

**STRATEGY
RESEARCH
PROJECT**

The views expressed in this paper are those of the author and do not necessarily reflect the views of the Department of Defense or any of its agencies. This document may not be released for open publication until it has been cleared by the appropriate military service or government agency.

INFORMATION OPERATIONS CHALLENGES

BY

**LIEUTENANT COLONEL JAMES C. STRAWN
United States Air Force**

19980526 112

**DISTRIBUTION STATEMENT A:
Approved for public release.
Distribution is unlimited.**

DTIC QUALITY INSPECTED 2

USAWC CLASS OF 1998



U.S. ARMY WAR COLLEGE, CARLISLE BARRACKS, PA 17013-5050

USAWC STRATEGY RESEARCH PROJECT

INFORMATION OPERATIONS CHALLENGES

by

Lieutenant Colonel James C. Strawn
United States Air Force

Colonel Robert C. Coon
Project Advisor

The views expressed in this paper are those of the author and do not necessarily reflect the views of the Department of Defense or any of its agencies. This document may not be released for open publication until it has been cleared by the appropriate military service or government agency.

DISTRIBUTION STATEMENT A:
Approved for public release.
Distribution is unlimited.

U.S. Army War College
Carlisle Barracks, Pennsylvania 17013

ABSTRACT

AUTHOR: James C. Strawn, Lt Col, US Air Force

TITLE: INFORMATION OPERATIONS CHALLENGES

FORMAT: "USAWC Strategy Research Project"

DATE: 15 APR 1998 **PAGES:** 35 **CLASSIFICATION:** Unclassified

This paper examines the need for a coherent and well-defined national strategy for information operations. The impetus is today's environment and the realities of the environment we will face as we enter the next century. The paper begins by evaluating the present environment and highlighting key factors that contribute to the imperative nature of this challenge followed by a review of the current status of national initiatives. Finally, the paper discusses key steps to be taken in this arena.

The review of the present environment includes a macro-level look at the United States and its information needs. This look contrasts and compares the United States with its allies and its potential adversaries. With the review of the environment providing a foundation, a candid discussion of our nation's information operations initiatives helps to bring the issues into focus. The initiatives cannot be viewed solely from a Department of Defense perspective as they are addressing national challenges. These challenges share similarities with those in the arena of the asymmetric Weapons of Mass Destruction (WMD) threat. The solutions to those WMD threats demanded interagency and multi-national cooperation, the same is true for threats in cyber space.

Tangible action to date has been almost wholly one dimensional and defensively focused. To capitalize on information dominance, offensive information operations at the strategic level

must be a viable contributor. In conclusion, the paper discusses the weaknesses of our present course. Following with some recommendations to address some of the challenges.

TABLE OF CONTENTS

ABSTRACT iii

INTRODUCTION 1

SECTION 1 2

SECTION 2 6

SECTION 3 10

SECTION 4 14

CONCLUSION 16

RECOMMENDATIONS 19

TERMS AND DEFINITIONS 22

ENDNOTES 25

BIBLIOGRAPHY 29

INFORMATION OPERATIONS CHALLENGES

“History does not teach that better technology necessarily leads to victory. Rather victory goes to the commander who uses technology better, or can deny the enemy his technology.”

- Office of the Chief of Naval Operations¹

Many in our profession of arms would read the quote above and immediately think of weapons systems. The first weapon system to come to mind might be an airplane, a tank, or a ship depending on your individual background. The fact is that more and more the key technology might well be an information system. Additionally, it is almost a certainty that if the militarily significant technological marvel is of the next century, and it is not an information system, it will depend heavily upon one to be effective.

This paper will hold that relationship, or dependence, to be self-evident as it examines our information operations (IO) strategy. The IO strategy has to be examined in context. The context cannot be today's environment. We may use today as a foundation but the perspective must focus on the future as the objective. Our current information environment is significantly different than it was ten years ago. Based on the rate of change we have experienced to date we must conclude that our information environment ten years hence will be even more drastically different.²

Do our current strategies position us well for this future? Are the probable threats being addressed? Is the course and speed on track? What corrections should we make? These are all questions that this paper explores. The answers to the first three are not very comforting. The answer to the last question could be the foundation for our nation's future security.

Section 1

“I see a worldwide market for about three computers.”

- James T. Watson, Chairman of IBM, 1947³

“There is no reason for any individual to have a computer in their home.”

- Ken Olsen, Former President of Digital Equipment Corp., 1977⁴

These quotes carry a message about our current and future information environment. Here we have two information industry “insiders” who made bold predictions. In the 30 years between Mr. Watson’s comment about the worldwide market for computers and Mr. Olsen’s comments in 1977, a technological revolution occurred. In hind sight one could say his misprediction was understandable. After all 30 years had passed and a tremendous number of breakthroughs occurred in those three decades. However, consider Mr. Olsen’s comments in 1977, only 20 years ago, and today there are well over 125 million computers. From our perspective, now some twenty years later, Mr. Olsen seems to have missed the mark as much as it seemed Mr. Watson had missed it in 1977.

