Information Operations:
The Hard Reality of Soft Power

Forward – Dr Dan Kuehl, Information Resources Management College, National Defense University 4

Introduction 5
- Electronic Disturbance Theatre
- The Power of Information

Chapter 1 - Integration and Coherence - The Language of Information Operations 8
- Power - What is Power?
  - Factors that Affect Power
  - Power in the Cold War Era - What has Changed?
  - Military Power and Asymmetric Threats
- Information Operations Theory
  - IO Theory and Doctrine
  - Differences between IW and IO
  - Capabilities and Related Activities of Information Operations
  - The Evolution of IO Doctrine
- Information Operations Organizations
  - Top-Level Leadership
  - IO and the Interagency Process
    - DOD - OSD and IO
      - DOD - Combat Support Agencies
        - The NSA's IO Architecture
        - The DISA's IO Architecture
      - DOD - The Joint Staff and IO
        - The CINCs
        - Additional DOD IO Elements
  - Cabinet IO Interests
    - Department of State IO Concerns
      - Traditional DOS Structure
    - DOC IO Architecture
    - DOJ IO Architecture
  - Transnational IO Groups
- Summary

Chapter 2 - Intelligence and Exploitation – Foundations for Conducting IO 29
- The Application of IO
  - The Intelligence Cycle
  - The Intelligence Community

IO and the IPB
The Releaseability Issues of IO
Conclusion

Chapter 3 - Information Protection- The Challenge to Modern Bureaucracies 39
Defensive Information Operations
Information Assurance and Computer Network Defense
A View of Defensive Information Operations
Counter-Terrorism Information Operations
What is Terrorism?
Combating Terrorism
Fundamentals of CTIO
PDD-62 (*Counter-Terrorism*)
Simulated Domestic Counter-Terrorism Operations
Partnerships for Counter-Terrorism: “Track Two Diplomacy”
PDD-63 (*Critical Infrastructure Protection*)
Summary

Chapter 4 - Information Projection - Shaping the Global Village 61
Offensive Information Operations
Computer Network Attack
Space and its Relationship with IO
The Relationship Between EW and IO
PDD-68 (*International Public Information*)
History of IPI
Outside Influences on IPI
What is IPI?
What was the Clinton Administration attempting to do with IPI?
Why has IPI been "less than successful?'
Conclusion

Chapter 5 - Organize, Train, and Equip 76
IO Planning
Military IW Service Centers
IO Planning Tools
Strategy-to-Task Planning
Tying together Strategy-to-Task Planning and IO Planning Tools
IO and JOPES
OPLAN, TPFDD and the IO Cell
IO Cell Responsibilities
IO as an Integrating Strategy
Legal Issues Connected with IO
An Overview of the Legal Landscape
Peacetime Treaties Impacting IO

Law of Armed Conflict
Domestic Law
The Solution for the Operator: IO ROE Planning
Summary of IO Planning and Legal IO Concerns

Chapter 6 - Recent Information Operation Campaigns 91
The Growing Role of Information in Russia
Information Superiority
Information Space
Russian IW Terminology and Theory
Informational-Psychological
Military-Technical
Systemological Aspects
IO in Kosovo
The Use/Misuse of IO in Operation Noble Anvil
An IO After-Action Report
How an IO Campaign may have succeeded
Information Warfare and the People's Republic of China
Chinese IO as a Warfighting Network
What is the future of IO in China?
Introduction to IO in Australian Defence Forces
The Evolution of IO and Related Concepts in Australia
The Australian Doctrinal Approach to IO
The Australian Experience of IO – Two Case Studies
Bougainville - Background
IO Contribution to Operation BELISI
East Timor - Background
IO Contribution to Operation STABILISE
Lesson Learned and Directions Forward
Summary

Conclusion: What is the Future of Information Operations? 117

APPENDIX A – National IO Organization 119
APPENDIX B – IO Acronyms 120
APPENDIX C – IO and JOPES 123

Contributor's Biographies 125

Endnotes 128

Forward

Dr Dan Kuehl
Information Resources Management College
National Defense University

As I write this foreword, I watch the unfolding story and imagery of the 11 September terrorist attacks on the World Trade Center and the Pentagon, and reflect on the evolving and complex synergy between information and national security. As tens of millions of Americans sit, like myself, glued to our TVs and computers, the realization that literally hundreds of others worldwide are watching the same images simultaneously merely reinforces what we in the Information Operations field have been arguing throughout most of the past decade…the world in which we live and work has become an information fishbowl. More than a fishbowl, in fact, the global information environment has become a battlespace in which the *technology* of the information age – which is the aspect that we all too frequently focus on – is used to deliver critical and influential *content* in order to shape perceptions, manage opinions, and control behavior. It is perhaps merely coincidence that the time gap between the two aircraft crashes into the twin towers of the World Trade Center was sufficiently wide to allow for live TV coverage of the second crash – but I doubt it. As we watched in horrified amazement, the 18-minute gap between the two attacks allowed for virtually every available TV camera in new York City to be trained on the Towers and thus capture the dramatic and terrible imagery live. Ironically, the very day before this tragic event, I told a class at the National Defense University that someday we would see a terrorist act staged and timed to be seen by a live TV audience…little did I imagine that I would see it enacted so soon, and so close to home.

Thus the importance, relevance and timeliness of this book. Information Operations are playing an increasingly important role in our national security affairs, and as these event's indicate, that role will not be confined to the traditional battlefield on which tanks, ships and planes move and fight. This new battlespace is focused on the "wetware", the "grey matter" of the brain in which opinions are formed and decisions made. The most – perhaps only – effective weapon in this battlespace is information, and the hallmarks of the information revolution, such as transparency of events and the global immediacy of coverage, have only heightened the importance and impact of Information Operations. These attacks provide a ghastly example of asymmetrical warfare that employed information technology and exploited the speed and reach of global connectivity to deliver content that has been described as "shocking" and "staggering", indicative of its emotional and potential political impact. Military personnel as well as civilians will need to incorporate the full range of Information Operations into their plans and future missions, therefore I believe that this book helps to educate these current and future leaders on the capabilities inherent to this new era of warfare. If our nation is to exploit the opportunities provided by Information Operations and defend our vulnerabilities, than it will be through education and training from books such as these that lead to a greater awareness and contribution toward our national security.

Introduction

"Would you recognize a revolution if you were in it?"

Deep in the jungles of southern Mexico, a rebel leader taps on a notebook computer. He is editing his dissertation that will soon be released to the world with a double click of the mouse. It is 31 December 1994, and Sub-Commandante Marcos has just begun a series of revolts throughout the state of Chiapas in the southern region of Mexico, taking control of several villages in the process. The Mexican Army response was immediate with 12 days of brutal fighting following the insurrection, yet inexplicably the Mexican government halted their operations short. Although the Mexican Army could have finished the suppression of the Zapatistas, they instead began a series of negotiations that continues to the present day. Why did President Zedillo and his cabinet stop their attacks on the Zapatistas? What factors led to the pause in the fighting that has kept all parties at the bargaining table?

Instead of operating an insurrection by holding rallies and conducting violent acts, the Zapatistas sustained their protest through a series of new and innovative acts of Information Operations (IO). In effect, they dominated the information realm, competing with the Mexican government in a creative information campaign, that effectively constrained and manipulated the Mexican government over the last six years in an effort to bring about reform in the Chiapas region. Using Non-Governmental Organizations (NGOs) and the media, Marcos spread the plight of the Chiapas people to activists that pressured President Zedillo and his cabinet. The media coverage forced the Mexican government to halt their suppression of the indigenous peoples of southern Mexico and effectively put any national policy under scrutiny.

Electronic Disturbance Theatre

More recently, a small group of activists, known as the Electronic Disturbance Theater (EDT) has supported the Zapatista movement. A typical scenario for the EDT was to publicize an attack weeks before the actual event. They used chat rooms, Internet advertisements and computer conferences to promote their next Floodnet attack and gain publicity.[1] To increase its effectiveness, the EDT signed up thousands of participants for their Floodnet attacks. In April 1998, the Floodnet program attacked Mexican President Zedillo's website, quickly crashing the server. More attacks continued during the summer of 1998, to include the Mexican Interior Ministry and Mexican Embassy in England with the largest event planned for 9 September 1998. Bulletins were released in late August and EDT publicized the impending attack with their Open-Ex exhibit at the Art Festival in Linz, Austria during this time. The intended targets were President Zedillo, the Frankfurt Stock Exchange and the Defense Information Systems Agency (DISA).

Since these were publicized "performances", DISA was concerned as to how to thwart these attacks. There were many inquiries by United States military personnel into Floodnet and the EDT during this period in order to gain knowledge about the purpose of the attack and the nature of the Floodnet applet itself. When the actual attack occurred on 9 September, DISA was ready to defend its network. A system administrator at DISA changed the Perl script on the Floodnet applet, which in effect became an electronic countermeasure effort and in some eyes, an

offensive act. This new applet shut down the web browsers of the users that were supporting the attack by EDT.

Fact or fiction? This scenerio is indeed true and it is a current example of IO at an unclassified level. In particular, the execution of "denial of services attacks" by the EDT radically altered the concept of cyberwar and brought a new term into our lexicon, namely "Hactivism".[2] These Zapatista sympathizers were true innovators and are recognized by their peers as information warriors' extraordinare. A measure of their success is the amount of space devoted to the Zapatista revolt by the media. Whether an attack succeeded or not did not matter to the EDT, as long as they received publicity. The Floodnet program was simply a "tool" to get media attention for the Zapatista cause. To date, the insurrection in Chiapas has garnered more media attention than any other insurgent group in Mexico.[3] The new President of Mexico, Vicente Fox has demonstrated his resolve for supporting a peaceful solution to the Chiapas situation, however it remains to be seen if the EDT can maintain their high focus of IO efforts.

The Power of Information

This book is written by the Joint Command, Control, and Information Warfare School (JCIWS) instructors at the Joint Forces Staff College (JFSC), as well as our guest speakers and former students. We are professional Information Operations instructors, who conduct the only joint Information Warfare (IW) course in the United States. In that capacity, we teach over 1000 personnel each year in a variety of IO and IW courses dealing with operations in the information age and how information is changing the way warfare is conducted. This book was written to meet a perceived gap in the education process of our IO students. It is structured to not only teach the capabilities and related activities of IW, but also give an update of the changes in IO that have occurred over the last three years. From the incredible reaction to Eligible Receiver '97 to the incorporation of JV 2020, IO has changed immensely. In essence, this textbook traces the IO doctrinal changes of not only the United States, Russia, and China, but also events around the world. The continual evolution of Information Operations makes this an exciting business. As will be detailed in the next chapter, in the last three years alone, 95% of the existing IO organizations have been created!

Often we are asked what has changed recently to make IO that different from other new weapons or military doctrine. The most important concept to remember about IO is that it is not a weapon per se; it is a process. IO is a way of thinking about relationships. IO is an enabler, a "source multiplier," a tool that increases one's ability to shape the operational environment. It is a planning methodology, which supports the strategic, operational and tactical use of traditional military forces. It is also a strategy, a campaign, and a process that is supported by traditional military forces. IO does this by using planning tools to synchronize, synergize, and deconflict activities as well as enabling the horizontal integration of these activities across the interagency spectrum. In this book, it is our intent to explain not only how important IO is to the future of warfare, but also how this warfare area is changing the way that the military is organized and how it conducts operations in the information age.

During the Cold War, the United States and its allies knew who was the enemy. The Soviet Union and the Warsaw Pact, were easily the most recognizable of the "threats" to the free world, but other nations such as China, North Korea, Iran, Iraq, Syria and Libya were also part of

the equation. To use an academic term, the bipolar Cold War era was an area of "realist" conflicts, with states as the prime actors and huge issues at stake.

Fast forward 10 years. The former Soviet Union is a shadow of its former self, with a population less than the United States and shrinking. Russia's defense budget is less than 5% of the DOD's and it cannot deploy a number of its forces because of equipment failures. Likewise North Korea is embracing South Korea; Iraq is in a box (literally); Iran is undergoing a transformation; Qadaffi is in self-imposed exile and even China is initiating some democratic processes. So why in this post Cold War era, when the great threats to mankind are gone or lessened, is the United States under attack? Its because the enemy has changed. There are still "rogue states" out there that can occupy the politicians and give credence to budget appropriations, but other groups have also attacked the United States as well. In the post-bipolar era, most of these NGOs or terrorist groups are now operating out from underneath the umbrella of either superpowers and therefore they have much more autonomy.

What has happened over the last decade and especially within the last 3-4 years, has been an explosion of attacks on networks within the United States by a host of organizations. Some are individuals, others are activists, foreign military units, terrorists and even nation states. Solar Sunrise, Moonlight Maze, Worm Explorer and the I Love You virus are all recent events that will be mentioned or alluded to later in this text. Each of these incidents in their own way has highlighted the vulnerability of not only the DOD but the United States government as well to these types of attacks.

What the future holds for the military forces and the National Security establishment is unclear, however there will be many times that the United States will be called upon to engage the multitude of threats and opportunities in this unpredictable age in which we live. Information and the incredible advances in technology have drastically changed the structure of world politics, military strategy, economics, information realm activities, and other familiar restraints that epitomized the Cold War. Now is the time to awaken to the realities of the information age. This book is not another high tech 'doomsday' scenario, instead it is meant to be an update for the millennium, to identify the threats to national security posed by cyber-terrorists, rogue states, foreign militaries, and the enemy within our borders, as well as showcase the opportunities available from a properly orchestrated information campaign. In addition, we also hope that this book illustrates the evolving military doctrine and national priorities that enhance the ability of the United States to win the information war and thus attain its national security goals in the future information age.

Chapter 1- Integration and Coherence - The Language of Information Operations

"There is a war out there, old friend - a World War. And it's not about whose got the most bullets; it's about who controls the information. What we see and hear, how we work, what we think. It's all about the information."[4]

Cosmo

This book is about power and how the face of power has changed immensely over the last decade. Our thesis is that information, as an element of power, is the most fungible and useful force at all political levels including the systemic structure of international relations in the post Cold War era. In an attempt to update the arguments set forth by Robert Keohane and Joseph Nye in their seminal book, *Power and Interdependence*, we will argue that the use of information is changing the idea of what we look for in the power capabilities within the world political structure. [5]

We base our theory on the fact that we now live in the information age - an era of networks and international organizations. Nation-states are losing power to hybrid structures within this interconnected architecture. Access and connectivity, including bandwidth are the two key pillars of these new organizations. Truth and guarded openness are the approaches used both in the private and government sector to conduct business. Time zones will be more important than borders. It will be an age of small groups, using networks to conduct swarming attacks that will force changes in policy.[6] Key features include:

- Wide open communication links where speed is everything
- Little to no censorship, the individual controls his own information flow
- Truth and quality will surface, but not initially
- Weakening nation-states and strengthening networks

Power - What is Power?

Power is many things to many different people. Generally people understand its use, they understand who has power and who doesn't. Power is one of those ubiquitous terms that everyone seems to understand but few can actually define. Many academics including Morganthau, Dahl, Waltz, Keohane and Nye have all written works on international relations that have addressed the nature of power and its effects on the global system. While one could agree on the merits of one definition over another, for the purposes of this paper, we will use the following construct. Power is defined as "the ability of A to get B to do something that B would not otherwise do."

Hans Morganthau, in his book *Politics Among Nations: The Struggle for Power and Peace*, defined the elements of national power as geography, natural resources, industrial capacity, military preparedness, population, national character, national morale and the quality of diplomacy and government.[7] No where is the use of information seen as an element of power. This begs the question, have the elements of power changed over the last three decades? If information is now accepted as an element of power, what has changed from previous theories? Or as many believe, information has always been an element of power, it's just that now we have the technology to harness that power. Whatever one believes, the explosion in computer, telecommunications and media technology has for better or worse changed our view of power.

> Traditional measures of military force, gross national product, population, energy, land, and minerals have continued to dominate discussions of the balance of power. These power resources still matter, and American leadership continues to depend on them as well as on the information edge... Information power is also hard to categorize because it cuts across all other military, economic, social, and political power resources, in some cases diminishing their strength, in others multiplying it.[8]

Critics of this new view of power have argued that because only 16% of the world has access to the Internet, that information cannot truly change global politics. Maybe that is true, but the standard has been set, and that benchmark is high.[9] No longer can dictators rule their country as a fiefdom, once people understand the power that is so readily available to them. The masses will clamor for the information revolution and as they experience its power, they will threaten the sovereignty of the nation that impedes their progress.

