activities.[25] Not all of these activities take place in the context of machines and networks; however, they are all information related.

If information can and should be harnessed as a kind of warfare, not merely as a critical enabler in warfare, then the question becomes whether a service-level entity should be forged to conduct information warfare. History provides two precedents for

conferring service and service-like status for an emerging “domain” or kind of warfare. The establishment of the Air Force as a separate service department in 1947 and the establishment of Special Operations Command in 1987 are examples.[26]

The Air Force’s original *raison d’être* rested on two fundamental propositions: 1) an air force, if allowed to develop strategies independent from its ground-enabling missions, is capable of winning conflicts without the assistance of other service organizations; and 2) the dynamics of the air domain warrant radically different knowledge, skills, training, and culture.[27] Therefore, to succeed the Army Air Force had to break the Army’s constraints in order to realize their full potential.[28] Whether this same logic applies to the cyber domain or to information warfare is an interesting question. The same can be said for the Special Forces Command, which evolved beyond the conventional service departments mostly because of congressional initiatives.[29]

While there may be some justification for creating a separate information service, it does not appear likely at this time. The US currently cannot afford such a large-scale undertaking. Also, current joint doctrine recognizes that dominance in any single domain is insufficient to win most wars. It is necessary to maintain superiority across several domains to prevail in wartime.[30] The domination of the “cyber domain” alone will not likely prove decisive in future conflicts.[31] As one recent Vice Chief of the Joint Staff said, “The goal is not the single beautiful target that ends the war in one shot. That doesn’t exist… The military needs more of a brute-force approach that allows it to get at a thousand targets as quickly as possible.”[32] For the time being, military services may struggle to establish jurisdictional boundaries for the expanded framework of the cyber

domain; however, it is unlikely that the current structure will expand to create a cyber or information service. Instead, like Special Forces Command, US Cyber Command will be responsible for leveraging each of the services' cyber capability and will likely continue to borrow and consolidate emerging service components to defend the US and its interests in the cyber domain.[33]

Even if US Cyber Command continues to synchronize service efforts in the cyber domain, a holistic framework that addresses the information environment for information warfare could prove more effective. It would include all forms of information warfare not simply the ones that were cyber related. Non-cyber capabilities are necessary to secure our own "information sources" while also destroying or preventing the enemy from producing, storing, and effectively disseminating information. Therefore, constraining US Cyber Command to the cyber domain is a limiting construct.

In some ways, the Army has taken a broader, more comprehensive approach to the issue of information warfare over the last two decades. The Army's personnel organization is the result of deliberate efforts, in part, to build a force suitable to meet the challenges of the information age.

Information in the Army Personnel Structure

In July 1996 the Army Chief of Staff convened a task force to recommend personnel changes that maintain the excellence of the modern army while preparing for the 21st Century. The new Officer Personnel Management System (OPMS) had to maintain quality personnel who were ready for current and future wars while simultaneously supporting the institutional Army's most important functions.[34] The Army Chief of Staff's guidance was to "develop officers to meet the challenges of a changing

world—officers who can fight and win today's wars and wars of an uncertain future."[35] OPMS XXI, subsequently known as OPMS III was the result of his vision.

OPMS III organized an Information Operations career field containing seven functional areas in order to meet "the requirements of the 21st century information age. The *Army Vision 2010* document identified gaining information dominance as fundamental to all future Army patterns of operation."[36] Information Dominance is described in joint publications as operating without effective opposition or prohibitive interference in the information environment. Any system that delivers information dominance will require a robust and secure mission command system able to deliver a competitive advantage over an adversary's system— superior knowledge and information management, effective Operational Security (OPSEC) measures, disruptive cyber capability, military deception operations and more.[37]

The seven Army Information Operations functional areas included human and machine based specialties from public affairs to telecommunications engineering (see Figure 1). These specialties provided the means and expertise to handle many aspects of information in war. Army publications described a need to develop highly trained specialists to "take full advantage of information systems—both on the battlefield and in the institutional base," and to "fulfill the need for warfighters trained with the information related skills necessary in the next century."[38]

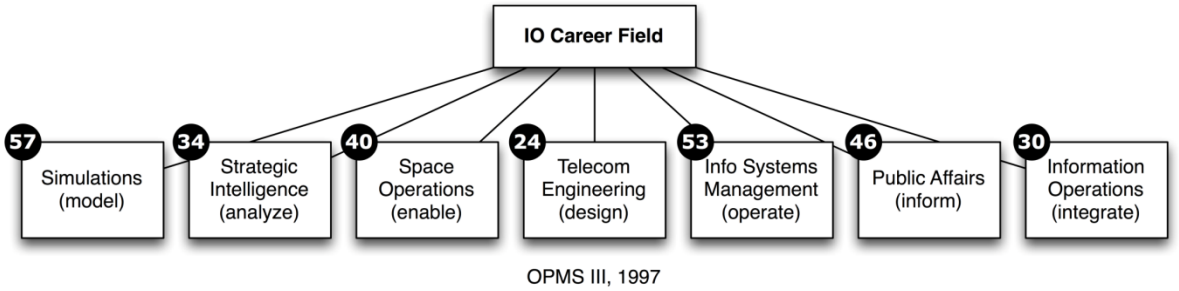

Figure 1. IO Career Fields Established with OPMS XXI

While information dominance requires broad action across a joint force, it also requires specialization. The problem is that specialization can turn into overspecialization, uncoordinated action and, in the worst case, waste.[39] Achieving a balance of specialization and integration is a difficult challenge.[40] The Army has many information related career fields and branches that are closely related. However the standard for delineating what requires a functional area, additional skill, or branch is difficult in a dynamic security environment.[41] The various iterations of officer personnel management policies continuously expand, contract, and reorganize the workforce. The top level grouping of branches and specialties determines categories for promotion, and these categories have changed over time. The taxonomy has gone from dual tracked, Combat Arms, Combat Support, Combat Service Support, and Special Branches in OPMS II; to single tracked, tiered career fields in OPMS III; to simply three groups in OPMS IV (see Figure 2).