The message is not that these gentlemen did not have a grasp on the direction and pace of their own industry. The message is that technological progress in this arena is advancing at such an accelerating rate that even knowledgeable people in the business have difficulty prognosticating the trends. The danger is that this difficulty will continue to be present as we look into the future and will lead to the potentially fatal error of discounting possibilities. The term fatal, as used here, was carefully chosen. If you are a business leader the fatality could be your market share or your business itself. If you are a national leader the fatality could be your nation’s power or its survival. Finally, if you are a nation’s military establishment, the fatality could be your ability to defend your nation’s interests.

Given the accelerating rate of progress, or at least the rate of technological evolution, it is easy to extrapolate that the next ten years will find us in an information environment at least as different from today as today's is from 1977.⁵ Exactly how it will be different may be open to much debate, but certain elements are quite probable. Our global economy will become even more integrated than we find today and international financial interdependency will increase.⁶ Most nations, even economically emerging nations, will have access to a global information infrastructure vastly superior to today's systems. All of these changes will be accompanied with an exponential growth in the international and transnational flow of information. These environmental predictions are conservative compared to those of many futurists.

What does this change to a global information environment mean to our nation or any nation? The answer to that question depends on the nation, where it stacks up in the global hierarchy, and whether it is prepared for the future. The Tofflers put forth a model that is very useful in looking at these issues. They see nation-states falling into one of three categories. First Wave countries are those which are primarily agrarian. The Second Wave countries are those which could be classified as industrialized nations. While the Third Wave countries are information and innovation based powers. They produce and sell information, innovation, advanced technology, financial services, and other information and technology based services.⁷ History has shown us that there is a tendency for nations to evolve from First Wave toward Third Wave status. However, for the foreseeable future there is no reason to believe that there will not be nation-states in all three stages of evolution. Indeed many futurist suggest that the gap between First Wave and Third Wave nations may widen and become more pronounced in many respects.

The basic difference between a Third Wave nation and a Second or First Wave nation can be characterized by their dependence, and ability to capitalize, on information and information technologies. Additionally, the Third Wave nation will depend heavily on those factors for its economic and social well being, while capitalizing on the associated advantages across the spectrum of international conflict and competition. The impact on the economic and military instruments of power for those nations will be most pronounced. The enjoyed advantages are accompanied by associated dependencies and vulnerabilities. These dependencies and vulnerabilities could represent a potential achilles heel which must be properly evaluated and managed. An attack on this achilles heel could be termed information warfare.

Information warfare will become more and more attractive to a variety of actors in the international arena. It is a natural by-product of modern information systems that the global nature of information infrastructure, the international networking of networks, and the totally transparent flow of information all combine to degrade a nation's borders and security. This can actually be looked upon as a global technological breaking down of national borders. Invasion of information systems and attack on sources of national power will be possible with no physical presence required. In some respects an attacks on our information may represent the path of least resistance, or the "most bang for the buck", to a potential adversary.

It has been written that four components are required to support high-level Information Warfare: A new world order (information based civilizations and global interdependencies); computer proliferation; a global information network; and megabyte money in a financial economy (vast sums of money and transactions that exist primarily in cyber space).⁸ The United States is entering that realm today and must be prepared to protect its interests into the next century.

Some contend that by 2010 - 2020 we may experience a scenario where currency, as we know it today, may not exist. Personal and business transactions will be accomplished via debt cards and other forms of automated transactions. If so, the criticality of such a community currency, perhaps on a global scale, will demand extraordinary protective measures. This scenario provides a glimpse of the challenges we must be prepared to address.

Section 2

“There is a war out there, and it’s all about who controls the information. It’s all about the information.”

- Cosmo in Sneakers⁹

The United States, some of its allies, and potential adversaries will enter the next century as bonafide Third Wave nations. As such, the country and its interests can expect to be targeted in ways yet to be imagined. If a nation is to protect its interests, economic, political or otherwise, then it must be prepared to protect its information. The spectrum of this challenge is enormous but the potential consequences are too high to ignore.

On the low end of the spectrum, in terms of damage to the country, are the ad-hoc or random attacks. These are often executed for personal gain or satisfaction, but they represent a growing drain on the economy. An example of the magnitude was detailed in the 1992 study Toll Fraud and Telabuse: A multi-billion Dollar Problem. The annual cost to the nation’s phone systems, based on 1991 statistics, was over 8.8 billion dollars.¹⁰ Apply that template to the other information based industries and the potential economic impact to the nation is staggering.