Yet ideas about the use and elements of power are changing. Twenty years ago, Barbara Haskell first discussed the idea of information as power in her article "Access to Society: A Neglected Dimension of Power" in *International Organization*. In 1990, Joseph S. Nye argued for the concept of "soft power", which includes information in his book *Bound to Lead*. More recently in a number of articles starting in the spring of 1996, various authors have highlighted the issues involved with the technological revolution of information. These ideas have also been mirrored by recent books such as *The Rise of the Virtual State* by Richard Rosecrance and *In Athena's Camp* by John Arquilla and David Ronfeldt, all of which discuss the role of information and how it is used to conduct foreign policy.[10]

The idea that information is the most important element of power has not been accepted by all academics. Neorealists still promote ideas of power politics while neoliberals talk about the globalization of the world. Both are correct, but neither camp has adequately been able to explain the changes in world events, especially in the last decade. Other academics have seen the power of information, but do not believe that it will change the basic fundamentals of world politics. And there are still a few who are unwilling to realize that they live in a world that is undergoing a revolution. That is where education and the power of information will play a key role. For whether these academics realize it or not, changes in technology especially in the last decade have rendered their old theories of power obsolete.

> Information technology is the sine qua non of both globalization and power - the locomotive on each track. It is integrating the world economy and spreading freedom, while at the same time becoming increasingly crucial to military and other forms of national power. Information technology thus accounts both for power and the process that softens and smooths power.[11]

Factors that Affect Power

There are many factors that are included by academics in the equation of power. Our belief is that information is now the most important element of power because it is the most transferable. The ability to transfer the power of information is what makes it so useful in the current political situation. Groups, organizations, nation-states and even individuals can now influence policy at the systemic level by using information. This was not necessarily the case a decade ago, but the vast explosion in technology, particularly in telecommunications and media propagation has vastly changed the power paradigm.

Power in the Cold War Era - What has Changed?

All of these changes have been recognized by a number of individuals from government, military and academia as noted in previous sections. As mentioned earlier, a number of books and articles have recently recognized how important information is as element of power. But it is the use of that information and its fungibility that makes it truly useful. The ability to transform information, to move it or display its power, all relates directly to its transferability. That is where technology has revolutionized the power structure. The merging of what were once stovepipe and separate areas has opened to everyone, access to information and a means to distribute it around the world. These ideas are important because they show the true power of information, and that is what has changed.

How one uses information will of course determine whether it is useful or not, but the mere fact that many academics are writing about the power of information shows that something has truly changed. Even the United States government has come to realize that indeed information is power and has begun a process to reorganize itself to take advantage of that fact. This process began with Operation Desert Storm and is continuing today. Lessons learned from that conflict point to the fact that the nation that can control the flow of information is going to win the conflict. Whether that information is in the form of military intelligence, propaganda, electronic wavelengths or a computer data stream, the ability to manipulate information will be a primary effort of future conflicts.

Military Power and Asymmetric Threats

In a technical sense, military power is often the easiest variable or factor of power to measure. Nation-states have done this since time immortal to compare and contrast military forces. Power throughout the ages has often been ranked solely on the perceived military capability of a nation and the ability of that country to use those forces. This factor is more scientific than some of the other areas and it has a somewhat useful function of defining weapons and hardware as tools of power. History has generally proven that military capabilities are not so much a reliable factor as many academics would have preferred. For example, how did the United States compare militarily to North Vietnam in 1964? By technical definition, there should have been no contest, yet 11 years later it was American forces that were withdrawing from an ill-fated contest. Likewise, what about the former Soviet Union and Afganistan? There was a huge disparity in military capabilities but it was the former Soviet Union who lost that military campaign and returned home vanquished. So why are military forces not a good measure of power? Because in our view, these weapons and hardware are not fungibile. You cannot adequately translate power in most cases without reverting to total war, which most nations are unwilling to do. Therefore, the most militarily powerful nations are handicapped in their ability to use their forces to affect desired political outcome.

Information Operations Theory

From the previous discussion, one should realize that the models and theories used by academics to analyze world politics, economics, and military power for the last fifty years are obsolete. Liberalism, realism and neo-realism are no longer sufficient constructs which adequately explain the current dynamics of international power. In addition, there has been a

substantial change in the nature of strategic, operational and tactical issues. Previous theories held that strategic concerns were normally a global issue, yet that construct has changed considerably. Now there are numerous events at the tactical level that can quickly elevate to affect the global area of responsibility (AOR) with the use of advanced technology or mass media. Therefore, we propose that in reality, the new construct for relating the level of military activity cannot be automatically assumed to correlate to a comparable AOR. In fact, as many people can realize, with today's new technology, often the smallest incidents can spark international or strategic concern as is readily apparent today.

New capabilities that have arisen from the marriage of technology and information have challenged the traditional elements of power including military, diplomatic and economic factors. These capabilities combined with advanced computing capability and data networking now makes available options to not only military and government officials but also commercial companies and private citizens that previously did not exist. However, the threats to the United States have risen as well.

Attacks on computer systems, negative publicity using the mass media, Internet spamming and the threat of infrastructure failure have been symptomatic of operations in this new era. No longer is the military and economic might of the United States transferable in many political solutions (witness Somalia). General Aideed manipulated the media to keep the militarily superior United States forces off balance throughout most of the operations during 1993. In fact, with the use of a $600 video camera, Aideed changed forever the United States foreign policy in the region. It was Aideed, a true information warrior, whose actions in Somalia, perhaps more than any other recent United States military operation, showed the internal power of information. While Operation Desert Storm introduced the world to the advantages of this revolutionary era, it was Somalia where the true power of Information Operations came to fruition. By no means is Somalia on par with the United States in a comparison of power, whether militarily or economically. Yet, because Aideed effectively used the mass media to his advantage, he in fact controlled the flow of events. The use of information to level the effects of power was instantly recognized and has since been established in doctrine. Since that time, IO has evolved to serve as a model for future assymmetrical conflict and by implication international relations.

IO Theory and Doctrine

Information Operations is an attempt by the United States to develop a set of doctrinal approaches for its military and diplomatic forces to use and operationalize the power of information. The target of IO is the adversary decision-maker and therefore the primacy of effort will be to coerce that person into doing or not doing a certain action. United States Counter-Terrorism Information Operations, as discussed in Chapter 3, are good examples of the use of this theory in action. To affect the adversary decision-maker, IO attempts to use many different capabilities such as deception, psychological operations and electronic warfare, to shape and influence the information environment.

The capabilities mentioned above have existed for a long time, but the umbrella term of IO is a relatively recent doctrinal definition. Originally developed in 1996 as a component of Joint Vision 2010 (JV 2010), IO is formally defined as "those actions taken to affect an adversary's information and information systems while defending one's own information and

information systems."[12] This white paper was written to establish a vision for how the United States military will operate in the uncertain future. To implement this vision and achieve "full spectrum dominance," four operational concepts were introduced in this publication.

- Dominant maneuver
- Precision engagement
- Full dimensional engagement
- Focused logistics

The essential enabler for all four of these concepts was doctrinally encapsulated as information superiority.[13] Defined as "the capability to collect, process, disseminate an uninterrupted flow of information, while exploiting or denying an adversary's ability to do the same," information superiority consists of three components of which information operations was a prime factor. [14]

Yet IO is still not understood very well. To many people, IO is simply computer warfare. Yet as discussed earlier in this book, IO is really about much more than that. It is as we have tried to articulate, an attempt by the United States to develop a strategy to use all of its capabilities to affect the many issues that it deals with in the post-Cold War era. With these changes in the elements of power has come the realization that militarily the United States could not solve all of its problems through kinetic means. IO is therefore an attempt to bring these different facets of power to bear on an adversary in a synergistic manner to achieve our natural objectives.

In June 2000, the United States published Joint Vision 2020 (JV 2020), the most recent explanation of future oriented military doctrine. This document elevates IO from the conceptualized sub-component in JV 2010 to one of two essential elements for success in future military engagements. This latest conceptual document reiterates the dominance of IO within the United States as a key to successful operations over the next two decades. Why is this so? What happened to make this change? Specifically in the four years between the publication of JV 2010 and JV 2020, much in fact has changed within the United States military, with many officers and government officials realizing that future warfare is going to increasingly involve IO. Lessons learned from Rwanda, Bosnia, and Kosovo have taught the United States military the value and inherent power of information. Officials within the government and uniformed services are beginning to understand how effective this new warfare area can be in shaping the battlespace. They have witnessed the impact of IO and understand that if used correctly and early enough in a campaign, IO can even allow one to avoid armed conflict, to not reach the point where the military must be called in to conduct operations.

Differences between IW and IO

The real key to making IO effective is to ensure that the horizontal integration and coordination of the interagency organizations are conducted early on, i.e. in the peacetime environment. As mentioned earlier, IO can be an effective tool for shaping the environment in the pre-hostilities phase, so that the actual need for hostilities may be avoided or minimized. However that is not always possible. Many military theorists contend that IW is what you do when IO fails. That is one difference but there are also subtleties between these two warfare areas as well. The difference between these two terms is that IW contains six elements and is mostly involved with the conduct of operations during actual combat, while IO on the other hand, includes these six capabilities and two sometimes integrated or related activities. IO is broader

than IW and is intended to be conducted as a strategic campaign throughout the full spectrum of conflict from peace to war and back to peace. Therefore IO is much more comprehensive than IW and it is in IO that the full integration across government agencies and with private industry must occur.

Information Warfare	**Information Operations**	
Elements	*Capabilities*	*Related Activities*
Computer Network Attack	Computer Network Attack	Public Affairs
Deception	Deception	Civil Affairs
Destruction	Destruction	
Electronic Warfare	Electronic Warfare	
Operations Security	Operations Security	
Psychological Operations	Psychological Operations	

A common complaint about IO is that because its definition is so broad, at once IO is everything and it is nothing. The elements, capabilities and related activities of IW and IO as listed above are separate and discrete warfare elements. Most have very old traditions and long-standing histories that do not necessarily mean that every action conducted in these areas is always associated with IO. There are elements of destruction that are not part of an IO campaign, likewise not every public affairs activity has to be tied to information operations. Yet in reality, all elements and their components of national power can be integrated into a satisfactorily planned/designed/executed strategy to allow the United States to attain its national security goals in the new millennium.

The concept of IO is intended to use the different capabilities and related activities to produce effects in an integrated fashion. Therefore, while one can try to use all eight capabilities and related activities to conduct an operation, more often than not, a good IO plan will probably only incorporate a few of these warfare areas. The basic idea is that one does not always have to resort to kinetic means. Instead for IO to work properly, the operators must understand the environment, assess their interests and the adversary's pressure points and then use whichever capability or related activity that will best affect the adversary. IO is much more of an intensive study of not only your adversary, but also your own forces more than perhaps many current military commanders have grown accustomed to. Yet, this idea is not new. Many theorists contend that Sun Tzu was the first information warrior. Even still, the capabilities and related activities of modern information operations have drastically changed since the days of Sun Tzu.

Capabilities and Related Activities of Information Operations

Listed below are the capabilities and related activities for Information Operations. These give a foundation for the umbrella theory of IO. Employment of these effects of IO are predicated on the ability of higher headquarters to articulate their intent, direction, restrictions, measures of effectiveness and timelines for the use of IO capabilities and related activities within their area of responsibility. Hence, a commander does not derive IO requirements in isolation of theater or strategic requirements.

- Civil Affairs (CA)
- Computer Network Attack (CNA)
- Deception
- Destruction

- Electronic Warfare (EW)
- Operations Security (OPSEC)
- Public Affairs (PA)
- Psychological Operations (PSYOPS)

The Evolution of IO Doctrine

The evolution of information operations as a major military doctrine in the United States is a relatively new phenomenon, and much of that critical thinking began in the early 1980s.[15] The size of the former Soviet Union's military concerned United States military analysts and planners. From 1975-85, the former USSR often outnumbered United States conventional forces 3:1, and, while the United States may have had a qualitative advantage, there are times when only sheer numbers count. In the Pentagon, military strategists were looking for methods to cut down on the former Soviet Union's advantage by attempting to counter traditional strengths with asymmetric non-nuclear attacks. In addition, these analysts noted that the former Soviet Union relied heavily on electronic warfare or *radioelectrionyaborba* (translated as Radio Electronic Combat) in much of its doctrine, and there was a feeling that the United States must combat this threat as well.[16] It was in this era, that some of the early ideas about effects-based planning began to evolve.

The demise of the Soviet threat to the continental United States and the shift from bipolar to multi-polar political scenarios has seriously affected American force structure and military doctrine. However, the biggest change in doctrine has been the huge technological changes that have evolved over the last 10-15 years. The advances in computers, software, telecommunications, networks, etc. have revolutionized the way the United States conducts military operations and makes it the premier armed forces in history. The sheer magnitude of the coalition victory in Operation DESERT STORM clearly showed to the world the overwhelming technological superiority of the U.S. military.

Thus from the lessons learned from both the United States experiences of the Cold War as well as the Persian Gulf War, perhaps the most important result has been the rise in the apparent value of information. It has became apparent to warfighters that the side that controlled the most information and retained the ability to accurately manipulate, use and disseminate that information was going to be victorious. Strategic planners at the Joint Chiefs of Staff began to think and write new strategy, most was highly classified, on the use of information as a warfighting tool. In fact, the first document, Department of Defense Document (DODD) TS3600.1 was kept at the Top Secret level throughout its use, due to the restrictive nature of this new strategy.

While the publication of TS3600.1 started a dialogue on IW within the DOD, its classification restrained a more general doctrinal exchange. The need for strategy to fit these revolutions in technology still existed, so a new concept of Command and Control Warfare (C2W) evolved. Officially released as a Chairman of the Joint Chiefs of Staff Memorandum of Policy 30 (CJCS MOP 30) *Command and Control Warfare* (8 March 1993), this document laid out for the first time in an unclassified format the interaction of the different disciplines which gave the warfighters the IW advantage. C2W was defined as containing these five pillars:

- Destruction
- Deception

- Psychological Operations
- Operations Security
- Electronic Warfare

Intelligence supported these five pillars in order to conduct offensive and defensive C2W. Some quarters of the military greeted this new concept of warfare with enthusiasm, while others were wary of any new doctrinal developments. However, the ability to integrate these different military disciplines to conduct nodal analysis against enemy command and control targets was highly lauded as a great improvement. Many units and all four services developed C2W cells and began training in this new doctrine throughout the mid-1990s. But there was a conflict between the CJCS MOP 30 and the DODD TS3600.1 doctrine, since IW was a much broader attempt to tackle the issue of information as a force multiplier, while C2W was more narrowly defined to apply only to the five pillars. The fact that the United States was writing strategy to conduct operations in peacetime against nations was considered very risky, therefore IW remained highly classified throughout much of the 1990s.

Yet the United States military recognized the need to develop commands and agencies to conduct these types of warfare in the information age and therefore, even though doctrine was still in the formative stage, organizational changes began in the early 1990s. The Joint Electronic Warfare Center at Kelly AFB in San Antonio, Texas, was renamed the Joint Command and Control Warfare Center in 1993, and would later be renamed the Joint Information Operations Center in October 1999. The uniformed services also created a number of new agencies beginning in 1995, including:

- U.S. Air Force - Air Force Information Warfare Center (AFIWC)
- U.S. Army - Land Information Warfare Activity (LIWA)
- U.S. Navy - Fleet Information Warfare Center (FIWC)
- U.S. Navy - Naval Information Warfare Activity (NIWA)

In addition to organizational changes by the services, new courses and schools were being developed to teach new tactics. The National Defense University (NDU) created a School of Information Warfare and Strategy in 1994 that was a full 10-month-long academic curriculum designed to immerse the National War College students in IW. Held for two years, NDU graduated 16 students the first year and 32 the second, however the course was subsequently canceled in 1996. This may have been due to a belief that IW instruction needed to be disseminated to a wider audience, so shorter courses and classes were developed instead to teach NDU students. Several of these still exist today, including a five-day intermediate IW course for mid-grade officers and a two-day IW overview for senior officers. The other official joint course on IW is taught at NDU's Joint Forces Staff College, formerly the Armed Forces Staff College in Norfolk, VA. Held for two weeks, seven times a year, the Joint Information Warfare Staff and Operations Course (JIWSOC) is aimed primarily at mid-grade officer's or civilian equilvalent government personnel who are serving in an IO cell or billet with a joint agency.