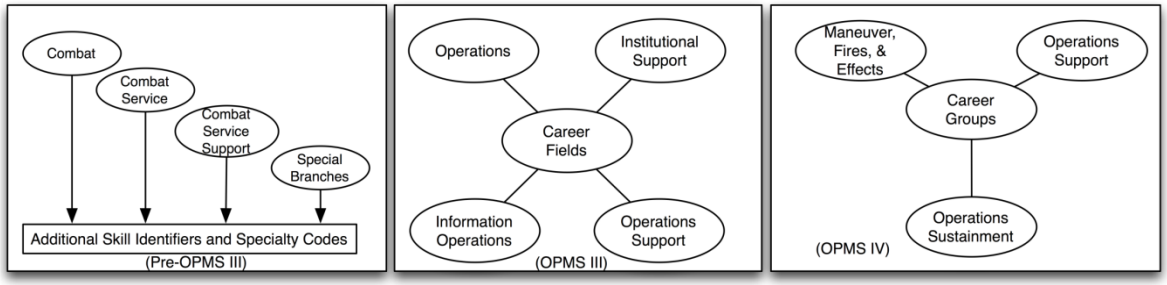

Figure 2. Various Army Organizational Structures and Concepts

It is difficult to identify the organizing principles behind various officer promotion groupings. As originally designed, IO Career Field officers competed against other information-related career fields for promotion. Eventually, these same career fields competed in different groups. For example, Public Affairs and Information Operations career field officers used to compete with Simulations and Network Systems Engineers. Now they compete with Infantry, Armor, and Artillery officers. This situation voids an important part of OPMS III. It would be more appropriate to re-consolidate these personnel into an Information Operations career group for promotion with similar information related disciplines.

The current organization has other consequences. For instance, the grouping of Information Operation specialties, Chemical officers, and Engineers into a single competitive category means that career field groupings exist as divergent disciplines rather than convergent, cooperative disciplines. The previous grouping of like-disciplines would be more equitable and consistent. This situation is complicated by the fact that functional areas are sometimes managed by basic branch officers. This creates potential conflicts of interest between branches and related functional areas such as the Intelligence Branch and the Strategic Intelligence Career Field.[42] The situation is also incoherent as a design for information dominance because it does not take full

advantage of a dedicated career field with IO-knowledgeable managers. Clearly, the officer management situation is not well structured for information dominance.

To examine potential paths out of this morass, we can look to historical precedents. An analogous situation existed in the years between WWI and WWII with the armor branch. One historical report describes the challenges in reforming manning policies:

> Congress, acting on General Pershing's recommendation, had deprived the Tank Corps, created during World War I, of its status as a separate combat arm. Between the wars the roles and missions of the armored forces in this country as in Europe were the subject of bitter internal dissension within the Army. The strongest opposition to the tank came naturally from the Cavalry whose chief, Maj. Gen. John K. Herr, in 1938 urged: "We must not be misled to our own detriment to assume that the untried machine can displace the proved and tried horse."[43]

That historical situation was ultimately resolved when the Armor Branch was provisionally established by the secretary of war in 1940. The subsequent Reorganization Act of 1942 abolished the offices of the chiefs of the combat arms as "an unnecessary staff layer(s)," transferring their powers to the Army Ground Forces (AGF) and "integrating the several arms into a single, unified fighting team."[44] All Army branches nested into the categories of Army Ground Forces (AGF), Army Air Forces (AAF), and Army Service Forces (ASF), pre-cursors to future manning constructs. These logical functional alignments provided for efficient and effective personnel management. It may be that the current Army can better manage its IO officers by establishing an information branch.

Alternatively, Intelligence and Signals Branches and other information related functional areas (24, 30, 34, 40, 46, 53, and 57— Telecom System Engineers, Information Operators, Strategic Intelligence Officers, Space Officers, Info Systems

Managers, and Computer Simulations experts) all have special skills that relate to the transmission of information and digital battlefield systems. These functional areas were part of the original, broader Information Operations Career Field established by OPMS III. They were designed to be "capable of integrating and optimizing the Army's relevant information, intelligence, information systems, public affairs, space operations and simulations to gain information dominance."[45] However, these technical specialties are just one part of information dominance. Except for the intelligence branch, which encompasses human intelligence, each of these branches and functional areas subordinate human factors to technical ones.

In terms of human information and influence factors, career management of officers working military deception, psychological operations, civil affairs, foreign and public affairs may not be optimally organized. The IO career field did not originally include PSYOP because that branch did not exist apart from Civil Affairs in 1997.[46] However, those specialties are information related and might be subsumed in the IO career field to create a comprehensive set of information specialties that include the human dimensions of information such as polling, target audience analysis, and target audience influence.

If information dominance is more than a machine-based affair, then the Army must take into account the dynamic of information interchange via direct human contact as well as network mediated contact. It must not settle for networks and nodes. The common link between human and machine systems is the information itself, which transcends both the human dimension and the cyber domain. Capitalizing on the human dimension along the seams of the cyber domain provides demonstrably improved

effectiveness in both areas. For example, well-crafted social engineering enables successful phishing attacks. Social engineering also can provide physical access to restricted information systems or other critical humans-in-the loop.[47] Additionally, human factors can be exploited to discern passwords and circumvent other physical safeguards that secure cyber infrastructure.[48] The increasing convergence of human social activity within a ubiquitous cyber domain makes the management of information-related personnel in different specialties inefficient. While cyber commands are pursuing limited network related objectives and human factors personnel are treating cyber as merely a means for transmitting information to target audiences, both are missing the opportunities afforded by closer integration and synchronization.

The concept of “mission command” further obfuscates the issue of information operations. Previously the three war-fighting functions of Command and Control (C^2), Intelligence, and Maneuver, represented a division of labor and a conceptual differentiation between signaling, producing intelligence, and directing operations through the publication of orders. The C^2 function has been replaced by mission command, which now includes knowledge management, information management, inform activities (public affairs), influence activities (PSYOP), and cyber-electro-magnetic operations while excluding orders production (an area handled by operations sections of the staff). Nothing is more important than commanding and controlling the Army’s vast forces in the field; however, the current force structure does not yield a coherent arrangement in officer functional areas versus core staff skills.

The Army has spent significant resources developing personnel with functional competencies in media, propaganda, intelligence, and communications technology

areas. Additionally, the Army recently established a “mission command” center of excellence at Fort Leavenworth to integrate many cross-functional information activities. However, some information related functional areas are being co-opted by cyber or re-assimilated into intelligence branches instead of re-organized into a “mission command” system-of-systems. Importantly, the holistic, combined arms approach to information dominance is now in jeopardy.[49]

The Army has adapted force structure steadily over time. Recent trends include the consolidation of closely related career fields and officer branches and the re-organization of those into multi-functional branches and advanced career tracks. For example, the Army Adjutant Generals Corps (Branch) merged with Human Resource Management.[50] The Finance Corps and the Comptroller Functional areas also merged. The Quartermaster, Ordinance, and Transportation branches also merged into a multi-functional Logistics Corps. Although officers are still commissioned into those three branches, they merge into a single Logistics branch as they become senior captains and majors. The Intelligence Branch has re-coded and reduced many Strategic Intelligence Functional Area positions. The PSYOP branch has begun to add discrete skill sets such as military deception and electronic warfare via an internal MISO (Military Information Support Operations) master practitioner career track. All of these changes have affected the continuity and coherence of Army personnel management. Notably, both the Navy and Air Force are facing similar challenges in managing information-related personnel specialties.