The middle of this spectrum could be defined as terrorism. Info-terrorism like any other type of terrorism must be understood for what it is, a terrorist act. Terrorism involves acts that affect the social structure as well as the individual. It upsets the framework of the precepts and images upon which the members of society have come to depend and trust. Since one no longer knows what behavior to expect from other members of society, the system becomes disoriented. The community dissolves into a mass of anomic individuals, each concerned with personal survival.¹¹ Terrorism is therefore principally a political problem with its own political goals and objectives.¹² The target is not the building that was blown up, nor the subway passengers killed

by the poisonous gas, nor the regional power grid that was disabled. The target is the society as represented by the will of the people and the actions of the government. Info-terrorism, is a strategy that can be applied in support of domestic, transnational, or international terrorist efforts. The attacker does not have to have an extensive information infrastructure of their own, nor possess the ability to develop this technology. The requisite technology and expertise is available on the open market. The goal of info-terrorism is to target the information infrastructure upon which modern societies depend. The potential target list runs the gambit, from commercial communications, to international stock and monetary systems, to transportation systems and utility switching systems.¹³ This approach could be a particularly attractive option when the targeted country is a Third Wave nation.

Terrorism by its nature is an asymmetric attack or form of war. It is often the methodology used when the perpetrators do not have the capacity to challenge symmetrically. If the terrorist are domestic the challenge of dealing with the threat, though significant, is somewhat simplified. This is an area where the United States has had significant success and to date suffers from less of a threat than many of our allies. The challenges of dealing with international or transnational terrorists are significantly greater. Transnational terrorism is carried out by groups that operate without regard for national boundaries.¹⁴ While international terrorism is supported and controlled by nation-states as part of a strategy for waging asymmetric surrogate war against their enemies.¹⁵ The potential external terrorist threats against the United States represents such a hybrid of transnational and international terrorism that they can be difficult to separate and should (and will) be addressed simultaneously in this paper.

International terrorism continues to thrive. There has been a world-wide trend of sponsor nations turning to terrorist groups to conduct proxy terrorist wars against the "enemy states".

The sponsor finds that the proxy wars are significantly cheaper than maintaining the requisite standing military forces. Additionally, there is a perceived reduction in the risk of retribution, as long as the connection is deniable.^{16,17} There is no reason to believe that this trend will not continue well into the next century. As the remaining military super-power in today's multi-polar world, it is less likely that we will be challenged in a symmetric fashion and much more likely that we will be targeted asymmetrically. International terrorism would be an obvious course of action and either weapons of mass destruction (WMD) or info-terrorism could be among the logical weapons of choice.

Our nation's policy towards international terrorism has been relatively clear throughout recent history. The present policy is articulated in the President's National Security Strategy published in 1997:

*"U.S. counterterrorism approaches are meant to prevent, disrupt and defeat terrorist operations before they occur, and if terrorist acts do occur, to respond overwhelmingly, with determined efforts to bring the perpetrators to justice. Our policy to counter international terrorists rests on the following principals: (1) make no concessions to terrorists; (2) bring all pressure to bear on state sponsors of terrorism; (3) fully exploit all available legal mechanisms to punish international terrorists; and (4) help other governments improve their capabilities to combat terrorism."*¹⁸

The question we must ask ourselves is, are we prepared to execute this policy in the arena of info-terrorism?

The high end of this spectrum of information warfare is represented by acts in support of, or in conjunction with, symmetric attacks against the United State, its allies, or interests. While conflict at this level is not as likely as those already discussed, the results could be much more catastrophic.

By our own admission our vision for future military success rests on the foundation of information superiority and technological innovation.¹⁹ Even our allies leverage our systems to support their operations and our shared security interests. For our military of the future we are developing concepts like “just in time logistics” and “total asset visibility”, both of which are information based. Additionally, we tout our ability to “find, fix and target anything on earth” and we plan to do it using elements of the global information infrastructure. We extol our approach to future warfare to all who show an interest, focusing on its advantages. But, what about the flip side of that coin?

A well placed and timed attack on our information infrastructure would go a long way towards leveling the playing field for a more conventional symmetric attack. Crippling our domestic rail and air transportation control systems just as we are attempting to mobilize for an international crisis could mean the difference between success and failure. Our command and control systems ride satellite networks that can be targeted with rudimentary methods. An important point to consider is that none of this would have to be executed from within our borders. In some cases no military or government system would have to be targeted to degrade or national defense capabilities.²⁰ We might not even be able to identify where the information attack originated. As we integrate more commercial systems with our military systems our defenses will become more porous. It is apparent we must take steps today to preclude a costly lesson in the future.

Section 3

“Information technologies are a two-edged sword of both tremendous opportunities and vulnerabilities.”

- National Defense Panel, 1997²¹

The observation by the National Defense Panel addresses the dilemma the United States finds itself attempting to manage. The phrase “the genie is out of the bottle”, which is often associated with discussions about nuclear weapons, is just as applicable to our information technology explosion and our dependence on that technology. If there is a significant difference, it would be that very few would seriously wish we could put our information technology “back in the bottle”. The benefits to a modern society are so great that information and its supporting infrastructure can be considered a national resource. Additionally, this is a resource that does not suffer from some of the disadvantages of so many others. There are no limited reserves, no polluting impact to the ecology, nor does it appear there is anything on the horizon that might supplant it.