Doctrine continued to develop after the publication of MOPP 30. The formation of IW agencies and commands in the 1995 time period, not only filled voids in the services but also helped to resolve the conflict in the development of information doctrine and policy within the United States Government. There was a concerted push for declassification and better understanding of these concepts within the DOD, which resulted in the publication of DODD S3600.1, *Information Operations* (9 December 1996). By downgrading this document to the

Secret level, DOD opened IO to a wider audience. In a related effort, the Defense Science Board published its report on Information Warfare–Defense in November 1996. Together these documents attempted to clarify the differences between the older doctrine and for the first time introduced the use of Computer Network Attack (CNA) as an IO capability.

Thus, the formation of IW agencies and commands in the 1995-1996 time period have somewhat helped to resolve the conflict in the development of IO doctrine and policy within the United States Government. However, since DODD S3600.1 was still classified Secret, it limited greater discussion on the differences between IO and IW. The mid-to-late 1990's were also a period of early experimentation with IO. A number of exercises were conducted elevating the awareness of IO within the military and civilian communities. The CNA operations conducted during 1996 and 1997 exercises were particularly effective and drew attention to the fact that the DOD was vulnerable to this type of operation. There were still however questions regarding IO definitions and lexicon that would not be fully addressed until the release of the seminal publication, Joint Publication 3-13, *Joint Doctrine for Information Operations* (9 October 1998). For the first time, the DOD released an unclassified document to widely disseminate the doctrinal principles involved in conducting Information Operations. In addition, since IO efforts are often conducted long before the traditional beginning of active hostilities, the White House and the DOD realized they needed better coordination. This interaction between federal agencies within the executive branch brought about a renewed emphasis on the IO organizational structure. With so many different commands conducting different portions of IO, the staff at JFSC feel that IO Organization efforts are so important, that we devoted an entire section of this textbook to the intricate and complicated relationships of the quickly evolving IO structure.

Information Operations Organizations

IO by definition is normally broken down into offensive and defensive disciplines in order to better understand the relationship between different capabilities and their related activities. One can view the organizational structure of IO in the same manner. Most of the offensive capabilities of IO are retained and used by the DOD, Department of State (DOS), Central Intelligence Agency (CIA) and the White House. While these organizations do not control all offensive IO capabilities of the United States government, in general they tend to be responsible for the vast majority of such operations. The same, however, cannot be said of the defensive IO architecture, because these capabilities tend to be distributed out much further among the agencies. In fact it can truthfully be said that every organization is ultimately responsible for maximizing its own defensive posture whether it comes in the form of information assurance, force protection or operations security.

Therefore the overall U.S. Government IO architecture is neither simple nor easy to understand. Relationships have evolved over a number of years, for a variety of circumstances including political, budgetary and perhaps even arbitrary reasons. Many organizations originally designed to conduct certain missions are currently being asked to change in this new era of interagency cooperation. In fact, even as this book was going to print, the IO organizational structure was still evolving. The Secretary of Defense initiated an effort to take control of the somewhat chaotic DOD IO relationships to develop in concert with other agencies a more coherent organizational architecture.[17] The new Bush Administration has also recently indicated that additional changes would be forthcoming. However, for the purpose of this discussion, the

current (September 2001) disposition of commands, services and agencies involved in IO are outlined below.

Top-Level Leadership

To start at the top, the United States government has always been led by civilians. The President of the United States is the senior elected official, and together with the Secretary of Defense, forms the National Command Authorities (NCA). While the NCA can initiate offensive military action, only Congress can declare war.[18] What is very interesting about IO in relation to the NCA is that because offensive IO is often conducted before hostilities begin, the approval process for these operations often happens only at the very top of the chain of command. Therefore it is important to keep in mind that even though many organizations may have a role in the formulation of IO strategy, policy and tasks, the actual decision to undertake a particular offensive IO action will often come only from the NCA, in support of national-level goals. In addition to the President and Secretary of Defense are the Vice-President and the Secretary of State who are the statutory voting members of the National Security Council (NSC). When the NSC meets during periods of national crisis, they are supported by a number of other non-statutory and non-voting members.[19] The Cabinet, which is composed of 14 department heads known as Secretaries, assists the President in these executive efforts. These cabinet heads are also often referred to as the Principals Committee, and they have Assistant, Under, and Deputy Secretaries who are sometimes referred to as the Deputies Committee. Because IO is not limited to the DOD in its missions, other cabinet members, notably the DOS, Department of Commerce (DOC) and the Department of Justice (DOJ) have also begun to play major roles in the national IO architecture. In addition to cabinet-level agencies, the White House also has a number of different offices and agencies that are directly responsible to the President.[20]

Since IO is a process to integrate operations in the information age, it will be conducted across the spectrum of conflict. Due to the continuous nature of IO, the DOD may not always be the lead agency from the United States Government. In fact, there are many instances where other departments such as State or Commerce may be much better suited than the DOD to lead a part of the IO effort. A classic example may be a nation-building mission in Central America or perhaps the development of a business infrastructure in Southeast Asia. A byproduct of the horizontal integration and cooperation that evolved between the different government agencies is the development of whole new interagency partnerships.

Although the DOD doctrine for interagency operations can be found in Joint Pub 3-08, *Interagency Coordination during Joint Operations*, Vols. I & II, more likely it may take a much broader aspect of organizational and structural change to be truly effective in this new era. And that is exactly what President Bush proposed on 20 September 2001, when he authorized the development of a new cabinet level agency, charted with the mission of Homeland Defense. Chaired by former Pennsylvania Governor Tom Ridge, this new agency will probably most likely be modeled after the recommendations of the Hart-Rudman Commission on the National Security in the 21st Century. Conducted before the terrorist attacks on the World Trade Center or the Pentagon, the key component of this commission was the proposal to create a National Homeland Security Agency (NHSA) consisting of:

- Federal Emergency Management Agency (FEMA)
- US Coast Guard

- Border Patrol
- Customs Service
- National Infrastructure Protection Center (NIPC)
- Critical Information Assurance Office (CIAO)

While all the details of this new agency were not known by publication time, to be sure, it will be a major player in IO in the near future.

IO and the Interagency Process

The United States interagency process consists of both formal and informal procedures, which can be used to conduct IO missions. Established bodies such as the NSC characterize the formal interagency process, with its Principals and Deputies Committee, as well as the former Interagency Working Groups, now called Policy Coordinating Committees in the Bush Administration. These bodies attempt to coordinate, from the bottom up, with every effort made to resolve issues at the lowest level possible.[21] In addition, the Clinton Administration also published a number of policy documents called Presidential Decision Directives (PDDs). One of these, PDD-56, *Managing Complex Contingency Operations*, is especially important concerning the interagency process because the NSC is perhaps the only government agency that is tasked to coordinate the different departments of the government. By law, each department is a separate organization and only reports to the President. Therefore, the ability of the NSC to coordinate activities within the different departments is crucial to the overall success of any United States government policy. Thus, we see that the NSC will continue to evolve as an important entity in the interagency process.[22]

In addition to the formal and informal interagency process, the NSC is also involved in the promulgation of administration strategy and policy in several different methods. The first is the National Security Strategy, which was most recently published in its latest version in December 1999. This is a collaboration of many different departments and is a formal unclassified method of addressing the security concerns of the United States throughout the world. In addition, the Administration can initiate strategy and policy issues through a variety of means including Presidential policy (whether its Presidential Decision Directives (PDDs) for the Clinton Administration or National Security Presidential Directives (NSPDs) for the new Bush Administration), Presidential Determinations, Findings, Executive Orders, Presidential speeches, letters, memoranda, the State of the Union Address, press conferences, interviews, and statements by the President and other Administration spokespersons. The Administration can also issue policy through the use of reports to Congress and other published reports, including testimony to Congress, directives and instructions issued by various departments and agencies. Specifically concerning IO and the interagency process, the Clinton Administration used the promulgation of PDDs to form numerous groups and committees in its two terms to lead these specific interagency coordination issues:

- Peacekeeping Core Group (PDD-25)
- Counter-Terrorism Security Group (PDD-39 and PDD-62)
- Special Coordination Group (PDD-42)
- Executive Committees - Complex Humanitarian Emergencies (PDD-56)
- WMD Preparedness Group (PDD-62)

- Critical Infrastructure Coordinating Group (PDD-63)

In addition to the NSC, there are other executive advisors involved with IO. For example, within the Office of Management and Budget (OMB) resided the President's Council on Year 2000 (Y2K) Conversion. The council comprised more than 30 major federal executive and regulatory agencies that were responsible for coordinating the USG's efforts to resolve the Y2K issue.[23] Guidance for the Y2K council was amended in 1999, with the establishment of an Information Coordination Center (ICC) at the General Services Administration (GSA).[24] The ICC worked in concert with other Computer Emergency Response Teams to handle not only Y2K-related issues but also viruses and computer network attacks (CNA).

The other primary White House agency that is heavily involved with IO is the Office of Science and Technology Policy (OSTP) and its two sub-directorates, the National Science and Technology Council (NSTC) and the President's Committee of Advisers on Science and Technology Policy (PCAST).[25] These two councils act as executive advisers to the President and cabinet to coordinate the science and technology policy-making process within the U.S. government. Both agencies were highly successful in legislating technology-oriented issues during the Clinton Administration, specifically sponsoring and recruiting for federal support of computing and communications research and development. The OSTP also sponsors the Committee on National Security, which serves as the focal point for the debate on national encryption standards.[26]

DOD - OSD and IO

Turning from the White House to the Office of the Secretary of Defense (OSD), the primary assistant secretaries involved in IO issues include the Assistant Secretary of Defense for Command, Control, Communications and Intelligence (ASD/C3I) and the Under Secretary of Defense for Policy (USD(P)). Within the ASD/C3I there are a number of Deputy Assistant Secretaries (DASDs), with the most important from an IO viewpoint being the DASD for Security and IO (DASD S& IO). This organization is crucial because it is the one single directorate within the OSD that has both the offensive and defensive elements of IO for policy and programming. The DASD S& IO is also further divided into four different sub-directorates. Two of these, Infrastructure and Information Assurance (I&IA) and Information Strategy and Integration (IO S&I), employ most of the OSD staffers who are involved day in and day out in IO planning, policy, and strategy. Elements of the DASD S&IO organization are shown below:

To see how these interrelationships work, consider the IO mission-tasks of the OSD. Within the DASD S&IO directorate are sub-elements that coordinate across with many different agencies. One good example is the Critical Infrastructure Protection (CIP) policy branch, whose personnel coordinate daily with the Critical Information Assurance Office (CIAO) and the National Infrastructure Protection Center (NIPC), both of which are explained in detail later in this chapter.

Thus the various directorates of the ASD/C3I branch are prime proponents of both the offensive and defensive portions of IO. The other directorate of OSD, the USD(P) is also heavily involved with IO policy and doctrine. Most of their authority was derived from PDD-29 *Security Policy Coordination.*[27] This revision of the security policy process was needed to help give the United States greater security, given a wider diversity of threats in the post-Cold War era. The USD(P) also has a number of sub-directorates which have a number of IO policy issues including

who coordinates processes such as PDD-68 mentioned later. There has also been confusion on IO policy within the OSD. In a memorandum of understanding between USD(P) and the ASD/C3I during 1999, it was agreed that the USD(P) would have the policy lead on development and oversight of offensive IO, Psychological Operations (PSYOPS) and International Public Information (IPI).[28] The Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict (ASD SOLIC) retained IO tactics, technique and procedures that are unique to special operations forces. In turn, the ASD/C3I would have the lead for policy development and oversight of Information Assurance (IA) as explained in Chapter 3.

DOD - Combat Support Agencies

The Secretary of Defense is also supported by combat support agencies, of which there are nine. The three main staffs involved in IO are the National Security Agency (NSA), the Defense Information Systems Agency (DISA), and the Defense Intelligence Agency (DIA). Each of these agencies, in addition to conducting its typical support for traditional military operations, has also formed new units to support the unique needs of the IO organizational structure. The first two of these organizations will be discussed in this section, while the DIA will be covered under the intelligence community.

The NSA's IO Architecture

The NSA is the primary United States intelligence agency officially tasked to conduct signals intelligence (SIGINT).[29] Their charter takes many forms, most of which are highly classified, but clearly the NSA is very interested in the increase in computer hacker activity in the United States. Since it needs to monitor Computer Network Defense (CND) issues as much, if not more than other agencies, it is not surprising that it formed it's own Computer Emergency Response Teams (CERT). Titled the National Security Operations Center/Information Protect Cell (NSOC/IPC), this organization is a separate cell that stands a 24/7 watch to monitor SIGINT and information security incidents in order to protect NSA's networks from attack. Tied to this NSA CERT is another organization, the National Security Incident Response Center (NSIRC), which operates as an analysis center. This entity shares incidents and threat vulnerability information with all U.S. governmental departments and agencies and their contractors involved with the National Security Strategy.[30] The NSIRC develops the National Information Systems Weekly Incident Summary, which contains national-level, operationally fused data that correlates computer incidents and events that might formerly have been viewed in isolation by a uniformed service, CERT, or agency. NSA also participates in the National Security Telecommunications and Information Systems Security Council (NSTISSC), which was established as a senior-level policy coordinating committee to consider technical matters and policies. Its members include personnel from 10 different government departments and its primary mission is to protect national security systems.[31] In addition, the council also supports IA, information security and CND training, with a scope limited to national security information and systems. A final command under the NSA umbrella is the Joint COMSEC Monitoring Activity (JCMA). With detachments deployable around the globe, this activity performs information security monitoring, analysis support, communications security, and cryptographic monitoring.[32]

The DISA's IO Architecture

DISA, like NSA, is also located in the greater Washington, D.C. metropolitan area. Chartered to maintain and protect the majority of the DOD's computer networks, DISA is also very concerned with the detrimental effects of CNA efforts against the United States. It has had a CERT capability for a long time, namely its Global Network Operations Security Center (GNOSC), which is tasked to monitor the operational and security posture of the Defense Information Infrastructure (DII). While DISA does have a direct tie to the uniformed services for CND efforts, it does not have command authority to direct a military service to change network configurations or settings. Therefore, in 1998 after a series of well-publicized attacks on U.S. government computer networks, the OSD directed that DISA set up the Joint Task Force-Computer Network Defense (JTF-CND).[33] This command directly communicates with the other government agencies including the DOJ, the federal CERT, and NSA's CERT and the various Service CERTs. The JTF-CND is in effect the senior military CERT and the DOD response cell for CND issues, including recommending changes to the Information Condition (INFOCON) status when the situation dictates. In April 2001, this organization was renamed the Joint Task Force – Computer Network Operations (JTF-CNO) to reflect its growth in missions.

A number of other organizations within the larger DISA umbrella have existed for years, but are now being adapted to perform IO missions. These include the National Communication Systems (NCS), the National Security Telecommunications Advisory Committee (NSTAC) and the Joint Spectrum Center (JSC). The NCS was created to ensure governmental communications after problems occurred during the Cuban Missile Crisis. Comprised of 23 federal agencies and the telecommunications industry, the NCS maintain's a coordinating center to resolve failures of the public switching network.[34] The NCS maintains a private communications network, in addition to a HF radio system, independent of the public switched network, to provide connectivity to the Federal Communications Commission, regional Bells, GTE, Sprint, and switch manufacturers.

