NATIONAL DEFENSE UNIVERSITY
NATIONAL WAR COLLEGE

CYBER POWER THEORY FIRST, THEN INFORMATION OPERATIONS?

ANTOINETTE G. SMART
CORE COURSE 5605
MILITARY STRATEGY AND OPERATIONS
SEMINAR E

PROFESSOR
COLONEL DAVID PEELER

ADVISOR
COLONEL JOHN NELSEN

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
2001		**00-00-2001 to 00-00-2001**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Cyber Power Theory First, Then Information Operations?	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **National War College,300 5th Avenue,Fort Lesley J. McNair,Washington,DC,20319-6000**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
The original document contains color images.

14. ABSTRACT
see report

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**		**13**	

Cyber Power Theory First, then Information Operations?

> *In less than one generation, the information revolution and the introduction of the* ***computer*** *into virtually every dimension of our society has changed the way our economy works, how we provide for our national security, and how we structure our everyday lives.*
>
> *In the future,* ***computer****-related technologies will continue to open new vistas of opportunity for the American people.*
>
> *Yet this new age of promise carries within it peril. All* ***computer****-driven systems are vulnerable to intrusion and destruction. A concerted attack on the* ***computers*** *of any one of our key economic sectors or governmental agencies could have catastrophic affect.*
>
> *We know that the threat is real. Where once our opponents relied exclusively on bombs and bullets, hostile powers and terrorists can now turn a laptop* ***computer*** *into a potent weapon capable of doing enormous damage. If we are to continue to enjoy the benefits of the Information Age, preserve our security, and safeguard our economic well-being, we must protect our critical* ***computer****-controlled systems from attack.*
>
> **President William J. Clinton**
> "Defending America's Cyberspace"
> The White House, 2000

The words we use to express ideas and concepts matter. To be present at the beginning of the twenty-first century, in the midst of an "information age," with no theory of *information* operations (IO) seems disconcerting, at least on the surface. Think tanks, government research organizations, and learned individuals have all pointed to the need for a viable theory of IO, yet no such theory has emerged. Despite the lack of a theory or national strategy for IO, the U.S. military does have IO organizations, doctrine, and training. The Department of Defense has the Joint Information Operations Center (JIOC), which provides "full-spectrum IO support" to CINCs and CJTFs. Each military Department has its own Information Warfare Center (IWC), which provide IO support to their respective services – AFIWC for the Air Force, Fleet IWC

(FIWC) for the Navy, and Land Information Warfare Agency (LIWA) for the Army. The U.S. military now has IO units, with some services redesignating intelligence units as IO units. One example is the mass Air Force redesignation of its Intelligence Wing and subordinate squadrons. The U.S. military has both joint and service IO doctrine – in some areas it is consistent, in other areas it is not. And there are many highly technological tools for IO, so of course there must be training. But there is no theory of IO from a national perspective. Carl von Clausewitz said that the primary purpose of theory is to clarify concepts and ideas that have become confused and entangled. A plethora of questions emerges from the apparent entropy surrounding the development of a theory of IO.

What does our national leadership think about information power and IO? Have we become so enamored by the explosion of information technology that we have not expended the intellectual capital required to discover the nature, or essence, of IO? The technical *means* available are *shaping* the current and projected *practices* of information operations. Are we letting the *practices* of IO *shape how we think* about information operations. And in so doing, are we letting *means shape* our *theory* of IO? Or, more fundamentally, is the concept of ***information*** operations too broad and all-inclusive to derive a useful theory for? Should we rather seek to understand cyberspace as an emerging domain of conflict? This paper seeks to explore possible answers to these important questions.

The Importance of Information in our National Strategy

The *National Security Strategy of the United States* describes our national approach to planning for and dealing with the future. It is the President's strategic vision and concept plan for the nation and is required by the Goldwater - Nichols Defense Department Reorganization Act of 1986. This document should assist in the development of a theory of information

operations because it expresses the relative importance that information power holds within the nation's overall strategic outlook.

A National Security Strategy for a Global Age, December 2000 (NSS, December 2000), represents the past administration's attempt to set a tone of continued engagement in an increasingly interconnected world. The title itself portends the extraordinary impact of the "information age" in facilitating global interconnectedness – both a source of strength and vulnerability. From an information perspective, the document falls short in recognizing *information* as an *element of national power*. It does address the importance of ensuring critical infrastructure protection, leveraging public diplomacy, maintaining information superiority, improving cyber security, and enhancing our ability to defend against hostile information operations. *NSS, December 2000*, provides a strategic definition of information superiority and addresses defensive and what we have termed "perception management" operations. A deeper look into the national strategy may yield some explanation as to why it is so difficult to develop a theory of information operations.