Given that advances in the information arena are for the most part good and represent a path we want to pursue, how will we deal with the vulnerabilities and threats touched on earlier? Our earliest efforts were somewhat successful but represented either a lack of vision or perhaps a chronic case of denial. It was, in all likelihood, a combination of the two. A lack of vision as to what the future held in the way of global networking and rate of attainment, coupled with denial as to the potential impact on the United States and the world community.

Our nation’s first approach to securing the information was one of isolationism. That is not the same political isolationism that we have practiced at periods in our history. However, this isolationism represents as valid an example of short-sightedness and adherence to an overly

simplistic strategy as did its political counterpart. This approach was used in both the government and the commercial world. However, industry abandoned it much earlier than our government.

The approach, as applied in government circles was straight forward. Government information systems of importance were developed and maintained in isolation. Locked doors, "air gaps" and dedicated circuits provided the security. We carried this approach so far that our own government systems could not communicate with each other. In addition, it could be argued that this approach contributed to many of them being technologically obsolete upon fielding. Special software was developed driving up the costs to both field and support the systems. We married the special software to hardware and fielded a unique system tailored for a particular mission. The government approach was to then attempt to maintain that unique system for ten to twenty years, while commercial information technology life cycles were approaching five to seven years. Within the Department of Defense this was carried to the extreme, to the point that separate services were developing separate systems to do the same mission. These systems were not only largely redundant in capabilities but incompatible with other existing or developing systems.

It is not the intent of this paper to blame this inefficient and short-sighted approach to the proliferation of information systems solely on the need for security. However, it was an easy short term answer to a challenging security problem. The role security concerns played became more obvious when, around 1990, the Department of Defense began to seriously attempt to integrate service unique systems for efficiency and improved support to the warfighter. One of the first excuses often raised against integration efforts was security. However, the direction of future systems and the absolute need to integrate and disseminate information was becoming

obvious to all. It was about the same time, around 1990, that global networks on a large scale were becoming a reality and along with it serious efforts were underway to develop the technology required to provide the required information security.

Driven by economic realities government agencies made the decision that commercial standards were to be used to the fullest extent possible. That approach was articulated by the Department of Defense in the Defense Infrastructure Common Operating Environment, which was published as the standard for non-legacy systems. While that was the smart decision and the correct path to pursue, it was not without risks. With the course set by the commitment to commercial standards the government Department of Defense found itself headed down the path that brings many of our government information systems into the same realm of vulnerability that already existed in the commercial world.

This has all helped to fuel the national dialog about how we will protect this resource called information. The obvious issues are now being agreed to and discussed, though most are far from being resolved. Nationally we have to evaluate the total threat picture as we integrate our information infrastructure and aggressively tie into the global systems upon which we have become dependent. As a military we must evaluate that threat and its implications to our ability to defend our national interests. The implications of certain commercial system vulnerabilities to the military and our national security may be much greater than our industry leaders are aware.

Then there is the issue of the development of the solutions and the associated costs to address the threat. Business would normally decide whether to pursue the solution or not based on some type of cost / benefit analysis. Our government has to worry about a different set of criteria. These criteria include the various aspects of national security. Finally, as we develop the technological solutions to many of these threats, to whom should they be available? The

nation's military strategy calls for information superiority.²² It defines it as follows:

"Information superiority is the capability to collect, process, and disseminate an uninterrupted flow of precise and reliable information, while exploiting an adversaries ability to do the same."²³

Additionally our military strategy recognizes that information superiority is dependent on technology.²⁴ As we develop these technologies to protect our information do we get one commercial developer to share the breakthrough with another? Do we provide it to our allies yet preclude commercially developed systems from being sold on the open market? What about the global implications with domestic, transnational, international, and non-governmental actors all of whom may target our information, or whose information we may wish to target? There are no universally accepted answers to any of these questions today. The dialog has begun, but roles and missions have yet to be determined.

Section 4

“We are racing into a strange and novel period of future - history. Those who wish to prevent or limit war must take these new facts into account, see the hidden connections among them, and recognize the waves of change transforming our world.”

- Toffler²⁵

Within the Department of Defense the challenges of dealing with the threats discussed in this paper have been daunting. Just coming to grips with the military's role, responsibilities, and boundaries has caused much debate. Terminology provides an example of the sensitivities that permeate the information security issues. The majority of commercial writings lump all defensive and offensive actions to protect your own information or to attack someone else's information under the heading of information warfare. Such a broad brush approach would not meet the needs of the Department of Defense. The United States military cannot prosecute information warfare, or any other type of warfare, if we are at peace as a nation. However, it is obvious that some legal efforts must be ongoing in this arena. At a minimum defensive measures, training and planning activities must be pursued. To address this the Department of Defense published the Department of Defense Directive S-3600.1, Information Operations and Chairman of the Joint Chiefs of Staff Instruction 3210.01A, Joint Information Operations Policy. Together they lay out both general and specific guidance and policy pertaining to IO. That guidance helps to define the scope of the military's responsibilities in the IO arena and to differentiate information warfare from the broader IO.