The NSTAC was created in the aftermath of the American Telephone & Telegraph divestiture and serves as a forum for addressing the risks to United States National Security posed by potential threats to national telecommunications and information industries.[35] It represents a joint government/industry partnership the likes of which have not been seen since World War II. Comprised of 30 chief executive officers from the telecommunications, information technology, aerospace, and banking industries, NSTAC makes recommendations to the President on issues critical to protecting the United States communication infrastructure, and their role grew in importance due to Y2K issues in 1998-1999. This committee also boasts a 15-year string of successes including the establishment of a National Coordination Center for Telecommunications, a Network Security Information Exchange and a Government Emergency Telecommunications Service. In addition to these public-private partnerships, DISA also has purely military units that have major roles to coordinate IO products. The Joint Spectrum Center in Annapolis, MD is an outgrowth of a need to coordinate frequency spectrum management, and it also assists in the development of the joint restricted frequency list, and the resolution of operational interference and jamming requests.[36]

A final command that is worth mentioning under the DISA community is the Information Assurance Technology Analysis Center (IATAC). This staff is responsible for a number of functions and tasks, but the one that is probably most useful to the IO operator or planner is the

education role. IATAC has done a magnificent job over the last few years in making and distributing a wide variety of IO and especially IA teaching tools. Some of these are soft copy, others are distributed as CD-ROMs, but nonetheless, they are invaluable to helping the IO professional complete their mission.[37]

DOD - The Joint Staff and IO

From the uniformed military perspective, the Secretary of Defense is supported by the Joint Chiefs of Staff, which is comprised of a senior military officer from each branch of service plus a chairman and vice-chairman. These officers, in particular the Chairman of the Joint Chiefs of Staff, are tasked to act as the principal military advisers to the NCA. While the Joint Chiefs of Staff do not "own" or actually command troops in combat, nonetheless their advice, more often than not, has a great effect on the U.S. military. The Joint Staff supports the Joint Chiefs of Staff, and it is organized along typical U.S. military doctrinal terms, with J-3 being Operations and J-39 being the Director of Information Operations. The J-39 directorate is responsible for IO doctrine and has authored the baseline DOD document, JP 3-13, *Information Operations.*[38] If there is one office that is the central point for IO in the Pentagon, then J-39 would be it. The J-39 staff is the primary JCS organization that interacts with OSD staffers (specifically DASD S&IO) and they are also the liaison to the Joint Chiefs of Staff for each CINC IO cell.

In a coordination role, you will also see the J39 staff working with a number of different DoD staffs such as ASD/C3I and USD (P) as well as other USG and interagency commands to ensure continuity of IO plans and doctrine. But since so much of IO is really nothing more than detailed integrated planning, J39 more often than not, will not be tactically involved with each and every CINC IO cell plan. Instead they will attempt to stay focused on the broader issues, such as those involving IO policy, strategy and doctrine. There is no such entity as a CINC IO. While several UCP proposals have illuminated this deficiency, to date, no new command or sub-unified agency has been formed. Instead all CINCs have emphasized their particular specialities and capabilities associated with IO. A good example of this is SOCOM which has combatant command of the PSYOP and Civil Affairs forces for the US Army. However with the emergence of CND and CNA as warfare areas, few CINC staff's has identifiable skills in these types of operations.

In the offensive-defensive IO terms mentioned in the last chapter, it would be preferred to have staffs represent both sides of the warfare spectrum for IO and that is what the DOD has done. Thus while J-39 is a full-spectrum staff for IO, it is also primarily an offensive-oriented organization. On the defensive side for the Joint Chiefs of Staff is the J-6 organization, or the Command, Control and Communications (C3) department. Specifically for IA or CND, J-6K has been designated as the responsible staff to deal with these asymmetric threats.[39] It maintains liaison closely with DASD S&IO as well as the Service CERTs, JTF-CNO, and CINCs' J-6s.

The CINCs

The real locus of operational-level planning for IO is usually with the military combatant Commander-in-Chief (CINC) and their IO Cells. It is the CINC who is often engaged in IO on a day-to-day basis. IO planners on the CINC's staff use the National Security Strategy (NSS) and National Military Strategy (NMS) as their guide to outline in broad terms the CINC's operations

plans and Theater Engagement Plans. These CINC IO cells are also involved in the day-to-day operations that are not necessarily directly combat related. For example, the 1999 NSS charters the CINCs to plan to conduct a variety of operations including Non-Combatant Evacuation Operations, Special Forces assistance to nations, humanitarian and disaster relief, etc. But probably most important is the daily overseas presence mission that encompasses a host of operations that take the U.S. military into areas far beyond their traditional bases. In addition, the task of supporting other national objectives also brings the United States into operations other than war. It is crucial that these CINC planners integrate these operations with their other executive department counterparts.

In the United States military, CINCs are also the actual commanders that "own" military forces. There are nine CINCs, of which four are regional:

- Central Command (USCENTCOM), Tampa FL
- European Command (USEUCOM), Stuttgart, Germany
- Pacific Command (USPACOM), Honolulu, HI
- Southern Command (USSOUTHCOM), Miami, FL

The other five are functional and conduct their missions across the globe:

- Joint Forces Command (USJFCOM), Norfolk, VA
- Space Command (USSPACECOM), Colorado Springs, CO
- Special Operations Command (USSOCOM), Tampa, FL
- Strategic Command (USSTRATCOM), Omaha, NE
- Transportation Command (USTRANSCOM), St Louis, IL

Each of these CINCs has an IO cell as part of his staff. Typically, these CINC IO cells are very small in manpower, but they can expand during actual contingency operations or planning. Each cell is responsible for the detailed IO planning done for its particular CINC; however, it also normally coordinates and works in conjunction with the J-39 division of the Joint Chiefs of Staff, which has overall responsibility for IO as discussed earlier.

Outside the strategy and policy arena, a number of DOD organizations have been formed in the last years or have evolved from older legacy commands agencies. In addition, some of these commands were in the "black" world and emerged only with the recent downgrading of the classification of certain IO terms. Originally a number of these agencies worked directly for the Joint Chiefs of Staff or USJFCOM. However, that changed with the Unified Command Plan 1999 (UCP '99) which gave USSPACECOM the lead in CND effective 1 October 1999 and CNA effective 1 October 2000.[40] USSPACECOM will be a supporting CINC to the other commands for these missions as well as coordinating with the Joint Chiefs of Staff on these issues. With UCP '99, JTF-CND as well as the Joint Information Operations Center (JIOC) were reassigned to USSPACECOM.[41] A counterpart to the senior federal CERT set up at the FBI headquarters (NIPC), JTF-CND was originally designed to be a small staff (24 personnel) who would stand watches and analyze the military implications of a failure to a network or system. Therefore not only did the original contingent include computer experts and military lawyers, but there were also operators including fighter pilots among the staff.

As mentioned elsewhere, on 1 October 1999, JTF-CND has assigned to USSPACECOM as part of the transfer of the CND mission to that CINC. Manning has been somewhat increased with a number of allied officers detailed to the command. In addition, there is also discussion of forming an international JTF-CND with Australia, New Zealand, Canada and the United

Kingdom as primary members. Most of the impetuous for this sharing actually came from the United States. When the "ILOVEYOU" virus hit last year, it was Australia and New Zealand commands that were the first to know, but releaseability issues hindered the notification of other Allies. To date, JTF-CND has had a pretty good track record. The use of INFOCONS by the DOD, an original function of the command has been well received and in many respects, JTF-CND gets more respect as a CERT than the NIPC. This is for a variety of reasons but most importantly may be the willingness to handle all agencies fairly and without a political agenda.

As recently as the winter of 2000-2001, additional changes occurred in the organizational structure of USSPACECOM with respect to IO. It was during this period when the Deputy Director of Operations for Computer Network Attack (DDO-CNA) was formed. This small staff of seven individuals was developed to support USSPACECOM in its efforts to advocate CNA within the Pentagon, as well as to facilitate the approval process. In February 2001, this group was merged with the JTF-CND to form the Joint Task Force – Computer Network Operations (JTF-CNO) to better meet the needs of USSPACECOM to conduct IO. Other changes occurred as well when on 2 April 2001, JTF-CND changed its name to JTF-CNO to better reflect its missions and operations. Once again, these changes emphasize the continual evolution of the organizational architecture of IO.

Additional DOD IO Elements

In addition to J-39, OSD, and CINC IO cells, a number of other "players" or agencies also have a piece of the IO pie. First, the Intelligence Community (IC) is made up of many diverse agencies, such as the CIA, DIA and NSA, which have a long history of involvement in capabilities normally associated with IO, such as operations security (OPSEC) and military deception. Originally many of these organizations were formed to conduct a certain mission or operation and not intended to interact as they are currently being asked to do. They were stovepipe agencies or legacy commands that reported vertically up and down the chain of command. Now, because of IO and the urgent need to have interagency cooperation, it has become much more common for all of these unique organizations to work together. In fact, most of the CINCs have a number of permanent intelligence representatives assigned to act as agency liaison for IO missions. The intelligence community is also heavily involved in supporting operational requirements for IO with permanent seats on a number of interagency groups and committees. Of particular importance are the Bilateral IO Steering and Working Groups (BIOSG/BIOWG) that define IO policy and deconflict IO issues between the DOD and other agencies. Typical members of the BIOWG are at the one-star level. These members define the issues and lay the groundwork for the BIOSG, which actually makes the decisions and writes policy at the three-star level and normally includes representatives from the OSD, the Joint Staff and the IC.

Cabinet IO Interests

Other departments besides the DOD also have vested interests in IO. Because of the global and over-arching role of IO, agencies such as the DOS, DOC and DOJ have begun to play roles that are much more important in IO, especially in the defensive arena. Much of IA is defined in business or legal rather than military terms; therefore, it is only natural that these organizations have begun to carve out their niches in the IO structural architecture.

Department of State IO Concerns

In the foreign policy arena, the State Department is the major activity that conducts diplomacy for the United States around the world. With the need to present a coherent public affairs and information front to the international media, DOS has recently reorganized to bring the formerly independent United States Information Agency (USIA) into it's larger umbrella organization. Renamed as the Under Secretary of State for Public Diplomacy and Public Affairs, this new directorate now coordinates both International Public Information (IPI) and Public Affairs (PA) areas within the DOS.[42] Although both of these areas are discussed later in Chapter 4, it is important to note that both are crucial to the success of an IO campaign. This was evidenced by the publication of PDD-68, *International Public Information*, during the middle of the Kosovo campaign in 1999.[43] To win the hearts and minds of an enemy, and to achieve one's operational and strategic goals, you must be prepared to influence foreign audiences with a coherent message.

Traditional DOS Structure

The interaction between the CINC and foreign nations relies heavily on the Ambassador and the country team. State Department representatives are essential to successful operations and as such have broad powers. The key members include:

- DOS Regional Secretary
- Ambassador
- Political Advisor
- Country Team
- Resident Military Representative

The Ambassador and the country team have several documents and policies that they use to plan their operations within their area of interest. These policies and programs are important to the interagency process because they must be taken into consideration in any CINC's TEP or operations plans. They include the DOS Regional Program Plan (RPP), which defines regional and country objectives and strategy. The DOS RPP is prepared by DOS Regional Assistant Secretary and is a product of the interagency process, which reflects the International Affairs Strategic Plan. At the Embassy, the Mission Program Plan (MPP) is prepared by the country team and is the Ambassador's country engagement plan. Of special notice to military planners, the CINC's TEP should consider all MPP's of interest in their AOR. These documents are readily available to the CINC's planners and can be found in the DOS's Congressional Presentation for Foreign Operations. These documents are important because they contain measures of effectiveness, objectives, and priorities for the State Department in support of the NSS.

DOC IO Architecture

The State Department is not the only cabinet-level agency that is changing under the influence of IO. The Department of Commerce (DOC) has also played a major role in IO over the last five years. One of the reasons for a cabinet agency that is primarily concerned with business and finance to be involved in this new warfare area is because the DOC is heavily involved in the second of the two new capabilities, namely Computer Network Operations.

While the DOS as mentioned earlier has a huge role in perception management, DOC on the other hand has an equally important mission concerning CNO.

The DOC is the host agency for the Critical Information and Assurance Office (CIAO), the sub-directorate agency that was established as a direct result of the proclamation of PDD-63, *Critical Infrastructure Protection (CIP).*[44] CIAO is officially tasked to coordinate CIP within the US government, and it evolved from the Presidential Commission on Critical Infrastructure Protection (PCCIP). This group was comprised of government officials, commercial businessmen, military and civil service personnel, as well as academics. These executives met over an 18-month period and in the end produced a document called *Critical Foundations*, which linked CIP to national security and identified eight critical industries:[45]

- Telecommunications
- Electrical power systems
- Gas/Oil storage
- Banking/Finance
- Transportation
- Water supply systems
- Emergency services
- Continuity of government

These industries are essential to the economic and security infrastructure of the United States.[46] The publication of *Critical Foundations* led directly to the formulation of PDD-63. Tied into a larger Clinton Administration effort to counter terrorism, PDD-63 has a sister directive, PDD-62, *Counter-Terrorism* with both documents coming under the authority of the NSC (discussed in further detail in Chapter 3). The eight industries identified as crucial to the security of the nation were then tied to a cabinet department as well as a comparable private industry association as tasked in the publication of PDD-63. Together, the United States government and private industry have produced a CIP plan to work together to protect these resources from attack.

In addition to the CIAO, the DOC also hosts the National Institute of Standards and Technology (NIST) and the National Telecommunications and Information Administration (NTIA). The mission of the NIST is to promote economic growth around the world.[47] It does this by working with private companies to develop and apply technology, measurements, and standards. Specific tasks include the following:

- Assist industry to develop technology to improve product quality
- Modernize the manufacturing process
- Ensure product reliability
- Facilitate rapid commercialization of products based on new scientific discoveries
- Develop information system security guidelines, procedures, and technological solutions to help Federal agencies implement OMB policy.[48]

The current areas of interest for the NIST include electronic commerce, public key encryption, common criteria for information technology, advanced authentication, and the Federal Computer Incident Response Cell (FEDCIRC). NIST also hosts the Federal Agency Computer Security Program Managers' Forum, which advocates information exchange on information technology issues.[49] The forum cannot command or regulate changes, but instead is mainly used as an information-sharing group. In addition, the NIST also collaborates with the

NSA in the National Information Assurance Partnership (NIAP). This organization was designed to combine the extensive computer security experience of both the DOC and NSA.[50] NIST is also the host for the Information Infrastructure Task Force (IITF), which works with the private sector and government agencies under the host of the OSTP. NTIA, on the other hand, is the principal voice of the executive branch on domestic and international communications and information technology issues.[51] Specifically this group was involved in the Telecommunications Act of 1996, that eliminated many barriers to ownership and operation in the telecommunications and broadcast industry, making private ownership far easier than before. The relaxing of requirements has made it harder to secure and control the National Information Infrastructure (NII) but one has to ask if you really can or should try to control the Internet. Finally, the DOC also hosted the United States government Y2K Task Force, which was an offshoot of the PCCIP process and the CIAO.

DOJ IO Architecture

The other organization recommended in *Critical Foundations* was an information-warning center. Although similar in concept to the CERTs (which were already in existence), it was envisioned that this new legal center would use Federal Bureau of Investigation (FBI) expertise to prosecute cyber-crimes at a national level**.** In 1998, the FBI formed the NIPC, which is charged to maintain liaison with law enforcement personnel throughout the nation, as well as with all 56 FBI field offices.[52] NIPC is also tied into the CND arena with contacts at the JTF-CNO and NSA. Together this allows the executive branch to use its legal authority under the FBI and DOJ to prosecute cyber-terrorism within the United States.

Interagency IO Organizations

The fact that IO requires significant horizontal integration is most significant with these different cabinet agencies. Numerous interagency groups and councils have been formed to help conduct the needed IO integration by the United States. Some have been mentioned previously but these included in the Clinton Administration:

- Bilateral Information Operations Steering Group (BIOSG)
- Bilateral Information Operations Working Group (BIOWG)
- Critical Infrastructure Protection Working Group (CIPWG)
- Defense Information Assurance Program Steering Group (DIAPSG)
- National Information Assurance Program (NIAP)
- National Science and Technology Council (NSTC)
- National Security Telecommunications Advisory Committee (NSTAC)
- National Security Telecommunications & Information Systems Security Council (NSTISSC)
- Office of Science & Technology Policy (OSTP)
- President's Committee of Advisors on Science & Technology Policy (PCAST)
- International Public Information Interagency Working Group (IPIIWG)

Some of these activities were mentioned earlier in the DOD section, but there are also other IO-related groups or councils in the OSD which include the Defense Information Operations Council (DIOC) and the Defense-Wide Information Assurance Protection Steering Group (DIAPSG). These activities are both three-star working groups that try to coordinate and

deconflict IO issues within the DOD. A final interagency working group from the Clinton Administration was the Forum of Incident Response and Security Teams (FIRST). Hosted by the Department of Energy (DOE), this forum has a long history of working with various CERTs to combat computer viruses and attacks.[53]

Interagency coordination involves much more than just organizations originating from the United States government. Academia, private industry and coalition governments are also crucial for the development of true interagency operations. This can be seen as recently as the Kosovo campaign in 1999. It was here that the utility of working not only in the joint world but also in the combined world with other nations and organizations demonstrates how crucial that interaction can be. In addition, private or commercial agencies may be involved in one form or the other in interagency operations. These include NGOs and Private Voluntary Organizations (PVO).[54] NGO is a term normally used by non-United States organizations and examples include:

- Concern Worldwide Limited
- International Organization for Migration (IOM)
- Medecins Sans Frontieres (MSF) - [Doctors without Borders]
- OXFAM
- Save the Children

A term that is starting to go out of use is that of Private Voluntary Organizations or PVO which is a non-profit humanitarian assistance organization involved in development and relief activities. In the last few years this term has started to disappear and most of these organizations are routinely called NGO's as well. Examples include:

- Action Internationale Contre La Faim (AICF)
- Adventist Development and Relief Agency International (ADRA)
- AFRICARE
- American Council for Voluntary International Action (INTERACTION)

In an IO mission, it is crucial that the CINCs understand and appreciate the importance of the NGOs. These organizations are crucial to the success of that mission when conducting IO during peacetime or in Military Operations Other Than War (MOOTW). These factors become much more evident when counter-terrorism information operations, as discussed in Chapter 3. Often the NGOs can operate where uniformed military personnel cannot and they can often gain the trust of the locals much better than any U.S. government agency. In addition, NGOs may have capabilities including communications, transportation, public affairs and medical facilities that rival or surpass those available to a CINC in a particular area. It is in the CINCs best interest to be actively engaged and to work closely with the NGOs and PVOs in the area of operations. As a CINC or United States military planner, one cannot command or direct NGOs to conduct missions. Instead, what normally works best is to facilitate these agencies and to work with them in order to conduct one's operation. Again, horizontal integration is the key to success for IO.