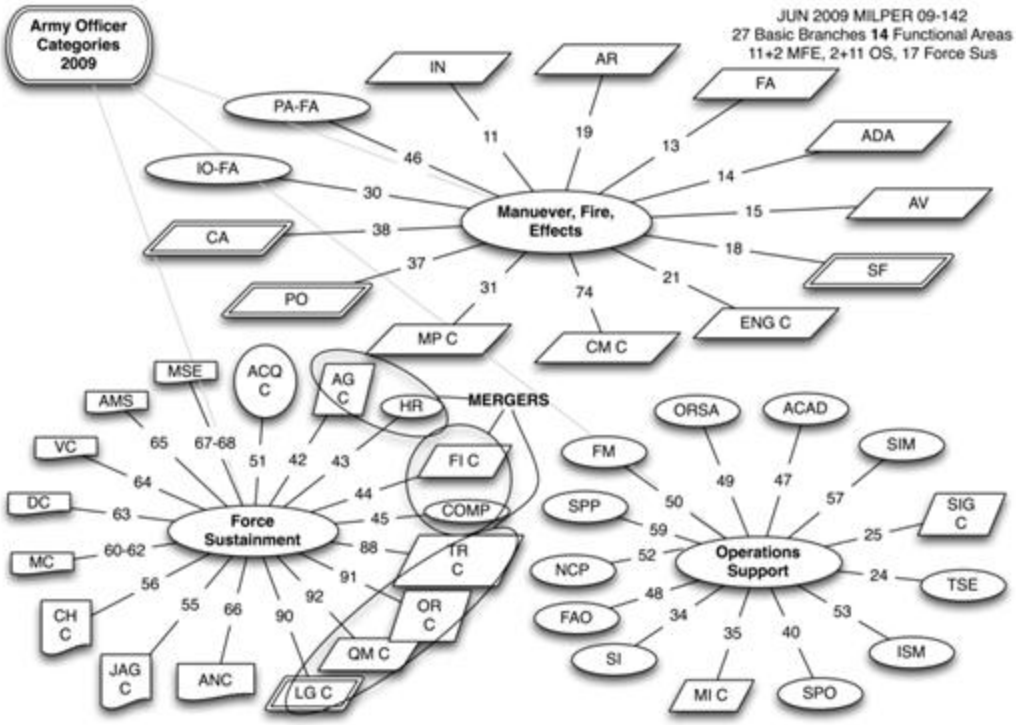

Figure 3. OPMS Organization of Branches and Career Fields

Other Department Models

The Department of the Air Force and Department of the Navy have undertaken significant efforts to manage information related career tracks under the cyber moniker. The Navy established an Information Dominance Corps, and at some echelons combined its N2 (intelligence) and N6 (communications) responsibilities.[51] Similarly, the Air Force established officer and enlisted cyber career paths that keep personnel in cyber-related positions throughout their careers.[52] The Navy and Air Force are investing broadly and deeply in cyber-related disciplines. In the Air Force's case, they are doing so largely to the exclusion of the human aspects of information operations. This is understandable given the clear demand for officers who can leverage cyber capabilities.[53] So far the Army approach has not been as broad as the Navy or as deep as the Air Force. The opportunity for Army redesign is ripe.

The Navy model is worth considering as an alternative because it acknowledges both the human and technical nature of information warfare. The vision for a Navy-based *Information Dominance Corps* is to develop and maintain a "battle management capability that synchronizes all elements of information, dominates the electromagnetic spectrum, and permits the Navy and our nation to wield information as a weapon."[54] The vision further describes an elevation of "information capabilities [that] evolve from 20th century supporting functions to a main battery of 21st Century seapower."[55] The vision goes on to define Information Dominance as "freedom of action to maneuver and act -- conduct offensive and defensive actions, kinetically and non-kinetically -- at the intersection of maritime, information and cyberspace domains." The Navy concept goes on to address information in and information-as-warfare along with officer personnel management.

For the Navy, information is no longer limited to an enabling role. For example, Navy *information-in-warfare* amplifies kinetic combat capabilities while Navy *information-as-warfare* delivers expanded maneuver space, new operational and strategic options, asymmetric operational effects, and capability for dominant control of the operating environment. Information as a weapon is applied to influence, deny, degrade, disrupt or destroy across the full range of maritime and naval missions.[56] The Navy's Information Dominance Corps' junior grade professionals are now required to strengthen and deepen their professional skills in their communities and sub-specializations, while also obtaining a broader understanding of cross-Corps disciplines. Senior officers within the Information Dominance Corps are also required to broaden their professional expertise, and a growing number of senior officers will be assigned to

cross-corps assignments.[57] These Navy personnel management initiatives can inform the development of Army management alternatives. The following section examines three viable alternatives for addressing the manning challenges associated with the increasing scope of information warfare.

Army Alternative 1: A Monolithic Information Corps (Similar to the Navy's IDC)