In the *Preface* to *NSS, December 2000*, President Clinton concludes by stating, "America today has power and authority never seen before in the history of the world. We must continue to use it . . . to seize the opportunities and meet the challenges of a global age."[1] Diplomatic/ political, military, and economic elements of national power are highlighted as the primary means of dealing with strategic situations that present a threat to our national interests and/or our national values. A few specific examples of the absence of information as an element of national power are illustrative. In the lead chapter titled, *Fundamentals of the Strategy,* the national response to new and emerging threats is dealt with by restructuring our national security apparatus to address new threats with ***diplomatic, economic, and military tools***.[2] America's

ability to prevent crises through the proactive use of ***diplomatic, economic, political and military presence tools*** is a preferable alternative, in terms of blood and treasure, to managing conflict.[3] And finally, the *NSS* states that, "There are times when the nexus of our interests and values exists in a compelling combination that demands action – ***diplomatic, economic, or military***."[4] There are numerous references throughout this document to instruments of power or strategic tools that do not mention information. While information operations capabilities are imbedded in each expressed element of national power, information is not viewed in and of itself as an element of national power – at least in the *NSS*. These three examples in the lead chapter point to a nation, or at least a national leadership, that has not fully come to terms with the role of information power in a "global age."

Maintaining national information superiority is purported as something very important to do, yet, it is only mentioned once within the chapter on *Implementing the Strategy*. The three principal elements of America's strategy are: S*haping the Environment, Responding to Threats and Crises*, and *Protecting the Homeland*.[5] It is noteworthy that the first mention of the importance of maintaining information superiority is made in the section that addresses *Responding to Threats and Crises*. In almost an afterthought and with a very narrow approach, the *NSS* states, "We are *also* committed to maintaining information superiority – the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting and/or denying an adversary's ability to do the same."[6] In the section on *Shaping the International Environment*, earlier in this same chapter, the *NSS* highlights the criticality of the intelligence community requirement to provide comprehensive collection and analytic capabilities to accomplish a host of tasks, including the maintenance our information advantage in the international arena.[7] Does this say something about how America's leadership feels regarding

the capability of information superiority to provide value-added in the element of S*haping the Environment*? The words indicate that information advantage/superiority is relegated to an intelligence community task vice a critical function deserving a comprehensive and integrated national approach.

Defensive information operations seem to be the "coin of the realm" in the current *NSS*. *Critical Infrastructure Protection* is linked to both vital and important national interests. The United States will "do what we must," to include the use of military force even in the form of unilateral action, to protect our critical infrastructures – energy, banking and finance, telecommunications, transportation, water systems, vital human services, and government services – from disruption intended to cripple their operation.[8] The *NSS* devotes an entire section on the strategic plan element of *Protecting the Homeland* to *Critical Infrastructure Protection*. The section explains, in great detail, the recognition that the information technology infrastructure that fuels our economy and national security is fraught with interdependencies and vulnerabilities.

To deal with these growing vulnerabilities and interdependencies, President Clinton initiated the *National Plan for Information Systems Protection* in January 2000.[9] The *Plan* presents a comprehensive vision creating the necessary safeguards to protect the critical sectors of America's economy, national security, public health, and safety.[10] The *Plan* and the National Infrastructure Protection Center (NIPC)[11] are discussed at length. The *NSS* also highlights the necessity for public and private sector cooperation to protect the full range of our critical infrastructure. It is very clear from the NSS, and the range of governmental initiatives that underpin it, that defending our critical infrastructure from cyber-attack is a national security high priority.

Another aspect of IO is captured in the *NSS* – perception management. I prefer to label this activity or capability *perception influence* because perception is something that seems difficult to impossible to *manage* but certainly subject to savvy influence. America's ability to influence perceptions worldwide primarily resides in the area of *Public Diplomacy*. *Public Diplomacy* is spotlighted as an increasingly vital component of our national security strategy. It is defined as America's efforts to transmit information and messages to peoples around the world. The programs focus on informing and influencing foreign publics in support of our national interests, broadening the dialogue between U.S. citizens and institutions and their counterparts abroad, and improving mutual understanding by reaching out to future leaders and informing the opinions of current leaders through academic, professional and cultural exchanges.[12]

The *NSS* outlines the key aspects of Presidential Decision Directive 68 (PDD-68), entitled "International Public Information (IPI)." PDD-68 defines activities that make effective use of America's information capabilities to advance U.S. interests abroad. IPI activities are designed to improve U.S. capability to coordinate national security related information efforts to improve their successful integration into foreign and national security policy and execution.[13] *Public Diplomacy* actions conducted over the World Wide Web/INTERNET are an increasingly valuable way to reach a larger number of people worldwide. This was demonstrated during the recent situation involving the downed EP-3 reconnaissance plane and the Chinese pilot that lost his life. Although the Chinese government was providing their people with a censored version of America's statement of sorrow over the loss of the Chinese pilot, Chinese people connected to the INTERNET could get a voice and video stream of the actual speeches made by American diplomats and leaders and then decide for themselves what really happened. Cyberspace is

providing a key venue for *Pubic Diplomacy* activities by enabling increased access to previously closed societies.