Summary

In conclusion, there are clearly a large number of "players" in the IO arena, and trying to understand how they all relate can be quite complicated. Much of this organization is relatively new and, in fact, has changed considerably from 1997 to 2001. However, throughout this discussion of national IO organizations, the one overriding theme to remember is that for IO to

succeed there must be cooperation between all parties involved. This means horizontal as well as vertical and includes not only U.S. government agencies and departments, but also non-governmental units and private industry as well. So much of IO now crosses old departmental boundary areas which is also important because IO encompasses much more than the traditional DOD missions and policies. Therefore if the United States is to succeed, it must coordinate its actions with all of the players involved and only through cross-departmental communication flow by all organizations will IO become the true force multiplier that it has the potential to be.

Chapter 2 - Intelligence and Exploitation – Foundations for Conducting IO

"Know the adversary and know yourself, and in a hundred battles you will never be in peril. When you are ignorant of the enemy but know yourself, your chances of winning and losing are equal. If ignorant of both your enemy and yourself, you are certain in every battle to be in peril.[55]"

Sun Tzu

Intelligence is the bedrock of IO. It is both foundational and essential to all military operations and its importance to IO is crucial. Skeptics may simply turn to the executive summary of JP 3-13, where the following statements appear within the first four paragraphs of the text:

"Intelligence and communications support are critical to conducting offensive and defensive information operations."

"Intelligence support is critical to the planning and execution, and assessment of IO."

"Intelligence preparation of the battlespace is vital to successful IO."[56]

Intelligence is also a key element of information superiority. As mentioned earlier, one of the components of information superiority is relevant information. There is some discussion within the intelligence community on the distinctions between "information" and "intelligence." JP 2-0, *Doctrine for Intelligence Support to Joint Operations* defines intelligence as "information and knowledge about an adversary obtained through observation, investigation, analysis or understanding," as well as "the product resulting from the collection, processing, integration, analysis, evaluation and interpretation of available information concerning foreign countries or areas."[57] Thus the key factors in determining the intelligence value of information are its "relevance" to the current military operation and its "applicability" to answering a Commander's Critical Information Requirements.[58]

The Application of IO

This section explains how intelligence supports information operations. It describes the intelligence cycle and how intelligence products get to the consumer, how the intelligence community is structured to support IO, intelligence support to IO planning, the joint intelligence preparation of the battlespace process and finally some of the unique challenges that JV 2010/2020 bring to the intelligence community.

Current JCS policy guidance on IO is set forth in CJCSI 3210.01 which states, "Intelligence requirements in support of IO will be articulated with sufficient specificity and timeliness to the appropriate intelligence production center or other intelligence organizations to meet the IO demand."[59] What this means is, that one must know exactly what one wants and one must know how to get it. An oft-heard cry in the IO field is, "I don't know enough to ask the right questions!" Like ships in the night, the IO and intelligence players are often just missing each other because they lack the ability to articulate exactly what it is they want to or can do to support the commander's mission. The way this often plays out is that intelligence producers "push" a lot of intelligence products to the consumers in the IO community who "pull" down what they want and discard the rest.[60] The formation of IO cells and the constant interaction of the J-2 and J-3 IO players on a CINC staff have done much to improve communication at the operational level, but there are still weak links at the strategic level between the intelligence and

operational communities, as well as the diplomatic (DOS) and military (DOD) intelligence communities.

Joint Publication 2.0 *Joint Doctrine for Intelligence Support to Operations* (March 2000), defines the central principal of intelligence as "knowledge of the adversary." Clausewitz stated it this way: "By 'intelligence' we mean every sort of information about the enemy and his country—the basis, in short, of our own plans and operations."[61] Sun Tzu has one of the most famous quotes on what it means to "know the adversary" and is considered by many to be the first "information warrior." Therefore, it is the fate of the intelligence professionals to know and understand the adversary's capabilities, limitations, and intent. That obviously is not an easy task. At some point, practically every intelligence professional must give his or her "best shot" and inform the commander of the adversary's anticipated course of action. General Colin Powell, former Chairman of the Joint Chiefs of Staff, said it best when he stated, "Tell what you know . . . tell what you don't know . . . tell me what you think . . . always distinguish which is which."[62] As discussed further in the following chapters, identifying the adversary in the information age is problematic. Intelligence officers trained to produce doctrinal templates of a Soviet Motorized Rifle Regiment in the attack find it much more difficult to "template" a hacker attempting a computer network attack. In addition, with the target of IO being the adversary decision-maker, the need for much more detailed intelligence profiling and human factors analysis grows exponentially.

As Sun Tzu's dictum reminds us, knowing the adversary is only part of the equation. The second part is knowing oneself, or for whom one works. At times, it may be easier to collect intelligence on the adversary than it is to get the commander's attention and have him or her articulate those desires as concrete requirements.[63] Each commander comes into the position of authority with biases and preconceived notions of what intelligence can and cannot do. Added to that, the skepticism that some senior officers have toward IO makes it extremely difficult to gain a clear indication of the commander's intent and expectations when it comes to producing intelligence that will support IO.

A good intelligence officer must be able to convince the commander that intelligence is more than simply a combat multiplier. Intelligence will help the commander focus combat power, resources, and provide force protection. It also helps a commander identify and determine objectives and plan the conduct of operations.[64] The J-2 Intelligence Officer on a joint or combined staff plays a key role in the deliberate and crisis action planning process by producing the intelligence analysis needed to wargame courses of action and recommend operations to the commander. Having the J-2 officer involved in the planning process early on helps to focus the available intelligence resources on the critical information requirements for a particular operation and identifies intelligence gaps that will need to be reported to supporting agencies.

The Intelligence Cycle

The process by which information becomes intelligence and responds to the commander's requirements is the Intelligence Cycle. Within the joint community, "the intelligence cycle provides the basis for common intelligence terminology, tactics, techniques, and procedures."[65] The intelligence cycle is a conceptual model composed of six phases: planning and directing; collection; processing and exploitation; analysis and production; dissemination and integration;

and evaluation of feedback.

The first phase, *Planning and Directing*, involves the identification of intelligence requirements and available resources. During this step, intelligence annexes are prepared, personnel support identified, and coordination effected between staff sections within the command and other agencies outside the command. The collection manager begins to formulate a collection plan that allows for the coordination of all intelligence assets, both organic ones and those of higher or adjacent units. Intelligence requirements that cannot be satisfied by organic resources must be communicated as requests for information (RFI) to other units or agencies.

The second phase is *Collection*. During this phase, requirements have already been married up with capabilities and actual collection of information is taking place. The intelligence community has a large number of disciplines to tap into when trying to collect information. The following are the seven major and subordinate intelligence disciplines:

- IMINT: imagery intelligence
- SIGINT: signals intelligence
- HUMINT: human intelligence
- MASINT: measurement and signature intelligence
- OSINT: open-source intelligence
- TECHINT: technical intelligence
- CI: counterintelligence[66]

A good collection plan will ensure that there is redundancy built into the process so appropriate cross-targeting of disciplines can occur. In other words, if IMINT identifies what appears to be a new command and control facility, then SIGINT or HUMINT assets could be refocused on that location to confirm or deny the existence of such a structure. The collection plan must also be synchronized with the operation plan so that the intelligence indicators will be there in time to allow the operational commander to make the appropriate adjustments to the plan. For example, identifying a named area of interest like a bridge, and placing collection assets on that point, may help to confirm or deny an adversary's intentions to move its forces through that junction. Those indicators need to be provided in a manner timely enough to allow the commander to react.

The third phase in the cycle is *Processing and Exploitation*, where raw information is converted into a product that can be used by the intelligence analyst. Processing depends on command, control, communications and computers (C4), since that is the transmittal means (links and nodes) that gets the information to the analyst. Collection is only as good as the means to get the information where it needs to go and in a usable format. For example, captured documents or open-source information may need to be translated first before going to an analyst who will evaluate that new information against present holdings.

The fourth phase is *Analysis and Production*, where processed information or "raw intelligence" is turned into usable intelligence products. At the joint commands, this step occurs in the Joint Intelligence Center.[67] Here, analysts having regional or functional production responsibilities (like Korean Order of Battle) fuse all-source intelligence information into an intelligence product that aims at satisfying a commander's Priority Intelligence Requirements (PIR).

Intelligence products can take many forms. They can be bound into hard copy reports, displayed on maps or as images, and/or reproduced electronically. Generally they fall within the

following six categories:

- current intelligence
- indications and warning
- general military
- target intelligence
- scientific and technical
- counterintelligence[68]

The categories respond to the purpose for which the intelligence product was produced. There is often overlap since the data can frequently be used by a number of different consumers with different specific needs.

The fifth phase is *Dissemination and Integration*, in which the final product is transmitted to the customer. DIA Director, RADM Wilson describes this as "the hardest part of the intelligence cycle to get right," since intelligence is of little value if it does not get to the intended recipient, "at the right time, in the right format, at the right amounts, in the right place."[69] Means of transmission can include verbal reports, written documents, video teleconferencing, electronic databases, graphic products, etc. Dissemination can occur through either a "push" system (getting information out to the consumer) or a "pull" system (allowing consumers to access a database and search for the information they need). A valuable dissemination tool that accommodates both the push and pull systems is the Joint Deployable Intelligence Support System (JDISS). Through this system, intelligence users have access to the Joint Worldwide Intelligence Communications System (JWICS), the sensitive compartmented information (SCI) portion of the Defense Information System Network (DISN). JDISS provides a means of dissemination of intelligence products, as well as a means of communication.

Another tool under development to help the timely and accurate dissemination of intelligence products is the Joint Intelligence Virtual Architecture (JIVA). The purpose of JIVA is to create intelligence products that are "modular" or "living" in the sense that they can be updated much more quickly than your typical intelligence reporting procedures. JIVA allows intelligence analysts the ability to insert new information into intelligence products, unit or updating geographic coordinates or personalities. Through a process called collaborative white boarding (CWB), intelligence analysts can store information and reach decisions on intelligence assessments in a much more timely manner, thus improving the responsiveness of the intelligence cycle to the end user's needs. The drawback with JIVA is that it requires "buy-in" by all agencies within the intelligence community who share production responsibilities for certain products.

The final phase is *Evaluation and Feedback*. In the original intelligence cycle model, feedback and evaluation were understood, rather than articulated, because there has always been an evaluation process with HUMINT reporting.[70] Intelligence analysts are routinely asked to respond to collectors who have cited a user's requirements in an intelligence information report, whether the information provided was "of major significance, of value, or not of value."[71] The intent of the evaluation process is to ensure that the collectors are responding to the users' needs and to realign collection efforts when they are not. When they fall short, the system must adjust to correct the deficiency or else the entire discipline suffers.[72]

The Intelligence Community

To further understand how the entire process works, a brief review is needed to focus on the makeup of the Intelligence Community. At the national level is the Director of Central Intelligence (DCI), dual-hatted as the Head of the Central Intelligence Agency. The National Security Act of 1947 tasks the DCI with "directing and conducting all national and foreign intelligence and counterintelligence activities."[73] Intelligence production and collection activities of all 13 of the U.S. intelligence agencies come under the purview of the DCI, including those belonging to the Department of Defense.

The Defense Intelligence Agency (DIA) is the national-level intelligence organization with responsibilities for intelligence production and collection in support of DOD elements. DIA and other national-level intelligence agencies provide a wealth of collection platforms, resources, and capabilities that can be tasked by the DCI to support military operations and is the conduit through which joint commands get their time-sensitive requirements. In addition, the DIA, National Reconnaissance Office (NRO), CIA, and other intelligence agencies work with the Joint Staff J-2 to run the National Military Joint Intelligence Center (NMJIC) in the Pentagon. Liaison officers from these national agencies sit in the NMJIC and respond to time-sensitive requests from the field. They also provide the "reach back" to national HUMINT, IMINT, and SIGINT systems that can be tasked to support operational requirements.

In the early 1990s following the Gulf War, Joint Intelligence Centers (JICs) were established at each combatant command with the intent to "improve the quality of intelligence support to the warfighter while decreasing the resources required to provide such support."[74] By "pushing" more collection and analytical responsibilities to the CINCs, the DOD also created the linkages needed to ensure connectivity to the national-level agencies. In other words, along with the formation of JICs at the combatant CINCs, came liaison officers from the DIA, CIA, and NSA and the necessary Command, Control, Communications, Computers and Intelligence (C4I) linkages to these national-level agencies through the JWICS and the JDISS.

When a CINC needs to form a joint task force (JTF) to support an operational requirement, they can tailor the intelligence support needed to perform the mission. This is accomplished with the formation of a National Intelligence Support Team (NIST) comprised of representatives of the CIA, DIA, NSA, and/or others, tailored to support a JTF commander. An operational element of the JIC, called a Joint Intelligence Support Element (JISE), may also be formed to directly support the JTF. A JISE is usually formed during a crisis and serves under the JTF J-2 to "manage the intelligence collection, production, and dissemination for a joint force," and it may also function in a "split-base" mode, which allows the JTF J-2 to keep the bulk of the intelligence support at the JTF home base, with a smaller footprint within the Joint Operational Area. [75]

In addition to deploying theater-level intelligence resources, a J-2 must also plan for the integration of service and coalition intelligence capabilities and resources. Each service component has a unique array of intelligence collection platforms that must be integrated with the operational collection plan. Coalition capabilities may or may not be available, given the constraints on intelligence sharing and releasability of intelligence methods and sources. The services and coalition partners also bring unique challenges with connectivity and the ability to disseminate intelligence. Standardization of equipment and the use of standard operating procedures will always be problems, yet increased use and availability of JWICS and JDISS are helping to alleviate this situation.

IO and the IPB

In order to respond to the unique needs of IO, the intelligence community has revised its support through the means of conducting intelligence preparation of the battlespace (IPB). This is an analytical process or method used by individual intelligence officers and their staffs as well as intelligence organizations. The ultimate goal of IPB is to reduce uncertainty and allow a commander to focus combat power to counter an adversary's most likely course of action. In other words, done correctly, IPB gives the intelligence officer a level of confidence in his or her assessment beyond "gut instinct."

In the joint community, the joint intelligence preparation of the battlespace is defined as:

> The analytical process used by joint intelligence organizations to produce intelligence assessments, estimates, and other intelligence products in support of the joint force commander's decision making process . . . . The process is used to analyze the air, land, sea, space, weather, electromagnetic and ***information environments***, as well as other dimensions of the battlespace, and to determine an adversary's capabilities to operate in each.[76]

The inclusion of "information environments" in the definition of battlespace indicates how the intelligence community has come to recognize the unique challenges posed by information operations and the unique intelligence requirements needed for conducting IO in peacetime, as well as information warfare in times of conflict.