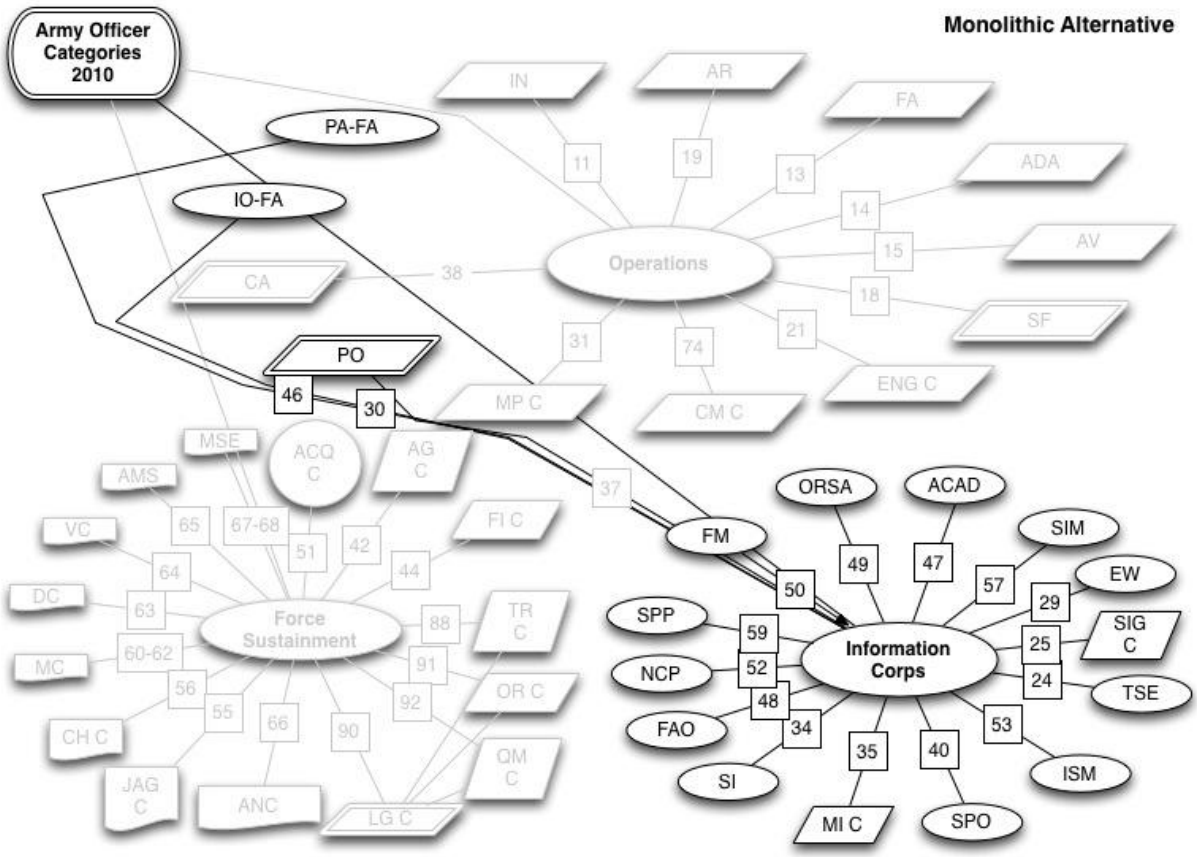

Figure 4. Monolithic Alternative

The Army analogue to this Navy model would be an Information Corps or Career Group that combines all information related officer branches and functional areas. If the Army were to combine its seven original Information Operations functional areas with Signal, Intelligence, and PSYOP branches it would have a broad base of information related fields. Adding Foreign Area, Strategic Plans and Policy, Academy Professors,

Force Modernization, and Operational Research functional areas could also expand the functional areas and integrate all information-related concepts and capabilities in the Army. Because the dynamics of information are constant and common across these disciplines, it makes sense to closely coordinate or combine them to gain efficiencies. It may even be possible to reduce the number of centers of excellence. The Army has taken this approach before with the combination of Infantry and Armor Centers of Excellence into the Maneuver Center of Excellence. In regard to information-related capabilities, the Signal, Intelligence, Mission Command, and JFK Centers of excellence could collaborate, combine, or more closely de-conflict their information related mission areas. Economies of scale would have to be found along the margins to make this an attractive alternative. It is the boldest, most comprehensive option.

Army Alternative 2: A Multi-functional Information Corps

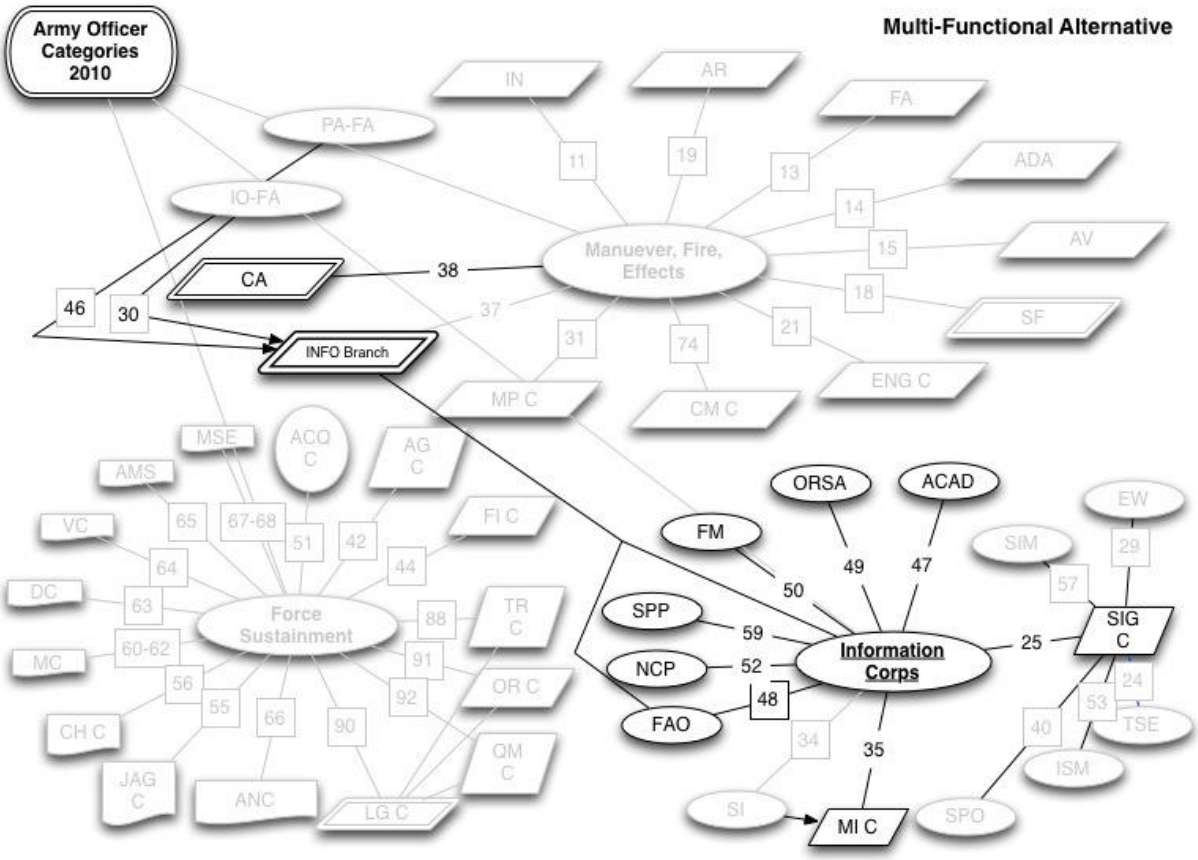

Figure 5. Multi-Functional Alternative

Alternatively the Army could choose to re-absorb its information related capabilities into three branches (Military Intelligence, Signal Corps, and a newly established Information Branch that combines newer information specialties and career fields). In this alternative, non-intelligence and non-signal related, human oriented information systems and mission command specialties would be subsumed into an Information Branch. Additionally, Strategic Intelligence would rejoin Military Intelligence; the Signal branch would absorb Electronic Warfare, Info Systems Management, Network Engineering, Simulations, and Operational Research along with the cyber mission. (See Figure 5)

This alternative combines the Army's non-technical, information-related disciplines into an overarching, multidisciplinary Information Corps, like the multifunctional Logistics Corps. All dynamics of information, especially as it passes between automated and human systems, could be studied, refocused or otherwise improved.