What can we derive from this analysis of the *NSS* with respect to strategic thought on the importance of information and information operations? Information superiority, albeit narrowly defined, improving cyber security, and enhancing our ability to defend against hostile information operations are all important to our nation. Beyond this, three major observations merit note. First, information is not considered an element of national power on the same level as political/diplomatic, economic, and military elements of national power. Second, protecting America's critical infrastructures from cyber attack is a vital national interest. As such, defensive IO is given an important position within the strategy. Last, perception influence in the form of *Public Diplomacy* is expressed as being an increasingly vital component of our national strategy. What the *NSS* says about various IO capabilities is significant. But what it leaves unsaid about IO from a strategic thought perspective shows that there is no integrated approach to all aspects of IO from the national level. From this strategic point of departure, we can examine the current Joint military doctrine to begin to understand what makes IO unique and if that uniqueness lends itself to development of a theory.

What the Military Thinks Today - Joint Doctrine for Information Operations

Joint Doctrine for Information Operations, Joint Pub 3-13, was first published on 9 October 1998, over seven years *after* the conclusion of the Gulf War, which was noted as an immense IO success in the April 1992 *Final Report to Congress*.[14] In the words of General Henry H. Shelton, Chairman of the Joint Chiefs of Staff,

> This doctrine represents a significant milestone in defining how joint forces use IO to support our national military strategy. Our ability to conduct peacetime theater engagement, to forestall or prevent crisis and conflict, and to fight and win is critically

> dependent on effective IO at all levels of war and across the range of military operations.[15]

Doctrine defines IO as involving actions taken to affect adversary information and information systems while defending one's own information and information systems. It delineates both offensive and defensive actions, with perception influence (management) being included in offensive actions.

Offensive IO capabilities are a mixture of familiar Command and Control Warfare (C2W) capabilities, that include operations security, military deception, psychological operations, electronic warfare, and physical attack/destruction, and *one new capability – Computer Network Attack (CNA)*. It is interesting to note that doctrine explains all the familiar offensive capabilities in great detail and the one new capability - *CNA* - is mentioned in one sentence stating that guidance concerning the planning and execution of this capability is published separately in a classified Appendix A to *JP 3-13*. Similarly, joint doctrine does not even make mention of the term *Computer Network Defense (CND)*, yet it alludes to this activity as an emerging *Information Assurance* capability. The current IO doctrine focuses on IO as an integrating strategy. Does that mean that the familiar C2W capabilities were not integrated into the commander's concept of operations previously? The answer is that they were – except for those capabilities dealing with operations in the domain of cyberspace.

Cyberspace is not even defined in current joint IO doctrine. It is difficult to understand the apparent void in unclassified IO doctrinal thinking about the impact of computer *networks*, *network-centric warfare*, and *cyberspace* on our conduct of military operations. Instead of trying to first come to grips with cyber operations in and of themselves, the defensive, offensive and perception influence capabilities residing in cyberspace have been inexorably entangled within the term *Information* Operations – a conglomeration of mostly old capabilities discussed with a

sometimes digital twist. The significant impact of operations in the new domain – cyberspace – is lost amidst the familiar comfort zone of C2W capabilities plus the supporting capabilities of Public Affairs and Civil Affairs.

In the March 1999 JCS document, *Information Operations: A Strategy for Peace; The Decisive Edge in War*, the U.S. military begins to come to terms with the pervasiveness of cyberspace and network-centric operations. Important trends expressed are: the explosion in electronics-based information systems technology; the convergence of computing and communications capabilities on a global scale, enabling a shift to network-centric computing and network-centric operations; and the fact that these capabilities are essential to economic, social, political, and defense sectors – using information to create a competitive advantage.[16] This JCS pamphlet supplements joint IO doctrine and for the first time, conveys the significance of cyberspace as an operational domain presenting our nation with both vast opportunities and significant vulnerabilities. The unique aspect of IO is that offensive, defensive and perception influence capabilities previously bound to the physical domain of operations and conflict can now function and thrive within the construct of the cyber domain. One anticipates that the next iteration of *JP 3-13* will incorporate the new thinking presented in the supplemental pamphlet. Doctrine tells us how to think about conducting IO today. *Joint Vision 2020 (JV 2020)* provides a conceptual glimpse as to how the military views IO in the future.