Joint intelligence preparation of the battlespace is a four step process: (1) defining the total battlespace environment, (2) describing the battlespace's effects, (3) evaluating the adversary, and (4) determining and describing the adversary's potential courses of action, particularly the most likely courses of action, and the courses of action most dangerous to friendly forces and mission accomplishment.[77]

In step one, defining the battlespace environment, a number of planning factors must be considered. For example, what are the operational limits of the joint operational area? What is the joint force commander's mission? What are the unique characteristics and dimensions of the battlespace? What amount of detail is required? What information already exists in databases, etc.? What information requirements exist and what intelligence collection is needed? These types of questions occur early on in the planning and directing phase of the intelligence cycle. What is unique about intelligence support to an IO plan is that these questions and others must be asked far in advance of any operational deployment and do not lend themselves to crisis action planning. Intelligence products, to be timely, accurate, and available for IO planning, often need to be "warehoused" and easily retrievable. Also due to the interagency structure of IO, it may not necessarily be a DOD organization requesting the information.

Step two of the IPB process describes battlespace effects. Traditional considerations such as military aspects of terrain cannot be ignored, nor can the impact of weather, mission, troops available, time, etc. [78] Yet in the information battlespace, other effects must also be considered:

- Media access and availability (foreign and domestic)
- Information systems usage (government, industry, military)
- Internet access (population)
- Critical infrastructures and architecture (power, banking, telecommunications, etc.)
- Public opinion (both domestic and foreign)

- Other actors present and their agendas including nongovernmental organizations

Therefore in an IO environment, practically every facet of an operation (military, diplomatic, etc.) must be considered against the potential impact of all these factors.

In step three, evaluating the adversary, IO seeks to target the adversary decision-maker. Therefore, identifying those who actually make the decisions and their closest advisers is critical. In developing the appropriate human factors analysis of these individuals, other questions need to be asked:

- What is their psychological mindset?
- What are their political goals and strategic objectives?
- What intelligence sources and methods do they employ and trust for their information?
- What are their biases?

These questions cannot be answered overnight, thus requiring long-term collection, in particular a dependence on HUMINT for understanding a decision-maker's intent. A recent development in the IC for this step of the IPB process is the use of Human Factors Analysis centers (HFAC). Many joint operational commands are developing HFACs within their Joint Intelligence Centers (JICs) in order to conduct this detailed level of analysis. Considering that the ultimate target set of IO is the adversary decision-maker, such developments as the HFAC are a welcome addition to the intelligence community.

In the final step of the IPB process, the analyst must determine an adversary's course of action. Here, intelligence officers must take a position and argue their case before the commander on what they believe the adversary will or will not do. In the recent case of North Atlantic Treaty Organization (NATO) military operations in Kosovo, past indicators of Serbian President Milosevic's behavior led to the intelligence assessment that after a couple days of NATO bombing, Milosevic would give in to NATO demands and support the Ramboullet Accords.[79] Since he did not capitulate, NATO planners conducted a "plan as you go" strategy until the conflict ended months later. As will be shown in Chapter 6, IO was not utilized correctly as an enabling strategy in Operation Noble Anvil.

The relationship between Information Operations and the Joint Intelligence Preparation of the Battlespace process is a continuous interaction between the J-2 and J-3 when developing a joint campaign plan or theater engagement plan. It is also evident that intelligence support of IO works best in the deliberate planning process when there is significant lead time before an operation, rather than in a crisis action mode. That's not to say that intelligence cannot support short-fuse contingencies, but when it comes to supporting the unique requirements for conducting IO, the system is not as flexible or responsive as one might wish. JP 3-13 states that offensive IO requires intelligence support that is "broad-based" and "dedicated" with "significant lead time" and "early employment." It also states that "intelligence must be collected, stored, analyzed, and easily retrievable" and that intelligence collection should include "all possible sources."[80]

The entire concept of information superiority depends on intelligence superiority. In order to have a tighter decision loop than the adversary, one needs to know that adversary better than one ever did in the past. Banking on technological improvements in information processing, collection platforms, and the entire reconnaissance, surveillance, and target acquisition process alone can produce vulnerabilities, particularly in the field of human intelligence. If the United States has learned anything from its intelligence failures of the past and the shortsightedness of

its intelligence policy in the 1970s, it is that technical means of intelligence collection alone cannot confirm or deny an adversary's intent. What is needed is a long-term investment in recruiting the appropriate HUMINT sources, to develop the analytical tools required for human factors analysis (adversary decision-makers), and structuring appropriate counterintelligence assets (to counter an adversary's IO efforts, particularly denial and deception operations) so that intelligence will truly provide the support of information operations envisioned in JV2020. Such a response will require increased national-level visibility for conducting IO and greater involvement of the interagency community in defining IO as a strategic priority that commands NCA attention. One means of emphasizing the growing threats to U.S. critical infrastructures posed by cyberterrorists, state-sponsored information warfare, or other information threats is to categorize these in the National Security Strategy as being on a par with other threats, such as those posed by weapons of mass destruction. Only then will the appropriate intelligence sources and requirements be adequately funded and directed to provide the necessary support of information operations.

For IO to be truly functional, not only does it need good intelligence support, but it also must be integrated across not only United States government agencies, but coalition nations as well. As will be noted in the following section, it may be some time before IO reaches its full potential because of these limitations on intelligence sharing among our allies.

The Releaseability Issues of IO

IO is still hampered by many issues, foremost among them the classification and releasability of information to coalition nations. To begin with, the Combatant Commanders (CINCs) conduct most DOD IO planning in an IO cell. These small groups are part of the Operations Directorate and are tasked to ensure that IO issues are integrated into the larger plan. They coordinate with the J-39 from the Joint Staff as well as other IO agencies. Therefore the problem arises with releaseability issues because much of IO planning is still conducted at high classification levels. Normally these plans are at least held at the Secret United States Only No Foreigners (S/NF) level and often rise well above the Top Secret/Sensitive Compartmented Information (TS/SCI) status. There are also Special Access Programs (SAPs) and Special Technical Operations (STO) that, while not exclusively devoted to IO, nevertheless play a significant role.

These high levels of classification for IO limit its appreciation by a wider audience. If you look at some recent operations to see how IO has been conducted, you will notice is that there are very few unclassified lessons learned available. Since most of IO planning is still conducted in classified areas or STO cells and the use of SAPs has been high, there has not been a consensus to declassify much material in the last few years. Of course it also depends on which capability or related activity that you are concerned with as far as its classification level. Much of the electronic warfare, destruction, psychological operations and operations security principles are common enough among the different nations to allow dissemination at a Secret level on these issues. Likewise public affairs and civil affairs are most often conducted at the unclassified level in order to gain the media and private contacts needed to conduct business. However, it is the computer network attack and deception capabilities that have most often been tightly held and have tended to remain the most non-releaseable in reference to foreign disclosure to other nations. Computer attack and defense programs are some of the newest technology and perhaps

the most far-reaching of the IO weapons. Therefore, their use has been highly restricted, not only to other nations, but even within the United States as well.

The basic document that provides guidance on the releasability of intelligence to foreign nations by the United States is the National Disclosure Policy (NDP-1). In addition, other documents such as the NSS, JPs and DCI Directives have all stated in different fashions, their views on foreign disclosure. Most publications, including JV 2020, stress that the United States will operate in a multi-national or coalition environment so it is crucial that intelligence be shared when possible. However the true guidance is laid out in NDP-1. Even DODD S3600.1 published in 1996 refers to NPD-1 for its disclosure policy. For disclosure of United States classified military information, the basic policy is:

- Classified military information will be treated as a national security asset which may be shared with foreign governments and international organizations only when in the interests of the United States
- Foreign governments must protect United States classified military information with a degree of security comparable to that received in the United States
- Disclosures must always be consistent with United States foreign policy objectives
- Disclosures will be made only when it can reasonably be assumed that information would not be used against United States interests

Other factors to consider are which United States agency or command is the originator of the intelligence, this determines who can downgrade or declassify the information. The other major factor is which country is involved. Depending on there being in a bilateral relationship with the United States or if a nation is currently involved in a coalition operation, may determine its access to releasable material. The basic principles for foreign disclosure listed in NDP-1 include:

- Intelligence sharing for common threat perception
- Level of Classification
- Dissemination Architecture

At an unclassified level, that is about all one can say concerning NDP-1 and IO. You cannot disclose what the rules and policies are for disclosure, nor can one go into great detail on what the different agencies in the United States intelligence communities are doing. While there has been some work to downgrade this technology to a lower classification level, at the current time, much of that effort does not go below Secret/No Foreign. Thus the use of information operations and in particular computer network attack in a coalition environment are going to be constrained and are probably going to be rather closely held secrets for the foreseeable future. This will constrain multinational operations and perhaps limit the effectiveness of IO, but that will of course depend on how these technologies are treated in future doctrinal updates.

Yet to make IO truly successful, you must have detailed and integrated planning. You must include as many players as necessary, reaching out beyond the traditional military agencies to the private sector as well as your allies and coalition partners. That takes trust all around, however, as we all realize, that trust will take time to develop and grow. IO is a relatively new warfare area that is still evolving and the releaseability of its capabilities and related activities is an issue that may not be resolved without a lot of effort by all parties concerned. To work successfully, the United States will need to bring its allies into the fold and release more aspects of these classified warfare areas. However the same is true for all coalition partners. To be effective, information must be shared on a timely basis. While there is a concerted effort to

downgrade many aspects of IO, it may not get to a level that will satisfy many allied nations in the near future. The capabilities of portions of IO, primarily CAN, are such that it may be a while before these technologies are released on a more general level by the United States. But that is not to say that in general, the level of interoperability among military forces concerning IO has not risen greatly over the last few years. As military commanders get more familiar with IO and its capabilities, then the interoperability and sharing issues will likely lessen between coalition partners.

Yet there are attempts to increase the information sharing between coalition partners. US Joint Forces Command (JFCOM) is the recognizant authority within the DOD for Joint Task Force (JTF) interoperability and as such they developed a system for secure information exchange. In an attempt to replace the dubious "sneaker" net operations, JFCOM built the Coalition Multi-Level Hexagon Prototype (CHMP). This system is composed of the following six functions that work together to ensure fast information exchange between allied nations in a secure and flexible manner.

- Marking Standards
- Document Marking
- Digital Labels
- Personal Authentication
- Hardware required for CHMP
- Security Management

The real key to this whole system, besides the obvious administrative benefits, was the development of a CHMP Hexcard, to allow for personal authentication. Similar to an ATM card, this system stores an individual's fingerprint, clearance levels, need to know and citizenship. When inserted into the workstations and servers, the Hexcards allow for the proper transfer of data between allied nations. While these attempts may not solve all the problems of information releaseability, at least they are a step in the right direction.

Conclusion

The role of intelligence is crucial to the implementation of IO by the United States. It must be horizontally integrated across the strategic, operational and tactical levels. This will hopefully ensure that the key pieces of intelligence are delivered to the decision-maker in a timely manner. Thus the role of the senior intelligence officer (J2) on a joint staff cannot be overstated. The J2 must understand the needs of the operational community and work hand-in-hand with the J3 to ensure the Commander is properly supported. As one CINC has commented, "IO can't wait" and the J2/J3 must be fully integrated into the concept of operations at all levels of planning and executing IO.

Chapter 3 - Information Protection - The Challenge to Modern Bureaucracies

"The best defense is a good offense."

Anonymous

Military operations have traditionally been categorized as either offensive or defensive in nature. In addition, weapons systems have also been described in this vein such as air defense artillery or interceptor aircraft. Yet, any defensive operation also has an inherently offensive side when it neutralizes the adversary's intent, either through active measures, such as physical destruction or more recently by using a set of passive computer firewalls. Thus the idea that a weapon is totally defensive or that one can truly protect one's self with purely defensive measures is usually not a concept accepted totally by United States military personnel. As a general rule, most military operations have both offensive and defensive components and this is evidenced in the doctrine as well. Joint Information Operations doctrine refers to both offense and defense as the two primary subdivisions.[81] For the purpose of this text, this categorization will be used, however the very nature of IO and its relation to agencies other than the military makes this distinction less critical and probably will prove to be a disservice in the end. The overall trend that the authors see is toward greater integration, or as stated in JP 3-13, "fully integrated offensive and defensive components of Information Operations are essential."[82]

Defensive Information Operations

Defensive IO are concerned with more than just computer-based information systems, yet you might not know that from reading recent publications. There has been a tremendous amount of press on CND and IA, as you learned in Chapter 1, however defensive IO is much more than that. That's because information is critical to all military operations, traveling over a number of mediums including satellites, broadcast media (television and radio), facsimiles, cellular phones, etc. Each of these systems therefore poses its own vulnerabilities that can be exploited by an adversary, and these are not necessarily always computer-based. For example, the television footage of dead United States Army Rangers being dragged through the streets of Mogadishu, Somalia did much more damage to United States political resolve and ultimately impacted warfighting capability more than a few well-placed precision-guided munitions. Likewise today through the use of low-cost commercial or over-the-counter technologies, any adversary can significantly impact the most sophisticated military organization's information processing and decision-making capabilities. Former Secretary of Defense and current Vice President Dick Cheney, once commented that advanced technologies have made third class powers into first class threats.[83]

So what exactly are defensive information operations? The definition found in JP 3-13 describes defensive IO this way:

> The integration and coordination of policies and procedures, operations, personnel, and technology to ***protect and defend*** information and information systems. Defensive information operations are conducted through information assurance, ***OPSEC***, physical security, counter-deception, counter-propaganda, counterintelligence, electronic warfare, 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.[84]

Interestingly, the only change in this definition that differed from the preliminary draft of JP 3-13 are the bolded phrases above. Are these significant? Adding OPSEC, hardly – probably an oversight. But, adding "protect and defend" implies more active, rather than passive measures. To provide an illustration, when one installs an intrusion detection system on one's home, they are employing passive protection measures. When the same individual keeps a loaded 9mm pistol in their nightstand drawer, they are employing a more active defensive measure to protect their family and property. Such an analogy is applicable to information operations, where the DOD employs more active defensive measures to protect information systems, rather than relying simply on intrusion detection systems.[85]

Within the discipline of defensive information operations, there are two main goals:

- To minimize friendly IO system vulnerabilities to adversary efforts
- To minimize friendly mutual interference during the operational employment of IO elements and capabilities

Quite simply, the second part of the equation is that one needs to protect oneself from oneself. Information fratricide is a very real concern on the information battlespace. Deconflicting the use of the electromagnetic spectrum becomes even more complex and necessary as available bandwidth decreases.

Joint Pub 3-13 describes the Defensive Information Operations as a process. Initially proposed by the Joint Staff J6K as the Defensive IO Model, it has been incorporated into the doctrine by J-39 for the conduct of IO. The diagram contains four embedded processes. The first is to *protect* one's Protected Information Environment. The process involves identifying which information systems are the most critical to an organization and determining the appropriate policies, procedures, technologies, and operations necessary to safeguard these critical systems. A critical part of the protect process involves IA, which is discussed later in this chapter. This process seeks to ensure that the information getting into one's system is just as valid as the information that is going out.

The second process identified in the diagram is *detect*. In other words, how does one know their organization is under an information attack? Many DOD elements are working to develop a system of indications and warnings specifically designed to detect if and when an information attack may occur. What makes this process so difficult is the need for a fully integrated indications and warnings capability across the spectrum of IO, which involves agencies other than just the DOD. As was explained in Chapter 1, a fully integrated National Infrastructure Protection Plan is crucial for linking DOD with other federal agencies, as well as industry in order to ensure the appropriate level of intelligence and warning sharing occurs in a timely matter.

The third process is *restore*. The key in any cyber attack is to maintain transparency of operations and not let on that the intruder is having an impact on the operations of one's organization. In addition, it is also very important to ensure redundancy in the restoration process, namely ensuring there are appropriate back-ups and routing capabilities to reduce the impact of an intrusion. Here again, cooperation between the government, society, and industry is crucial for ensuring continuity of operations and reducing vulnerabilities. A good example is a fully integrated system of CERTs that can share timely information on intrusions and sources of the attacks is crucial for ensuring continuity of operations in any environment.

The final step in the defensive information operations process is *respond*. The linkage back to the other processes is necessary in order to determine the nature of the attack: its severity, sponsorship, etc. and further to identify the actors and their intent. The response DOD takes will ultimately hinge on these criteria, as well as whether the attack has domestic or international implications. Depending on the source and the intent, the DOD may not be involved in responding to an attack, particularly if there are domestic law-enforcement equities at stake. If the military is involved in responding to an information attack, there will likely be very restrictive rules of engagement enforced and the traditional military reaction (steel on target, or overwhelming forces) may not be the most appropriate reaction.