Military Information Support Operations (MISO) is currently part of the special operations community, and could continue under a special operations identifier for information branch personnel. A refined, Information Branch would replace the IO Career Field Construct and eliminate confusion and duplication of effort. Technical systems and force structure would come from the Military Intelligence Branch, which currently houses the Army's more sophisticated cyber capabilities.

Army Alternative 3: Joint Reliance (Human and Technical Division of Labor)

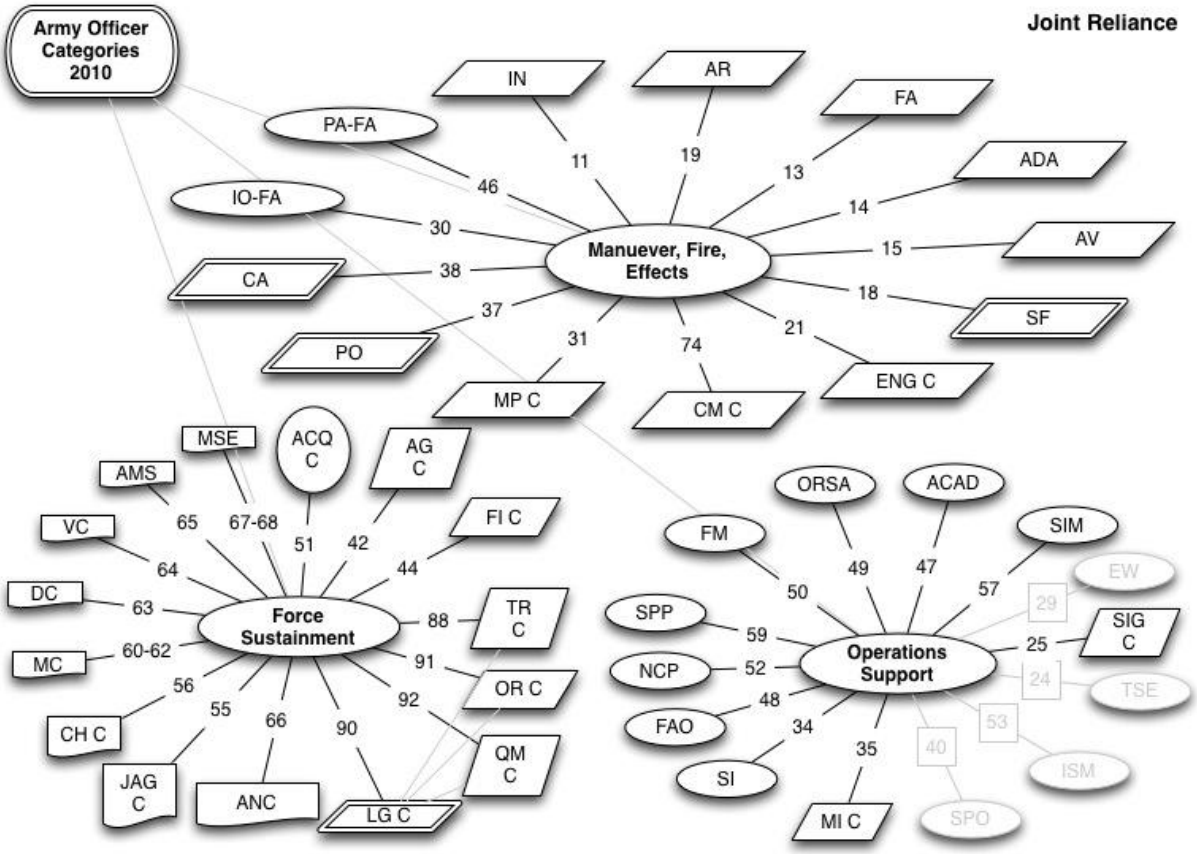

Figure 6. Increased Service Interdependence

Increased service interdependency is also an option. The Navy and/or Air Force are more technically oriented services.[58] These services could attend to information warfare's technical aspects while the Army supports the human dimension of information warfare. The advantage here is the elimination of service redundancies and increased reliance on service interdependent specialization. For instance, the Navy and Air Force could deliver electronic fires, special broadcasting capabilities, and offshore cloud computing, just as it does ship to shore artillery and combat air support. This concept would synchronize service capabilities across the information environment for joint effects. At the same time it would clarify funding streams and reduce duplicative

capabilities across DOD. Likewise, the Army's contribution would focus on the human dimension of information warfare. The Army currently has the preponderance of psychological operations forces, ground intelligence, and special operators. It could facilitate information warfare via close access, operations deep behind enemy lines, deception, information support, etc.

If the Navy is currently leading in integrating technical capabilities that achieve information dominance, then perhaps the best way forward is a division of labor across the remaining services. If the Navy can grow itself into a service that allows "our nation to wield information as a weapon" in the Cyber and Electromagnetic Spectrum, then the Army could focus on population centric information support missions.[59] Thus the Army could forego investment in high tech cyber and electronic warfare support. Instead it would invest and specialize in the human dimension and capitalize on its cultural and organizational predilection toward sustained, land-based operations in and among populations.

Populations live on the land domain. So traditional, human-based information capabilities such as Public Affairs, PSYOP, HUMINT, Foreign Area Officers, Operations Security and Military Deception Officers represent comparatively more useful capabilities for the Army. With a joint division of labor the Army force structure could be reduced substantially. The greatest impact would be in functional areas 24, 25, 29, 35, 40, and 53, because they are more technical in nature and have the greatest potential to address problems in cyber and space areas undertaken by the other services. The precedent for this alternative is the manpower and expertise the Navy loaned the Army to address its weak electronic warfare program in the first five years of OPERATION

IRAQI FREEDOM.[60] On the plus side, MI and Signal officers could return to their original operations support missions and forego the burden of undertaking a huge effort to organize for cyber operations.

There are drawbacks with this option. The specialization of information warfare by service would make integration along the seams of information warfare across technical and human areas problematic if not impossible. This, in turn, would prevent the synergy expected from a more integrated approach pursued within each service.

Comparison of Alternatives

The current environment requires an Army information posture capable of meeting the challenges of the 21st century in a fiscally constrained environment. The current organization and management of the Information Operations Career Field has become convoluted over time and requires reform and redesign because of the advent of cyber, the emergence of the PSYOP branch, and the advent of mission command as a war-fighting function.