The doctrine to implement the current guidance is under development as Joint Publication 3-13. Joint Publication 3-13's scope is stated as follows;

“This publication provides the overarching operational guidance for information operations (IO) in the joint context (to include information warfare (IW)) throughout the range

of military operations. It addresses IO principles relating to both offensive and defensive IO and describes responsibilities for planning, coordinating, integrating, and deconflicting joint IO. Guidance concerning intelligence support to IO, Defense and interagency relationships, and IO in training and exercises also is provided."²⁶

The general policy it lays out explains the military's approach to IO and succinctly differentiates between information warfare and IO in the following passage;

*"IO involve actions taken to affect adversary information and information systems while defending one's own information and information systems. IO apply across all phases of an operation and the range of military operations, and at every level of war. IW is IO conducted during time of crisis or conflict (including war) to achieve or promote specific objectives over a specific adversary or adversaries. Defensive IO activities are conducted on a continuous basis and are an inherent part of force employment across the range of military operations. IO may involve complex legal and policy issues requiring careful review and national-level coordination and approval."*²⁷

A detailed review of the draft joint doctrine reveals its major focus appears to be on defensive IO efforts. Commanders are tasked to incorporate IO into exercises and operations plans however, exercises to date have focused on defensive measures and awareness. Roles and responsibilities are addressed however, those listed are primarily defensive. Additionally, the only substantive guidance provided for IO efforts in support of military operations is at the operational and tactical levels of war. IO at the strategic level is addressed generically as an option available to the National Command Authority. The document then highlights the potential impact of strategic IO on all enemy elements of national power. However, roles and responsibilities for strategic level IO are largely ignored.

Conclusion

“We need a new National Information Security Strategy, and cryptology is only a small part of it. Information security is a much broader subject that relates to services in an open society.”

- Director, National Security Agency²⁸

In the military we understand that the centers of gravity (COG) differ for given adversaries. There are many factors that contribute to those differences, however on a very basic level the evolutionary stage of the nation-state (First, Second, or Third Wave) may be a primary factor. A Third Wave nation will derive national strength and freedom of action from information. Therefore information could reasonably be considered a COG. The vulnerabilities of the global information infrastructure that the information rides might make that COG a very attractive target to an international actor. Although we must be prepared to defend our nation's interests across the spectrum of conflict, in the information arena info-terrorism has to be considered a highly probable threat.

As a nation we have come to grips with the reality that an asymmetric attack against the United States, using WMD, is a probable occurrence.²⁹ Our nation has in recent years taken action to ensure a coordinated response to such terrorist acts. The State Department, Department of Justice, Department of Defense, Department of Energy, National Security Council, Federal Bureau of Investigation, Central Intelligence Agency, Defense Intelligence Agency, and a host of others all have defined roles in combating terrorist acts involving WMD.³⁰ The same aggressive broad-based approach must be initiated if we are going to be able to successfully prevent or deal with info-terrorism. To date no such coordinated broad-based approach has been initiated to address terrorist attacks targeting our information systems.

The reasons why we have failed as a nation to seriously address this issue are multifaceted. Perhaps the two greatest reasons are; there are no horrific images of casualties that come to mind as with WMD attacks and the whole paradigm is just too foreign to many decision makers and the public at large. Given those as primary reasons for past inaction they do not represent a roadblock to progress if we can just overcome the inertia of the inaction. A more valid difficulty in dealing with this threat may well be its scope.

To come to grips with the scope and implications consider the spectrum discussed earlier. Starting at the low end with the ad-hoc attacks which are probably targeted against primarily commercial systems. Those attacks are issues of civil, criminal, and perhaps international law. Law enforcement activities are outside the scope of the military and many other governmental agencies. It is up to business to report such crimes, but to whom and to what end? If an attack originates from an unknown location outside our borders and affects a company in Texas who will respond to the 911 call? That is just an example of the complexities at that level.

Now lets move up the scale to the asymmetric info-terror attack. In this realm there is still a high probability that the targeted system will be commercial. The purpose would be political and the results could be catastrophic. An example could be the disabling of the telephone switching systems for the mid-Atlantic states coupled with a major power outage on the west coast. Such an attack and its second and third order effects would affect commerce, probably result in casualties, and disrupt government functions.³¹ Who determines if these attacks are coordinated and what was the desired end-state? If targeted solely at commercial systems is this strictly a legal problem or a matter of national security? How is it reported and what resources are brought to bear on the resolution? Today we have no universally accepted answers to these questions. The environment at this level becomes more complex than the previous level. It is

significantly more complex than the WMD terrorist issues mentioned earlier and the response team is largely non-existent. The truth is that all of the players on the team have not been identified, let alone an understanding of what roles they are expected to play.