Currently United States military commands are implementing a series of defensive IO measures aimed at increasing their knowledge of and response to information attacks. Exercises such as Eligible Receiver and Warrior Flag, seek to educate and train commands about the dangers of information system vulnerabilities and help them develop the appropriate safeguards and response mechanisms. In March 1999, the Chairman of the Joint Chiefs of Staff published a directive on prescribed Information Conditions (INFOCONs) in order to standardize the reporting and declaring procedures for these conditions. These new directives have quickly been assimilated into the military structure and are now considered a standard part of any base infrastructure. As mentioned in Chapter 1, the JTF-CNO and USSPACECOM, have the responsibility for promulgating changes to these procedures on a daily basis.

These procedures mentioned here, and some of the technologies alluded to earlier, are good steps in building a defensive posture, but the most important component of any plan is people. No amount of high-tech intrusion detection devices or command-directed policy can overcome the effectiveness of unit personnel who take active interest and role in the defense of their command. Yet all too often, leadership is too enamored with new protection devices or software, when instead their money would be better spent on adequately training their people. As we have tried to emphasize throughout this book, IO is much more than just computers.

In summary, defensive information operations include a range of capabilities aimed at reducing vulnerabilities to information and information systems. The weak link in all these procedures as mentioned earlier is the personnel, primarily systems operators. The largest threat today comes from the trusted insider; however, just as significant a threat also comes from the individual who is untrained, unprepared, and uneducated in operating very technical components of a command's information system. By oversight or error, serious damage can occur by even the most well-intentioned individuals, crippling a military organization's "eyes and ears." In an age when information is an element of national power and decision loops need to become tighter, an educated and technologically sophisticated military workforce is more crucial than ever.

Information Assurance and Computer Network Defense

As we stated in the first chapter, it is the application of new technology that has revolutionized warfare by taking the elements of power and dispersing them to the people. The computer has been the primary driver of this huge change and while the authors will continue to state that IO is more than just computers, that is the area precisely where a great deal of current emphasis on funding and research are currently being conducted. So it is only natural with a growing awareness among government and military officials to the vulnerability of their networks and information systems, that more money and more emphasis would be placed on IA

and CND. Fortunately for these officials, the development of new doctrine has facilitated this emphasis on defense. In 1996, the JCS released a White Paper that formulated the direction and future strategy of United States military forces. Entitled Joint Vision 2010 (JV 2010), this policy document had many features, but one key area was its dependence on Information Superiority (IS). It was considered crucial to future military operations that the United States achieve IS, which was further subdivided into three areas. IO is therefore a subset of IS, which in turn is a subset of JV 2010. Remember that relationship, because it will change in the future as this policy matures.

As mentioned earlier, IO does not address either IA or CND directly, but within the military community, they have been incorporated under the greater IO umbrella. Some of that philosophy may go back to the old C2W doctine in which you had offensive and defensive components. Whatever the case, you can draw a direct connection between IA and JV 2010. Information Assurance is an umbrella term which covers many portions of the Information Protection construct or the Defensive IO area including CND.

Armed forces are increasingly relying on critical digital electronic information and communications capabilities to store, process, and move and visualize essential data in planning, directing, coordinating, and executing military operations. The implementation of the complex, massive Global Information Grid (GIG) through implementation of combat digitization and network centric warfare concepts using advanced communications and computer technologies means that warfighters are becoming so technologically dependent that system failure or disruption can completely change the tempo of the battle.

In this broad threat environment, where every connection to a network must be regarded as a potential avenue of attack, IO must defend not only our own information and information systems, but also affect adversary information and information systems to deny their capability to be utilized against us. Mentioned briefly before, this is done primarily through IA which is a major subset of IO. Information Assurance supports the full-dimensional protection aspect of JV 2010/2020 and comprises actions at the tactical, operational, and strategic levels that protect and defend information and information systems by ensuring *availability, integrity, authentication, confidentiality*, and *non-repudiation*. It also includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.[86]

To do this, IA seeks to insure the security of information in its myriad of forms, not just information transferred using telecommunications or stored computers. Thus there is a close, synergistic relationship between counterintelligence, operations security, communications security, information security and information systems security, all of which seek to protect information from hostile access and exploitation. This concept is much more expansive in scope than classic information systems security which many people normally tend to relate to. IA is also much broader than CND, which has gotten a great deal of attention recently. It encompasses those communications and computer network management functions that seek to provide for continued operations in the event of accident, natural disaster, deliberate act, and adverse operational environment.

The concept of IA also covers what was previously referred to as peacetime defensive IW and facilitates operational coordination with agencies outside of the DOD, including the civil agencies of the federal government, industry and the public sector. It should not be confused with defensive IO, which is a more of an active/reactive process that addresses the manifestation

of specific threats. The defensive IO process is cyclic and underpinned by the use of risk management as shown earlier. This change in terminology also addressed difficulties for those non-DOD agencies for which the idea of being involved in *warfare* has caused political difficulties through preconceptions of conflict. Thus the adoption of the term IA has also reflected wider recognition that issues such as CIP is much larger than the DOD and that successful IO, particularly IA, relies on a whole of government and community conducting an integrated approach and cooperation of military, intelligence, government, industry and public efforts. However, with respect to military operations, IA is a critical operational readiness and warfighting issue that commanders need to be cognizant of at all times and in particular factor into their battlespace appreciation when going into combat.

This holistic approach to IO protection taken by IA is good, because since the demise of the Cold War, the threats to the United States have changed. Threats come from a variety of sources including natural physical elements and forces that have been influenced or used through human intervention, accidental or unstructured activities through to hostile, structured deliberate misuse or attack. However, recent reports indicate threats from internal sources have not significantly diminished from previous years and the figures from the FBI/Computer Security Institute survey of 1998 are still valid. Organizations surveyed indicated 89% of their perceived threat is still internal.[87] This emphasis on protecting the computer systems and information resident is primarily covered in the discipline of Computer Network Defense. CND refers to those operational IA and defensive IO measures implemented in the computer network environment to defeat both internal and external threats. It takes IA out of the administrative sphere and places it in the operations community with the other elements of IO. Very recently, during the year 2000, there has been a move to combine CNA and CND into an operational discipline known as Computer Network Operations (CNO), but that is still undergoing analysis.

This emphasis on CNA has produced a tremendous amount of interest in the vulnerability of the United States and its military forces. In effort to validate anecdotal evidence of the possible impact of CNA on military operations and the NII, the JCS sponsored a series of exercises known as *Eligible Receiver* as mentioned in Chapter 1. The most famous of these was mentioned earlier and was called *ER '97*, which demonstrated in June 1997 that hostile forces could penetrate national infrastructures and DOD networks using CNA and other techniques to adversely affect the government's ability to conduct military operations. A number of non-DOD agencies were also involved including the FBI, DOJ, Department of Transportation, DOS, CIA, NRO and the NSC. The threat consisted of a NSA Red Team replicating the threat from a domestically situated but State sponsored team operating on behalf of a nation that had refused direct military confrontation with the United States. This nation concluded that the United States was now so militarily and economically dependent on vulnerable information systems that a non-attributable CNA operation offered a viable option. The aim of these attacks was to alter United States policy and delay or deny their ability to respond militarily to avoid detection and arrest.

The Red Team, using only open source intelligence and hacker tools available on the Internet, was able to fully demonstrate the vulnerability of DOD and national-level system and network vulnerabilities. The rules of engagement allowed the team to conduct actual attacks on DOD systems and conduct simulated attacks on NII systems. Lessons learned from *ER ' 97* emphasized the need for effective vulnerability assessments, network indications and warning, appropriate command and control, a designated cyber-defense command, consequence

management, interdepartmental/interagency planning, procedures, and processes. Probably the most important lesson learned from *ER '97* was the need for a central DOD agency to be in charge. As mentioned earlier, DISA is normally responsible for protecting the NII, however in reality, since they are a combat support agency, DISA cannot order a CINC or government agency to change any policies. It took over 18 months to solve this problem with the formation of the JTF-CND.

In February and March of 1998, the United States military, government and research and development sites experienced a large number of systematic intrusions that were determined to be related to one another. Code-named *Solar Sunrise*, the timing of these activities was very suspicious since it coincided with another build-up of United States military personnel in the Middle East in response to tensions with Iraq over United Nations weapons inspections. The intruders penetrated many unclassified U.S. military computer systems, including Air Force bases and Navy installations, DOE National Laboratories, NASA sites, and university sites. The timing of the intrusions, and the apparent origination of some activity from the Middle East, led many government officials to suspect that this could be an instance of Iraqi CNA aimed at disrupting the U.S. military build up in the region.

Subsequent investigation and detailed research by the NIPC and the FBI, working closely with Israeli law enforcement authorities, determined that after several days that two juveniles in Cloverdale, California, and an individual with several accomplices in Israel were the perpetrators. Once again, the need for a central government agency to coordinate an appropriate response was needed, but not available yet. *Solar Sunrise* showed the need for DOD to constantly coordinate with law enforcement agencies, especially the FBI, when dealing with unidentified computer intruders.

If *Eligible Receiver 97* and *Solar Sunrise* were eye opening operations to the vulnerability of the United States systems, then the next series of incidents code-named *Moonlight Maze* was the true wake-up call. Dr. John Hamre, the Deputy Secretary of Defense at that time, described the *Moonlight Maze* events to a congressional committee in 1999 stating bluntly: "We are in the middle of a cyber war." The *Moonlight Maze* operation was enormous and officials have publicly stated that the intruders systematically accessed and exploited hundreds of unclassified but sensitive computer networks used by the DOD, DOE, NASA, various defense contractors and several universities. A large amount of technical data related to defense research was copied and transferred to Russia. One defense technician trying to track the computer intruder is said to have watched in amazement as a document from a naval facility was "hijacked" from a print queue to a location in Moscow right in front of him. The first *Moonlight Maze* attack was detected in March 1998. Three months later, United States agencies were able to monitor a series of intrusions as they occurred and traced them back to seven dial-up Internet connections located near Moscow. The FBI is still attempting to determine if the United States was subject to intelligence collection over the Internet conducted by Moscow's prestigious Russian Academy of Sciences in *Moonlight Maze*, which so far has been the most insidious and focused assault yet on sensitive DOD and government computer networks. Intense attacks continued until at least May 1999 and the FBI investigation remains open. Yet Russia may just be the last line in a long series of transactions of a very determined data mining effort. Therefore caution is required with respect to attributing *Moonlight Maze* to the Russian Government, however, as there has been no definitive evidence of a military or intelligence connection. "It could turn out to be Russian

organized crime," stated one source that also indicated, "… and they could be acting as a front for the intelligence community."[88]

Computer attacks can also be conducted in the form of a virus. A virus is a program or software code that is designed to replicate and spread itself within a network or server. Generally this done without the operator's knowledge and in many cases can severely compromise the machine's ability to operate. Prudent system administrators insist on installing and updating the latest anti-virus software such as those programs sold by Symantec, McAfee or IBM. The Melissa virus was for many average citizens, the wakeup call for computer security. On 26 March 1999, this new virus first appeared and by the 30th, four days later, it had successfully infected over 70,000 e-mails. This was the first virus to prompt a warning to be issued by the FBI, and for many Americans, it was their first exposure to the dangers of a virus. While the majority of viruses are file viruses, the Melissa version was different. File viruses infect other files by attaching themselves as an executable file, with a .exe or .com extension, indicating executable program code. These are exactly the kind of files that a firewall looks for and tries to exclude from a network. Likewise the other common virus is a Boot Sector or Partition Table virus that are normally hidden until an operator executes the boot-up process.

Melissa was different however. Melissa was a macro virus, which means that its infectious code is part of a macro, in this case a Microsoft Word macro. Therefore it was able to bypass most firewall and virus scanning programs because it was not a .exe or .com file. Once the Melissa virus was resident inside an operator's computer, it proved especially deadly. Since it moved as an e-mail, once opened by the unsuspecting operator, the macro quickly read the first 50 names from the Microsoft Outlook address book and then forwarded itself on to them as another e-mail with an attachment. By spreading so quickly, the Melissa virus overloaded the server and eventually crashed a number of them in a classic denial of service attack.

However what was also different about the Melissa virus was that lessons had been learned over the last 18 months in the wake of *ER '97*, and so some new organizations were in place to effectively combat the virus. As was emphasized already, both the JTF-CND and NIPC were stood up and were able to quickly assess the threat, develop a defensive strategy and the to coordinate a whole host of defensive actions. For the first time in DOD and government history, someone could answer when asked who was in charge of network defense.

Solar Sunrise and *Moonlight Maze* and to an extent the Melissa virus also validated and reinforced the findings of *ER '97* by clearly demonstrating the need for a cooperative approach by Federal and DOD organizations to nationally manage the defensive IO battle. Possibly the most important lesson learned from *ER '97*, *Solar Sunrise* and *Moonlight Maze* has been the requirement for an effective and efficient incident and vulnerability reporting system. Comprehensive incident reporting is critical to determine whether an intrusion is local and isolated or part of a more, widespread activity. This reporting system must accept data from both automated systems such as intrusion detection system and firewall logs as well as manual incident reports based on personal observation and analysis of users and system administrators. Streamlining the incident reporting and analysis process requires standardization of reporting formats, handling procedures, data transfer and maintenance procedures and integration with response capabilities at all levels.

To meet these requirements the DOD implemented a new four tier incident and vulnerability reporting structure with reporting and analysis at Global, Regional, Service and

Local levels. All local military Network Operations and Security Centers (NOSCs), whether deployed or at standing bases, camps, posts, and stations, report upward through either or both of the two functional/command chains, one from a network perspective, the other from an operational perspective. Thus the process of reporting through DISA Regional NOSCs, many of which are collocated with warfighting CINCs, is consistent with the traditional network management processes for reporting network problems. From a command and operational impact perspective, reporting is conducted through individual Service or Regional CERTs, and reflects more traditional operational reporting. Both of these levels report to the DISA GNOSC and the co-located JTF-CNO. So if nothing else has been learned from these three major computer attacks has been the need for a centralized reporting and dissemination system.

In addition, another major lesson learned during *ER '97, Solar Sunrise* and *Moonlight Maze* was that in order to defend DOD computer networks properly, a commander was needed. Therefore to answer the deficiencies from these CNA incidents, the JTF-CND was formed on 30 December 1998, to provide a single command with operational authority to coordinate and direct the defense of the DOD computer systems and networks. There was now a command that could direct CINCs and service units to operationally change settings and set INFOCONs to protect against the threat. Originally reporting directly to the Secretary of Defense, JTF-CND has since become a command that reports directly to the USSPACECOM as of 01 October 1999, when that CINC officially took over the mission of computer network defense for the whole of the DOD. As mentioned earlier, one year later on 01 October 2000, USSPACECOM also assumed responsibility for the complementary offensive CNA role as well.[89]

A further development in the incident handling process that was also mentioned earlier is the development of INFOCONs, that support the threat warning of computer network based activities. This system provides a structured, coordinated approach consistent with Defense Threat Conditions (DEFCONs), with graduated responses to defend against CNA. INFOCON measures obviously focus on implementation of computer network-based protective measures to meet a changing threat level. Each level reflects a defensive posture based on the risk of military operational impact through the disruption of friendly communications and information systems. Countermeasures at each level include preventive actions such as changing passwords, actions taken during an attack such as enabling all system logging, and damage control/mitigating actions such as physical disconnection from the network. INFOCON levels are:

- NORMAL (normal activity)
- ALPHA (increased risk of attack)
- BRAVO (specific risk of attack)
- CHARLIE (limited attack)
- DELTA (general attack).[90]

These are descending order of increasing defensive protection, and once set, all commands must abide by the restrictions delineated in the Chairman's Memorandum CM-510-99 mentioned previously.

While to date the INFOCON system has received a lot of publicity, there are still some concerns that it may not be addressing all of the needs of the commands in the IA arena . Therefore in June 2000, USSPACECOM hosted a conference in Colorado Springs to look at revising the original document. From these meeting came a plan to concentrate on the following areas:

- Commander's Assessment Criteria
- Directed Actions
- Operational Reporting

Since that time, revisions have been made to the basic document, and these were implemented during fiscal year 2001.