All three alternatives to the status quo are suitable, feasible, and desirable, especially given that they all entail efficiencies or increased effectiveness. The most aggressive approach, and the most advisable, would be the establishment of a Monolithic Information Corps. The Navy model provides the precedent for this course of action, and the recent actions of potential adversaries provide compelling justification. The monolithic option refocuses the information effort via the officer personnel structure. However, such an effort would extend to the warrant, enlisted, and civilian work forces. Establishing a Monolithic information Corps is the broadest, most comprehensive approach that could also result in efficiencies. It responds to the present need to

harness *information-in-warfare* and the emerging need to harness *information-as-warfare* by posturing the Army to do both.

On the other hand, in a severely constrained fiscal environment the Army may need to adopt an alternative that preserves its core missions and assets by handing off what is viewed as a more technical cyber enterprise. That would mean transferring the more technical information capability requirements such as cyber and electromagnetic warfare to other, more technically oriented services like the Navy and Air Force. Outsourcing critical functions and roles can be a risky proposition, but it might be advantageous to clarify service roles and missions in this dynamic environment. The risks to the Army would have to be carefully weighed because its information infrastructure is the most dynamic— expanding, contracting and changing with every large-scale deployment in a way that the Air Force, Navy, and Marines' infrastructure does not.[61]

A Multi-functional Information Corps is an appropriate alternative in a moderately constrained fiscal environment. Maintaining traditional branches while consolidating newer functional areas into an Information Branch would not yield maximum efficiency, but would be more palatable to longstanding information-related branches. The precedent set by the multi-function logistics corps helps justify this approach. The main problem with this alternative is that it maintains and obscures the seam between intelligence, signal, and the emerging cyber doctrine, which is a strange admixture of information assurance, cyber exploitation, and electronic warfare.

The dynamics of information, whether transiting human minds or machine networks, departs from the dynamics of kinetic operations and terrain bound

operations— so much so that handling both *information-in-warfare* and *information-as-warfare*, requires deep expertise at the tactical, operational, and strategic levels.[62] It also requires more of the traditional Army specialties. The Army recognized this in the mid 1990s but has not yet harnessed the potential afforded by strategically organizing these loosely associated capabilities.[63]

The upcoming century will be one of information conflict and potentially wide scale information warfare. If the past few years is an indication, the role of *information-as-warfare* will expand. It will also require a new kind of integration across all information-related functional specialties. The role of information in operational and strategic environments is potentially immense, and much like the protection of territorial integrity, sovereignty, and freedom of the global commons, protection of our nation's information capital will prove vital to America's economic and social wellbeing.[64]

The correct strategy for warfare in the information age is not an overly technical approach-- neither is it an overly non-technical one. The correct focus is on the seams between information systems and human beings. The greatest potential is derived from manipulating how information affects and influences popular support as well as human and automated decision activities at the nexus between humans, media, and machines. Information dominance exploits the seams that connect people, data, and computers. Machine processes and human interpretation both influence operations. The explosive increase in the use of social media intelligence is just one emergent artifact of the information age.[65] It serves as a sign post for leveraging intelligence, public affairs, and psychological operations in new ways to integrate their effects. This kind of emergent environment also exemplifies why a consolidation of related branches and functional

areas is a necessary evolution on the path toward a more effective Army personnel system.

Conclusion and Recommendations

The information industry is the leading source of wealth in the United States. Information is power.[66] It is also a national resource well worth defending. Technology, publication, and telecommunications industries process, move, and publish information to produce wealth and influence. At the same time, the information age is empowering other governments and individuals that could threaten the United States' wellbeing via this emerging information ecosystem. The Army must determine how best to harness information and how best to leverage the enormous US information dominance potential.

Information contributes to warfare by extending command and control, shaping coalitions, revealing enemy capabilities and intentions from afar, and enabling remote capabilities that can extend US reach. This is *information-in-warfare*. However, *information-as-warfare* is also emerging, and there are unrealized opportunities to exploit its potential. This paper argues for the formation of a monolithic information corps inside the Army capable of integrating all information-related activities to achieve information dominance on the battlefield.

Whatever path the Army follows, it must assure information-related capabilities continue to develop and remain in the arsenal whether in a joint context or as an emergent Army capability. The volatile information environment is forcing rapid organizational changes and the development of new, related systems and processes. To stay abreast of the dynamic operational environment, the Army must view

Information Operations holistically and seek both efficient differentiation of tasks and missions and effective integration of capabilities.

In the final analysis, the best approach for the Army is to resist specialization in favor of a combined-arms approach to conflict in the information environment. Therefore the Army should consolidate its information-related specialties to facilitate future growth, development, and most importantly, employment. OPMS III gave the Army an "effective and flexible" tool for organizing its personnel and functional organizations.[67] It is time to exercise that flexibility to better prepare for information age warfare.

Endnotes

[1] Huba Wass de Czege, "Rethinking IO (Information Operations): Complex Operations in the Information Age," *Military Review,* (88:6, November-December 2008): 26. http://usacac.army.mil/CAC2/MilitaryReview/Archives/English/MilitaryReview_20081231_art006.pdf (accessed November 2012).

[2] Dennis Reimer, *Army Vision 2010*, (Washington, DC: US Department of the Army, 1996): 17. Army Vision 2010 described Information Operations (IO) as both offensive and defensive efforts to create a disparity between what [The Army] know[s] about our battlespace and operations within it and what the enemy knows about his battlespace. The purpose of IO is to gain "information dominance," which it describes as "The Key Enabler in 21st Century Operations." It included operations with the combined disciplines of psychological operations, military deception, radio frequency energy management, and an "aggregate of technologies" that assist in understanding and shaping the information dimension of the battlespace. Information dominance was further described as "the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same."

[3] "Annual Ranking of America's Largest Corporations: Most Profitable," *Money Magazine Online,* May 21, 2012, http://money.cnn.com/magazines/fortune/fortune500/2012/performers/companies/profits/ (accessed on March 3, 2013).

[4] US Congressional Budget Office, (Washington, DC: US Congressional Budget Office, October 5, 2012), http://www.cbo.gov/publication/43657 (accessed March 3, 2013). Terry Allison, *Christian Science Monitor*, August 24, 2012, http://www.csmonitor.com/USA/Society/2012/0824/Got-broadband-Access-now-extends-to-94-percent-of-Americans (accessed March 3, 2013).

[5] US Joint Chiefs of Staff, *Department of Defense Dictionary of Military and Associated Terms,* Joint Publication 1-02 (Washington, DC: US Joint Chiefs of Staff, April 14, 2006), 139.