IO and Cyber Operations in the Future – In Search of Strategic Thought

JV 2020 states that information operations are essential to achieving full spectrum dominance. This vision for 2020 espouses that activities and capabilities employed to conduct IO are traditional functions of military forces. It also acknowledges that the pace of change in the information environment dictates that the military expand this view and explore broader

information operations strategies and concepts.[17] An expanded view and broader conceptual look at IO necessitates an approach that deals with IO first at the national strategic level, then, within that integrated national framework, from a military perspective. The military is operating devoid of an integrated national framework for IO. In examining that piece of IO that deals with offensive, defensive, and perception influence operations in cyberspace, the lack of an integrated national strategy or underpinning theory dissipates the potential impact of cyber information operations. The military is just one of a host of players potentially wielding some aspect of our national power in cyberspace. Who integrates this effort? What should our nation do in cyberspace? And, more importantly, what shouldn't we do? As the U.S. Department of State increasingly uses cyberspace to conduct public diplomacy, how is this coordinated across all the elements of national power? National thought on cyber operations must mature before military application of cyber power to conduct operations can become decisive on the future battlefield. One particularly challenging area is that of the legal issues involved in conducting operations in cyberspace.

Information Operations are continuing to evolve as technology presents us with new opportunities and challenges. *JV 2020* emphasizes that as this evolution occurs, the conduct of IO, like all other military operations, will be in accordance with our societal norms and domestic and international laws.[18] Laws of armed conflict were written for operations in the physical domain. In the physical domain, there is a generally clear distinction between the military (combatants associated with the public sector) and civilians (non-combatants associated with the private sector). In cyberspace, the distinction between the public and private sectors is increasingly blurred – digitized information is disaggregated, bundled and sent over many different paths, potentially through many different nodes, to then be aggregated at its final

destination. The paths in cyberspace are neither neat nor distinct and the laws written for the physical domain do not accommodate the uniqueness of information travel in the cyber domain. Should the U.S. develop new laws due to the complexities presented by cyber operations? Should we also advocate a revision of international laws? We need a national strategy, framework, or theory of operations in cyberspace before that question can be answered.

Our nation will come to terms with cyberspace and operations in cyberspace, either in a thoughtful, deliberate fashion, or out of necessity borne by some tragic event that we are not prepared for. Until the U.S. develops a strategic framework for thinking about operations in cyberspace, integrated across elements of national power, attempting to develop a theory for something more encompassing, like information operations, seems almost futile. Modifying the words of the famous air power theorist, Giulio Douhet, one could add physical in front of surface, air forces to armies and navies, air to land and sea, substitute cyberspace for sky, and recognize that the words he wrote about air power in 1909 are as relevant to thinking about cyber power today.

> To us who until now have been inexorably bound to the surface of the earth; to us who smiled superciliously, almost with compassion, at the efforts of a few intrepid pioneers whom we thought deluded with visions of the impossible, but who proved the real seers, to us who have only armies and navies, it must seem strange that the sky, too, is about to become another battlefield no less important than the battlefields on land and sea.
>
> Giulio Douhet
> The Command of the Air

ENDNOTES

[1] *A National Security Strategy for a Global Age (NSS 2000)*, The White House, December 2000, p. iv.

[2] Ibid., p. 3.

[3] Ibid., p. 4.

[4] Ibid., p.5.

[5] Ibid., p. 9.

[6] Ibid., p.20.

[7] Ibid., p. 9.

[8] Ibid., p. 4.

[9] *National Plan for Information Systems Protection, Version 1.0, An Invitation to a Dialogue*, The White House, January 2000; available from http://www.ciao.gov/PCCIP/pccip_documents.htm; Internet; accessed 4/14/2001.

[10] Ibid., p. iii.

[11] Ibid., p. 24. The NIPC is the national focal point for warning, analysis, and response regarding threats to infrastructures. It was established in 1998 under Presidential Decision Directive 63 (PDD 63). For the PPD-63 White Paper, see http://www.fas.org/irp/offdocs/paper598.htm; Internet; accessed 1/16/2001.

[12] Ibid., p. 10.

[13] Ibid., p.11.

[14] *JP 3-13, Joint Doctrine for Information Operation* ,9 October 1998, p. I-20.

[15] Ibid., CJCS introduction.

[16] *Information Operations: A Strategy for Peace; The Decisive Edge in War*, JCS Pamphlet, March 1999, p. 4.

[17] *Joint Vision 2020*, U.S. Government Printing Office, Washington, D.C., June 2000, p. 28.

[18] Ibid., p. 30.