It is only when we step up to the high end of the spectrum of IO that there is some comfort level. Here the term information warfare can be comfortably applied. Now the IO guidance that has been published or is currently under development has some applicability. This is where government systems are expected to be targeted and all of our defensive efforts should start to pay dividends. Remember though this is the least likely scenario.

Why are we within the Department of Defense making the most progress preparing for the least likely attack? Perhaps it is because that is the only scenario where we are comfortable imagining the scope of our role and responsibilities. After all, at that level war, defense, offense, and a defined enemy all become tangible concepts. More probably though it is due to a lack of national guidance. In an effort to do "something" the Department of Defense appears to have taken on the IO challenge in the area where it can accomplish the most on its own.

Nothing of substance to address the full spectrum of this threat will be accomplished without a Presidential Decision Directive (PDD) to initiate a focused national agenda in the IO arena. It was just such a PDD that initiated the development of a coordinated response to the asymmetric WMD threat. In that arena efforts have been kicked off throughout the national government and at state and local levels. A response to threats in the information arena will require most of the same actors in addition to many from the commercial sector. Our current eclectic and somewhat half-hearted attention to the problem will not be in the best interest of the nation as we enter into the next century and see our window of vulnerability increase.

Recommendations

"We will fight on our own terms and we will win"

- General George S. Patton Jr³²

The General's quote should represent our approach to IO, especially the aspects that fall under the heading of information warfare. It denotes a degree of initiative and the ability to take the fight to the enemy. The national information security challenges, as already mentioned in this paper, are significant and varied. Admittedly, many are outside the direct scope of the Department of Defense. That should not be used as an excuse to pursue only the peripheral issues or the "easy fixes". The Department of Defense must push for a comprehensive government approach to the threat as was done with WMD.

Besides advocating a comprehensive national program several specific actions would greatly enhance our military capabilities. Currently IO is under the purview of the Joint Staff/J39.³³ This relationship is in keeping with the Operations Directorate's responsibility, as laid out in the National Security Act of 1947, to assist the Chairman of the Joint Chiefs of Staff with providing unified strategic direction to the combatant forces. The Joint Staff may be the best place for the IO proponentcy to reside along with the responsibility for doctrine. However, the Department of Defense needs an organization, not a staff function, designated as the lead if we are to develop combat capabilities. Give a commander the mission and the resources to meet the challenges and we will see the Department of Defense step to the forefront. If no one "owns" this mission it will not be well represented in the national debate as we shape our force for the future.

Another by-product of this action would be to have someone to orchestrate offensive information warfare planning and execution at the strategic level, operational, and tactical levels

of war. Offensive IO at the operational and tactical levels could be normalized into a supported / supporting commander relationship. With Theater Commanders in Chiefs (CINCs) being the supported commanders and using IO forces and expertise as combat multipliers. This approach would be founded on the same relationships we accept today and as currently laid out in joint doctrine. All of this could be incorporated into the next Unified Command Plan and would set up strategic level IO to follow the nuclear model.

In the nuclear arena CINC / USSTRATCOM is responsible for the planning and execution of strategic nuclear operations. However, that has not precluded him from assuming the role of supporting CINC as required. A CINC needs to be prepared to field, plan, and operate the systems required to execute strategic level IO at the direction of the National Command Authority in the same way one has been designated for the nuclear mission. IO at this level would not have to be in concert with traditional military operations. This approach may not fit our current models of war, but it is warfighting just the same and we in the military need to be prepared to prosecute it.

The Department of Defense must push for cooperative commercial sector / government action. Many of the technological solutions to the problems will come from the commercial sector. The ability and need to respond globally, as required to protect the national interests, will reside with the government. Solutions developed in isolation in either community will probably not be palatable to the other nor meet our nation's security requirements. This is an approach that will undoubtedly cause some discomfort because some of these players are not used to working together. However, the joint endeavor is an obvious necessity and putting it off until a precipitating event triggers action will be of benefit to no one.

To date the Department of Defense appears to have only been comfortable discussing and acting on defensive IO issues or offensive measures that are targeted at an opposing military force.³⁴ That approach is only adequate if we believe all other potential adversaries are willing to operate under the same rules. If we do not believe that is the case then we must be prepared to go beyond our comfort zone and take the initiative. This is an extremely challenging area that will no doubt eventually result in international agreements and legislative action. Those responsible for protecting our national security should help to foster and shape the debate.

word count - 5,805

APPENDIX

Terms and Definitions³⁵

Centers of gravity. Those characteristics, capabilities, or localities from which a military force derives its freedom of action, physical strength, or will to fight. (Joint Pub 1-02)

Cyber space.³⁶ A term commonly used in publications that generally encompasses the global information infrastructure and the associated information (as defined below).