The information environment is the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information.

[6] "Annual Ranking of America's Largest Corporations."

[7] David F. Carr, *Information Week,* January 25, 2012, "Facebook: The Database Of Wealth And Power," http://www.informationweek.com/thebrainyard/news/social_networking_consumer/232500412/facebook-the-database-of-wealth-and-power.

[8] Joseph F. Nye, Jr., "America's Information Edge," *Council on Foreign Relations* (March/April 1996): in Proquest (accessed March 6, 2013).

[9] Cisco Systems Inc., "Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2012–2017," http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white_paper_c11-520862.html (accessed March 3, 2013). This source describes the commodities that are delivered over the web and that consume the most bandwidth, *e.g.,* movies, software, and subscription-based information.

[10] Martin E. Dempsey, *Chairman's Strategic Direction to the Joint Force* (Washington, DC: US Joint Chiefs of Staff, February 6, 2012), 4.

[11] M.G. Mullen, *US National Military Strategy 2011*: *Redefining America's Military Leadership* (Washington, DC: US Joint Chiefs of Staff, February 8, 2011), 3. This document asserts that globally connected domains such as cyberspace are being increasingly challenged by both state and non-state actors.

[12] US Joint Chiefs of Staff, *Joint Operations,* Joint Publication 3-0, Chapter V, (Washington, DC: US Joint Chiefs of Staff, August 20, 2011), V-47. Full-spectrum superiority is the cumulative effect of dominance in the air, land, maritime, and space domains and information environment (which includes cyberspace). Superiority means the conduct of joint operations without effective opposition or prohibitive interference. It is essential to joint force mission success.

[13] Joby Warrick, "Clinton: US Losing Public Relations Battle," *The Washington Post Online,* March 3, 2011, http://www.washingtonpost.com/wp-dyn/content/article/2011/03/02/AR2011030206898.html (accessed November 2012).

[14] Timothy Thomas, "Like Adding Wings to the Tiger: Chinese Information War Theory and Practice," (Fort Leavenworth, Kansas, *Foreign* Military Studies Office, July 1, 2003), http://fmso.leavenworth.army.mil/documents/chinaiw.htm (accessed on February 6, 2013), 3; "New York Times' The Target Of Chinese Cyber Attack." Narrated by David Folkenflick. All Things Considered, *National Public Radio,* January 31, 2013. http://www.npr.org/2013/01/31/170787379/new-york-times-the-target-of-chinese-cyber-attack (accessed on February 6, 2013).

[15] Martin C. Libicki, *What Is Information Warfare?* (Washington, DC: National Defense University, 1995), 76-95. According to Libicki nformation warfare is conflict involving the protection, manipulation, degradation, and denial of information; there are seven forms that include 1) command-and-control warfare (which strikes against the enemy's head and neck), 2)

intelligence-based warfare (which consists of the design, protection, and denial of systems that seek sufficient knowledge to dominate the battlespace), 3) electronic warfare (radio-electronic or cryptographic techniques), 4) psychological warfare (in which information is used to change the minds of friends, neutrals, and foes), 5) "hacker" warfare (in which computer systems are attacked), 6) economic information warfare (blocking information or channeling it to pursue economic dominance), and 7) cyberwarfare (a grab bag of futuristic scenarios differentiated from hacker warfare because its aim is not disrupting systems but exploiting them to attack individuals).

[16] Eliot A. Cohen, “A Revolution in Warfare: Technology Strikes Again,” *Council on Foreign Relations* (March/April 1996): 2, in Proquest (accessed March 3, 2013).

[17] Grant T. Hamilton, “Myths of the Gulf War: Some Lessons Not to “Learn,”” *Airpower Journal*, (Fall 1998): 11. Communications, surveillance, navigation, and the use of space-based assets made a significant difference in the effectiveness of forces during the Gulf War.

[18] This was a terrorist event on the same scale as a tactical battle or engagement. It was very successful for the perpetrators.

[19] Noah Schactman, “How Gadgets Helped Mumbai Attackers,” *Wired Magazine*, December 8, 2008, http://www.wired.com/dangerroom/2008/12/the-gagdets-of/ (accessed on December 12, 2012).

[20] James P. Farwell and Rafal Rohozinski, “Stuxnet and the Future of Cyber War," *Survival*: Global Politics and Strategy, Issue 53:1 (2011): 25. http://www.tandfonline.com/doi/abs/10.1080/00396338.2011.555586 (accessed December 12, 2012).

[21] The terms *information warfare* and *information-as-warfare* are interchangeable. The use of *information-as-warfare* emphasizes that the operational environment for this type of warfare is largely a global information environment comprised of information, information systems, and humans in the information processing or programming loop.

[22] Vice Admirals Kendall L. Card and Michael S. Rogers. "The Navy's Newest Warfighting Imperative." *United States Naval Institute. Proceedings* 138, no. 10 (2012): 22-6, http://search.proquest.com/docview/1115097975?accountid=4444 (accessed on March 6, 2012).

[23] Timothy Thomas, “Like Adding Wings to the Tiger, 3.

[24] US Joint Chiefs of Staff, *Department of Defense Dictionary of Military and Associated Terms*, 139. The information environment is the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information.

[25] Timothy Thomas, “Like Adding Wings to the Tiger, 3.

[26] William C. Story, *Military Changes to the Unified Command Plan: Background and Issues for Congress,* Congressional Research Service (Washington, DC: US Library of Congress, Congressional Research Service, June 21, 1999), 8.

[27] Charles A. Stevenson, "The Story Behind the National Security Act of 1947," *Military Review*, (May/June 2008): 20.

[28] Stephen L. McFarland, *A Concise History of the US Air Force,* (Bolling AFB: US Air Force History Support Office, 1997), 23-25. http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA433274 (accessed on December 19, 2012).

[29] William C. Story, *Military Changes*, 8.

[30] US Joint Chiefs of Staff, *Joint Operations,* Joint Publication 3-0, Chapter III, (Washington, DC: US Joint Chiefs of Staff, August 20, 2011), 29.

[31] GEN Michael E. Ryan, "The Leverage of Airpower," interview by John A. Tirpak, *Air Force Magazine*, May 1999, 34.

[32] Ellen Nakashima, "With Plan X, Pentagon seeks to spread US Military Might to Cyberspace," *Washington Post,* May 30, 2012, 5. http://articles.washingtonpost.com/2012-05-30/world/35458424_1_cyberwarfare-cyberspace-pentagon-agency (accessed on February 17, 2013).

[33] Lisa Daniel, "Cyber Command Synchronizes Services' Efforts," *US Department of Defense Federal Information News*, Dispatch, July 9, 2010, http://www.defense.gov/news/newsarticle.aspx?id=59965 (accessed on January 23, 2013).

[34] MG David H. Ohle's, "OPMS XXI—An integrated Strategy," interview by Mary Blake French. *Army Magazine*, February 1997, 49-56, www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA500903 (accessed on January 23, 2013).

[35] Officer Personnel Management Task Force XXI, *Final Report to Army Chief of Staff*, (Washington, DC: Department of the Army, July 9, 1997), xix. usacac.army.mil/CAC2/cgsc/carl/docs/OPMSXXI.pdf (accessed on January 23, 2013).

[36] Ibid.

[37] Dennis Reimer, *Army Vision 2010*, 17.

[38] US Department of the Army, *Commissioned Officer Professional Development and Career Management*, DA Pamphlet 600-3 (Washington, DC: US Department of the Army, October 1, 1998), 219.

[39] LTC Christopher J. Munn, "The Evolution of OPMS XXI: The Need to Specialize Military Intelligence Officers," (Carlisle Barracks, PA, US Army War College, April 2001), 11.

[40] Ibid., 9.

[41] US Department of the Army, *Commissioned Officer Professional Development and Career Management*, DA Pamphlet and Army Regulation 600-3 (Washington, DC: US Department of the Army, 1983, 1986, 1989, 1998, 2005, 2007, 2010). Manuals include between 38 and 48 branches and functional areas between 1983 and 2010.

[42] Annette L. Torrisi, “The Military Intelligence Officer Corps: Evolving Into The 21st Century,” (Carlisle Barracks, PA, US Army War College, April, 2001), 17. LTC Annette L. Torrisi, a strategic intelligence functional officer, points out an attitude of managing *haves* and *have nots* in regard to joint management of Intelligence Branch officers and Strategic Intelligence Functional Area officers.

[43] James E. Hewes, Jr., *From Root To McNamara, Army Organization And Administration* (Washington, DC: Center Of Military History, United States Army,1975), 65-66.

[44] Ibid., 68-69.

[45] US Department of the Army, *Commissioned Officer Professional Development and Career Management*, Department of the Army Pamphlet 600-3 (Washington, DC: US Department of the Army, 2005), 397.

[46] Ibid., 2.

[47] Nate Anderson, “How One Man Tracked Down Anonymous — And Paid a Heavy Price, *Wired Magazine*, February 10, 2011, http://www.wired.com/threatlevel/2011/02/anonymous/ (accessed on March 3, 2013).

[48] Peter Benesh, “Corporate Espionage Taking Over Where Cold War Spying Left Off: Companies Aren't Just Spying On Rivals, They're Also Getting The Skinny On Clients, Potential Partners,” *Investor's Business Daily*, October 10, 2000. http://search.proquest.com/docview/1026809169?accountid=4444 (accessed March 2, 2013).

[49] *Information* joined leadership, maneuver, firepower, and protection as an element of combat power with the publication of the 2001 Operations Field Manual 3.0. These elements were pre-cursors to the battlefield operating systems and warfighting functions. The 2006 Operations Capstone Concept devoted a chapter to Information Superiority; however, in 2008 an updated version of FM 3.0 removed the chapter and substituted a chapter entitled *Mission Command*.

[50] Army Military Personnel Message 09-142, *Functional Designation (FD) Policies And Procedures*, (Fort Knox, KY: US Army Human Resources Command, June, 18, 2009),1.

[51] US Department of the Navy, *Navy Information Dominance Corps Human Capital Strategy*, (Washington, DC: US Department of the Navy, May 2010), 12. http://www.public.navy.mil/fcc-c10f/Strategies/Navy_Information_Dominance_Corps_Human_Capital_Strategy.pdf (accessed on December 19, 2012).

[52] Susan Hall, “Air Force Creating Cyber Career Path,” *IT Business Edge Online*, March 1, 2012, http://www.itbusinessedge.com/cm/blogs/hall/air-force-creating-cyber-career-path/?cs=49893 (accessed on January 18, 2013).

[53] Stu Magnesun, “Air Force Cyber-Operations Wing to Go on Hiring Binge (UPDATED),” *National Defense Magazine*, January 17, 2012, http://www.nationaldefensemagazine.org/blog/lists/posts/post.aspx?ID=1026 (accessed on January 10, 2013).

[54] Navy Information Dominance Corps Human Capital Strategy, May 2010, http://www.public.navy.mil/fcc-c10f/Strategies/Navy_Information_Dominance_Corps_Human_Capital_Strategy.pdf (accessed on December 19, 2012).

[55] Ibid., 3.

[56] Ibid., 4.

[57] Ibid., 7.

[58] Carl H. Builder, *The Masks of War: American Military Styles in Strategy and Analysis*, (Baltimore: Johns Hopkins University Press, 1989), 19.

[59] US Department of the Navy, *Navy Information Dominance Corps Human Capital Strategy*, (Washington, DC: Department of the Navy, May 2010), http://www.public.navy.mil/fcc-c10f/Strategies/Navy_Information_Dominance_Corps_Human_Capital_Strategy.pdf (accessed on December 19, 2012).

[60] Jet Bibler, "Rebuilding the Army's Electronic Warfare Capability," *The Nexus,* February 26, 2009, http://usacac.army.mil/cac2/cew/nexus/NEXUS_VOL_2-2_-_COL_Bibler.pdf (accessed February 18, 2013).

[61] While other services generally rely on the same telecommunications links while in the air or afloat, the Army extends cyberspace on the ground within its operating environment. It is not possible for the Army to outsource or plant its information infrastructure in one place or to rely exclusively on satellites. Thus the risks of increased inter-service reliance would have to be weighed carefully.

[62] Jan Kallberg and Bhavani Thuraisingham, "Cyber Operations, Bridging from Concept to Cyber Superiority", *Joint Forces Quarterly*, no. 68, (January 2013): 54.

[63] GEN Dennis Reimer, *Army Vision 2010*.

[64] President Barack Obama, *National Security Strategy* (Washington, DC: The White House, May 2010), 22.

[65] Andrew Marvin, "Social Media Intelligence: Log In, Tune In, Don't Drop Out" *Small Wars Journal Online*, http://smallwarsjournal.com/jrnl/art/social-media-intelligence (accessed December 13, 2012).

[66] Joseph F. Nye, Jr., "America's Information Edge," 1.

[67] LTC Frank Pedrozo, "OPMS XXI: Implications for SOF," *Special Warfare* 11 (Winter 1998), in Proquest, http://search.proquest.com/docview/199422600 (accessed February 14, 2012).