Defense Information Infrastructure. The shared or interconnected system of computers, communications, data applications, security, people, training, and other support structures serving DOD local, national, and worldwide information needs. The Defense Information Infrastructure connects DOD mission support, command and control, and intelligence computers through voice, telecommunications, imagery, video, and multimedia services. It provides information processing and services to subscribers over the Defense Information Systems Network and includes command and control, tactical, intelligence, and commercial communications systems used to transmit DOD information. Also called **DII**. (Upon approval of Joint Publication 3-13, this term and its definition will be included in JP 1-02.)

defensive information operations. A process that integrates and coordinates policies and procedures, operations, personnel, and technology to protect information and defend information systems. Defensive information operations are conducted through information assurance, physical security, operations security, counter-deception, counter-psychological operations, counterintelligence, electronic protect, and special information operations. Defensive information operations ensure timely, accurate, and relevant information access while denying adversaries the opportunity to exploit friendly information and information systems for their own purposes. (Upon approval of Joint Publication 3-13, this term and its definition will be included in JP 1-02.)

global information infrastructure. The worldwide interconnection of communications networks, computers, databases, and consumer electronics that make vast amounts of information available to users. The global information infrastructure encompasses a wide range of equipment, including cameras, scanners, keyboards, facsimile machines, computers, switches, compact disks, video and audio tape, cable, wire, satellites, fiber-optic transmission lines, networks of all types, televisions, monitors, printers, and much more. The friendly and adversary personnel who make decisions and handle the transmitted information constitute a critical component of the global information infrastructure. Also called **GII**. (Upon approval of Joint Publication 3-13, this term and its definition will be included in JP 1-02.)

information. 1. Facts, data, or instructions in any medium or form. 2. The meaning that a human assigns to data by means of the known conventions used in their representation. (JP 1-02)

information environment. The aggregate of individuals, organizations, or systems that collect, process, or disseminate information; also included is the information itself. (Upon approval of

Joint Publication 3-13, this term and its definition will be included in JP 1-02.) (NOTE: This term promulgated in DODD S-3600.1 of 9 Dec 96.)

information-based processes. Processes that collect, analyze, and disseminate information using any medium or form. These processes may be stand-alone processes or sub-processes which, taken together, comprise a larger system or systems of processes. (Upon approval of Joint Publication 3-13, this term and its definition will be included in JP 1-02.)

information operations. Actions taken to affect adversary information and information systems while defending one's own information and information systems. Also called **IO**. (Upon approval of Joint Publication 3-13, this term and its definition will be included in JP 1-02.) (NOTE: This term promulgated in DODD S-3600.1 of 9 Dec 96.)

information superiority. The capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same. (Upon approval of Joint Publication 3-13, this term and its definition will modify the existing term and its definition and will be included in JP 1-02.) (NOTE: This term promulgated in DODD S-3600.1 of 9 Dec 96.)

information system. The entire infrastructure, organization, personnel, and components that collect, process, store, transmit, display, disseminate, and act on information. (Upon approval of Joint Publication 3-13, this term and its definition will modify the existing term and its definition and will be included in JP 1-02.) (NOTE: This term promulgated in DODD S-3600.1 of 9 Dec 96.)

information warfare. Information operations conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries. Also called **IW**. (Upon approval of Joint Publication 3-13, this term and its definition will modify the existing term and its definition and will be included in JP 1-02.) (NOTE: This term promulgated in DODD S-3600.1 of 9 Dec 96.)

National Information Infrastructure. The nation-wide interconnection of communications networks, computers, databases, and consumer electronics that make vast amounts of information available to users. The national information infrastructure encompasses a wide range of equipment, including cameras, scanners, keyboards, facsimile machines, computers, switches, compact disks, video and audio tape, cable, wire, satellites, fiber-optic transmission lines, networks of all types, televisions, monitors, printers, and much more. The friendly and adversary personnel who make decisions and handle the transmitted information constitute a critical component of the national information infrastructure. Also called **NII**. (Upon approval of Joint Publication 3-13, this term and its definition will be included in JP 1-02.)

offensive information operations. The integrated use of assigned and supporting capabilities and processes, mutually supported by intelligence, to affect information and information systems to achieve or promote specific objectives.

These capabilities and processes include, but are not limited to, operations security, military deception, psychological operations, electronic warfare, and physical destruction. (Upon approval of Joint Publication 3-13, this term and its definition will be included in JP 1-02.)

ENDNOTES

- ¹Winn Schwartau, Information Warfare (New York: Thunder's Mouth Press, 1994), 291.
- ²President's Commission on Critical Infrastructure Protection, Critical Foundations, Protecting America's Infrastructures (Washington D.C.: U.S. Government Printing Office, 1997), 9.
- ³Schwartau, 49.
- ⁴Ibid.
- ⁵President's Commission, 9.
- ⁶Ibid, 8.
- ⁷Alvin Toffler and Heidi Toffler, War and Anti-War (New York: Little Brown and Co., 1993), 22.
- ⁸Schwartau, 64.
- ⁹Ibid, 215.
- ¹⁰Ibid, 134.
- ¹¹Donald J. Hanle, Terrorism, The Newest Face of Warfare (McLean, VA: Pergamon-Brassey's International Defense Publishers, Inc., 1989), 110.
- ¹²Ahmed Galal Ezeldin, Ph.D., Global Terrorism: an Overview (Chicago, IL: The University of Illinois at Chicago, Monograph No. 10, 1991), 38.
- ¹³Toffler, 149-152.
- ¹⁴Ezeldin, 29.
- ¹⁵Ibid.
- ¹⁶Bruce Hoffman, Responding to Terrorism Across the Technological Spectrum (Carlisle Barracks, PA: U.S. Army War College Strategic Studies Institute, April 1994), 9.
- ¹⁷Ezeldin, 12.
- ¹⁸The Office of the White House, National Security Strategy of the United States (Washington, D.C.: U.S. Government Printing Office, 1997), 10.

¹⁹Joint Chiefs of Staff, National Military Strategy of the United States of America (Washington D.C.: U.S. Government Printing Office, 1997), 17.

²⁰President's Commission, 8.

²¹National Defense Panel, National Defense Panel Report (Washington D.C.: U.S. Government Printing Office, 1997), v.

²²JCS, National Military Strategy, 17.

²³Ibid, 18.

²⁴Ibid.

²⁵Toffler, 219-220.

²⁶Joint Chiefs of Staff, Joint Publication 3-13 (Second Draft) (Washington D.C.: U.S. Government Printing Office, 1997), i.

²⁷Ibid, I-1.

²⁸Clarence A. Robinson, Jr., "Security Agency Finds Virtual Friends and Foes Collocated," SIGNAL October 1997, 17. Author's quotation of Lieutenant General Kenneth A. Minihan, USAF, Director of the National Security Agency.

²⁹National Defense Panel, 42.

³⁰Michael T. Brown, Lieutenant Colonel, U.S. Army, Weapons of Mass Destruction Terrorism Within the United States: Asymmetric Warfare in the 21st Century (Carlisle Barracks, PA: U.S. Army War College, 1997), 30.

³¹President's Commission, 4.

³²Peter B. Williamson, Patton's Principals (New York: Simon and Schuster, 1979), 135.

³³Andrew Wilde, Lieutenant Commander, U.S. Navy, interview by author, 13 November 1997, Pentagon, Washington D.C. Commander Wilde was the lead staff officer within the Joint Staff/J39 working the Draft guidance (Joint Pub. 3-13) for Department of Defense (DoD) IO activities. The Joint Staff/J39 is the military staff office responsible for oversight of IO activities at the DoD level. Questions about command relationships and orchestration of the military services' and combatant commands' efforts were discussed in detail.

³⁴Ibid. Discussions about the lack of Department of Defense guidance pertaining to offensive IO and the associated reasons and challenges.

³⁵Joint Chiefs of Staff, Joint Publication 3-13 (Second Draft), GL6-GL17.

³⁶Definition distilled from usage in context of several referenced works.

BIBLIOGRAPHY

- Brown, Michael T., Lieutenant Colonel, U.S. Army. Weapons of Mass Destruction Terrorism Within the United States: Asymmetric Warfare in the 21st Century. Carlisle Barracks, PA: U.S. Army War College, March 1997.
- Ezeldin, Ahmed Galal Ph.D. Global Terrorism: an Overview. Chicago, IL: The University of Illinois at Chicago, Monograph No. 10, 1991.
- Hanle, Donald J. Terrorism, The Newest Face of Warfare. McLean, VA: Pergamon-Brassey's International Defense Publishers, Inc., 1989.
- Hoffman, Bruce. Responding to Terrorism Across the Technological Spectrum. Carlisle Barracks, PA: U.S. Army War College Strategic Studies Institute, April 1994.
- Robinson, Clarence A. Jr.. "Security Agency Finds Virtual Friends and Foes Collocated." SIGNAL, October 1997, 17-19.
- Schwartzau, Winn. Information Warfare. New York: Thunder's Mouth Press, 1994.
- Toffler, Alivin and Heidi Toffler. War and Anti-War. New York: Little Brown and Co., 1993.
- U.S. Joint Chiefs of Staff. Joint Publication 3-13 (Second Draft). Washington D.C.: U.S. Government Printing Office, 1997.
- U.S. Joint Chiefs of Staff. National Military Strategy of the United States of America. Washington D.C.: U.S. Government Printing Office, 1997.
- U.S. National Defense Panel. National Defense Panel Report. Washington D.C.: U.S. Government Printing Office, 1997.
- U.S. Office of the White House. National Security Strategy of the United States. Washington, D.C.: U.S. Government Printing Office, May 1997.
- U.S. President's Commission on Critical Infrastructure Protection. Critical Foundations, Protecting America's Infrastructures. Washington D.C.: U.S. Government Printing Office, 1997.
- Wilde, Andrew, Lieutenant Commander, U.S. Navy. Interview by author, 13 November 1997, Pentagon, Washington D.C.
- Williamson, Peter B. Patton's Principals. New York: Simon and Schuster, 1979.