As mentioned earlier, prior to the formation of the JTF-CNO, no single DOD entity had the authority to coordinate and direct a department wide response to a network attack. Together with the multi-agency NIPC, the JTF-CNO now forms a strong collaborative team for dealing with attacks on DOD systems/networks and the wider NII. At the global level, the GNOSC reports to and coordinates with the NSA NSOC/IPC and NIPC. The JTF-CNO liaisons with the Joint Staff and the National Military Command Center providing the operational analysis and recommendations to the CJCS. [91]

The other major changes conducted over the last three years has also been of the addition the IA Vulnerability Alert (IAVA) process and vulnerability assessments that give the information protection managers more tools to make decisions to better assess the information threat. IAVA is the comprehensive distribution process for notifying appropriate agencies about system vulnerability alerts and work around/countermeasures information. It has developed into an extremely formal process that requires acknowledgment of the receipt of the vulnerability alert by the different commands to the reporting authority. The system also has time requirements that require specific response from the recipient of the alert that they have implemented appropriate countermeasures. Network vulnerability assessments, sometimes referred to as *On-Line Surveys* or vulnerability assessments, use technical scanning software as an active method of validating the installation and configuration of whether Global Information Grid (GIG) information systems meet appropriate requirements. In addition, another major growth area is the use of IA Red Teams to conduct active vulnerability assessments of networks replicating the threat posed by computer intruders. All of the United States military service Information Warfare Centers maintain these capabilities that have been employed mainly under exercise conditions. Red Teams provide the ability to validate not only the configuration of the systems, but also test procedures and systems user's/administrator's ability to detect and react to CNA, something that an on-line survey cannot do.

All of the measures listed above are part of an overall United States government defensive strategy called Defense in Depth (DiD). This approach integrates the capabilities of people, operations, and technology to achieve strong, effective, multi-layer, and multi-dimensional protection. DiD attempts to ensure that the level of protection of one system is not undermined by vulnerabilities of other interconnected systems ascribing a minimum standard of assurance that all systems connecting to the environment must attain. The idea is that the successive layers of defense will cause an adversary who penetrates or breaks down a barrier to promptly encounter another DiD barrier, and another, thereby increasing the likelihood of detection and offering the opportunity for one of the defensive mechanisms to defeat the attack. To be effective, the DiD strategy must protect against a variety of attack methods. To do this, a corresponding variety of complementary defensive mechanisms must be employed so that the weaknesses of one barrier are offset by the strengths of another.

The three key components of a comprehensive DiD strategy are people, technology, and operations. Appropriately trained and certified people, operating in accordance with well-defined

policies and procedures, using certified and accredited networks and systems with layered and distributed security technologies, are the key to DiD. Security background investigations, clearances, credentials and badges for critical network personnel are required given the internal threat. On 14 July 2000, the Deputy Secretary of Defense issued a memorandum on the implementation of the recommendations of the IA and IT integrated process team on training, certification and personnel management in the DOD.[92] This memorandum provided a framework for training and certification of IA personnel and directed the Service Chiefs, CINCs and DOD agencies to address retention issues given the increasing "brain drain" from DOD to private industry.

For the technical portion of DiD strategy, a number of policies and instructions have been promulgated recently. Ensuring systems components are certified and accredited in accordance with DOD Instruction 5200.40, the "Defense Information Technology Certification and Accreditation Process (DITSCAP)" throughout the system's life cycle is another critical procedural aspect of the DiD process.[93] As with any other military activity, policy drives IA operations by establishing goals, actions, procedures, and standards. The ASD/C3I issued two new Departmental policies with respect to IA, specifically IA 6-8510 *Guidance and Policy for Department of Defense Global Information Grid Information Assurance* and IA 6-8510 *Global Information Grid Information Assurance Implementation Guidance.* These documents detail the implementation of DiD and require development of three types of doctrinal policy.

To assist in the development of effective cyber-defense, the DOD must utilize technology, tools and products that have been evaluated under programs conducted by the members of the National Information Assurance Partnership (NIAP) framework. NIAP was established by a 1997 agreement between the Commerce Departments NIST and the NSA. All of these organizations were covered in chapter one and what we are trying to emphasize is that where possible all DOD systems should use NIAP assured products and services giving a level of trust in the hardware and software being utilized.

The third portion of the DiD strategy is operations, which contain many different programs. The Defense Wide Information Assurance Program (DIAP), as mentioned in Chapter 1, is a management process and structure established to centralize IA efforts within DOD. The program was designed to integrate and coordinate DOD IA activities to:

- Provide a structure to monitor and coordinate IA readiness
- Establish IA responsibilities and authorities across the department

The DIAP is the chief mechanism allowing the DOD Chief Information Officer to ensure IA information technology and resources are effectively managed and implemented to meet DOD operational requirements.

That the DOD has adopted Defense in Depth, as outlined by the JCS J6 Directorate, is a time-honored tactic to combat not only the malicious threat but the accidents and acts of nature as well. The basic idea is that you construct a series of defensive layers to protect your networks and systems against attack. Using a medieval castle as an analogy, J6 and in particular J6K have outlined a comprehensive series of protective layers that must be defended.

- Network and Infrastructure
- Enclave Boundary
- Computing Environment
- Supporting Infrastructures

All of this is spelled out in the DOD Guidance and Policy for Information Assurance. Together with this policy, the JCS has also been working closely with the OSD staff, in particular the DIAP to develop and procure equipment to protect each one of these layers.

Defense in Depth relies on this layered approach to ensure that there is not just one critical node that can be defeated. To do this, advances in technology have helped the manager and system administrator build protection into their networks. Some examples of these new trends include:

- High-Speed Networking (ATM/100 Mbps Ethernet)
- Wireless Technology
- DNS Security

Notwithstanding the need for advanced technology to help network security, there are already products on the market that can help a company, command or agency raise its network standards. These include:

- Public Key Infrastructure (PKI)
- Virtual Private Network (VPN)
- Firewalls
- Intrusion Detection Systems (IDS)
- Virus Scanners
- Smart Cards
- Secure Applications

PKI is a large part of the Federal strategy for providing security throughout the government. Based on the distribution and control of public and private keys, PKI will have three layers of assurance. The DOD has implemented a high-level PKI system called FORTEZZA that will operate in a similar manner. No matter what the particular PKI system is called, they all operate in generally the same manner. Corporations that have leading in this field include Cisco, Verisign, Axent and Entrust Technologies. All four companies have been developing PKI infrastructure and technology models to support the tracking of PKI certificates.

VPN is an attempt to secure the consumer with secure communications and data protection while still allowing access to limited-public network access. To date there are three types of VPN products loosely based in the following categories:

- Hardware-based Systems
- Integrated Systems
- Software-based Systems

Firewalls are a mechanism to deny or allow access to a particular network. They are great devices for limiting access to many harmful virus's but as was shown by the Melissa virus in 1999, they have their limits. Because many of the older versions were looking primarily for executable or .exe files, this particular virus slipped by many firewalls because it was a Word Macro. The generation of firewalls currently being developed include the stateful multi-layer inspection (SMLI) and SOCKS protocol. Offered by companies such as IBM, DEC and CyberGuard, these third-generation applications offer good protection against the current level of threat to a network. Basically SMLI works by analyzing the entire data stream, at all levels, and if an application comes with significant overhead, SMLI will examine each packet and compare to a data base. SOCKS on the other hand inspects both incoming and outgoing traffic at the session layer, applying security on packet-by-packet basis.

IDS are a natural complement to firewalls. While the latter attempts to filter malicious and subversive activity, IDS's monitor and try to detect attempts to subvert security measures already in place. Basically think of the firewall as a locked door that keeps unwanted visitors out and the IDS as your security guard who watches for suspicious activity. As mentioned earlier, IDS's monitor not only outside threats, but more importantly they also monitor the insider as well. In today's environment, the greatest threat to a network is not from the teenage hacker but instead from the disgruntled employee. At the present time, IDSs can be broken down into two categories: host and networked-based. The former normally protects one workstation or server while the latter are designed to work outside the perimeter firewall and record all activities of a particular network.

Access is a huge issue with respect to computer security and IA. However the days of just using a password to protect your system are long gone. There are many reasons why passwords don't work, but to the greatest weakness is that it is humans that use them. Since a password is something we must remember, many operators use a password that can be easily guessed, say their birthday or child's name. Others make the mistake of using the same password on all their accounts, rendering them vulnerable. Likewise many try to write down their password on a yellow sticky and then leave it where anyone can see it. For those reasons and more, many systems and networks are going to biometrics to identify a person, vice a password.

Biometrics is the science of measuring the human body and believe it or not, there are many different parts of your body that are unique and can be measured to identify you and only you from someone else. Listed below are a few of the current biometric processes. There are a number of methods for conducting biometrics with respect to identifying a single operator. Many companies are producing systems or kits that you can use and these are all listed in the appendix. In addition, the Biometrics Consortium is trying to develop standards for biometrics in this rapidly expanding field.[94]

Smart Cards are another attempt to use technology to prevent unauthorized use. Based on the PKI and FORTEZZA-based systems mentioned earlier, smart cards allow access, while still meeting authentication, confidentiality and integrity requirements of IA. These cards have embedded microchips that support different operating systems and various secret key encryption algorithms. They also support PKI infrastructures as mentioned earlier. Many analysts believe that smart card technology will be on the rise in the future. Current smart card use is estimated to be 100 billion transactions a year with much more growth projected for the future.

Secure Applications are a fact of life in this interagency joint world. In order to communicate and conduct business, computers must have the ability to trust the security of the applications that they utilize whether they are system or network based. Some common secure applications include:

- Common Operating Environment (COE)
- Secure Web
- E-Mail Encryptors
- Media Encryptors
- Secure Shell

An Intrusion Detection System (IDS) is like a burglar alarm. Combined with the firewall technology mentioned earlier, IDSs can greatly aid a company or government organization's attempts to protect their resources. By monitoring the network and notifying the system

administrator of abnormal occurrences, IDSs can go a long way in tracking and identifying computer attacks.

Security on the internet is just as important, maybe even more so than in a traditional business or government activity. If a crime is committed in a store, the owner may know about it because a window or door is broken and money or expensive merchandise is missing. Computer crime can be much more insidious. In many cases, it is easier to access the system, and unless a savvy technician is looking, the crime may actually go undetected. Incidents like these can result in huge financial losses and breaches of confidence in their overall integrity of a corporation. Therefore most companies have opted over the last few years to drastically increase their security posture with respect to their computer networks and have installed some sort of IDS system. While firewalls have been around for a number of years, the market for intrusion detection products is growing rapidly. One analyst predicted revenues of over $460 million by the year 2006.

However IDS tools face a very challenging task. These devices are attempting to identify unauthorized use, both internally and externally in real time. This is extremely hard and it is not made easier considering the fact that their adversary is normally a very intelligent hacker on the other side. In addition, with the increased proliferation of networks, protocols, internet access and applications, it is in fact easier for outsiders to gain entrance to a particular corporation's system. While a standalone computer offers the greatest protection, by being air-gapped, this system might also have the least utility to a company. Instead many business's are understanding that with the changing realities of the information world, that to succeed they must be and stay connected to the world wide web. Therefore most companies have opted for an increased security posture to include IDSs.

So therefore many corporations are building a defense in depth series of protections for their networks. They will combine physical security with one or a series of firewalls to prevent entry onto their network. These firewalls may also be checking for virus's and other malicious computer programs. Finally an IDS is used to monitor the network's activity. They do this by automatically poring through huge volumes raw data to look for suspicious activity. They can give the system administrators a better "feel" for what is good and bad within the traffic, as well as alerting them to negative trends. The use of IDS tools to identify false positives may in fact be just as important as identifying actual intrusions. By monitoring network traffic, these products develop audit trails that are very useful to system administrators to give them the knowledge they need to do their job.

The Automated Intrusion Detection Environment (AIDE) is an attempt to build an architecture of a number of IA sensors to reduce the number of false intrusion reports. Typically in a CERT, operators must wade through hundreds, if not thousands of "incidents" per day to look for the real "threat" to the system. What AIDE is attempting to do is to vastly decrease that number of false reports that currently exist to make the system administrator's job all that much easier. The concept behind AIDE is to incorporate existing sensors and devices that already exist at a CERT or NOSC. These different IDSs, Firewalls, virus checkers and network management tools all send their data to the AIDE which incorporates a data bridge as an interface layer. From there, the information is filtered and correlated, before a display is used to look for similarities (ie false positives) that can be weeded out of the system. AIDE relies heavily on mutual and comprehensive reporting between the local, regional and global security centers. This

hierarchical structure is crucial to ensuring secure networks throughout the chain of command.

A View of Defensive Information Operations

The threat to information structures is wide and asymmetric, therefore the need for appropriate IA has never been greater. Insiders are still the greatest threat despite the increasing level of threat from external sources requiring appropriate physical and personnel security and counter-intelligence measures. As noted earlier and hopefully appropiately, IA is not composed of magic black box solutions but an integrated suite of capabilities encompassing people, training, technology and policies.

> *"[T] he amorphous nature of today's security environment means the threats will be far more difficult to anticipate and counter. These asymmetric threats pose end games that are still potentially devastating to countries and alliances. We must, individually and collectively, anticipate these types of threats and have the courage to deal with them."* [95]

To conclude, JV2010/2020 is vulnerable without supporting IA and the computer network threat to civilian infrastructure supporting operations must be considered and adequately planned for. JV 2010/2020 will not be protected by any single organization, plan or policy and the distribution of stakeholders and resource owners should convince any skeptic that the task is broad and needs to be coordinated at the organization, national and international levels. Commanders must accept that everyone has a stake in IA and that the capabilities required to effectively protect United States and Allied information infrastructure will only be achieved through the cooperative, collaborative efforts across the domain of critical infrastructure supporting military operations.

Counter-Terrorism Information Operations

During the Cold War between the United States and the Soviet Union, American policy centered on the possibility of a nuclear attack. This threat was well known and efforts were conducted to prevent it at any costs. However since the collapse of the bipolar world power paradigm in 1991, predictability has broken down and the United States is now engaged in crisis engagement around the world. Often these set the American military forces against the "rogue of the month" instead of a single force or even an ideology. Hollywood portrays terrorists in many forms with various causes, from the recent James Bond film, *The World is Not Enough* where petroleum distribution was paramount, to *Air Force One* where the freedom of foreign political prisoners was the terrorists' cause.[1] These films may be fictional in story line, but these threats and others like them are all too real to United States national security.

This new reality became shockingly close to Americans when visions of terrorist acts were flashed across millions of television sets as office workers climbed their way out of the World Trade Center rumble in February 1993. A little over two years later, the scene was replayed when terrorism struck the nation's heartland on the morning of 19 April 1995 at the Alfred P. Murrah Federal Building in Oklahoma City. These incidents have greatly raised the awareness of terrorism within the United States. In this section, the authors will explain current anti-terrorism and Counter-Terrorism Information Operations (CTIO). In addition, the culture of counter-terrorism will be analyzed to provide a foundation to better understand the reason why governments respond to terrorism in the manner that they do. Finally, the importance of PDD-62

is discussed to demonstrate the changing use of information operations management.

Yet through these incidents did a lot to heighten the awareness of terrorism, nothing changed the American attitude more than the attacks of 11 September 2001. The effects of those four airplane crashes and the loss of over 6,000 lives have forever altered the concept that the United States has about CTIO, and although the outcome of the retaliation operations were not known when this book went to print, it is an understatement to say that America will never be the same after that day. In addition, as mentioned in Chapter 1, although President Bush has declared intentions to build a new cabinet agency (NHSA), no more details were available in late September 2001, as to what exactly the mission and organizational structure would be. Therefore, this section on terrorism and CTIO will mainly address the situation as it was known prior to the attacks on the World Trade Center and the Pentagon.

What is Terrorism?

According to Bruce Hoffman in his latest work *Inside Terrorism*, "Like 'Internet'- another grossly overused term that has similarly become an indispensable part of the argot of the late twentieth century - most people have a vague idea or impression of what terrorism is, but lack a more precise, concrete and truly explanatory definition."[96] As Walter Laqueur writes, "No definition of terrorism can possibly cover all the varieties of terrorism that have appeared throughout history."[97] Thus, the interpretation of the classification of terrorism is most important in the development of a definition of terrorism.

Although some scholars have cited up to 109 different definitions of terrorism, the FBI currently uses the following definition, "the unlawful use of force or violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives."[98] The FBI also classifies acts of terrorism as either domestic or international, depending on the origin, base, and objectives of the terrorist organization.[99] For the purposes of this book, the following sub-definitions are also used:

- Domestic terrorism: the unlawful use, or threatened use, of force or violence by a group or individual based and operating entirely within the United States or Puerto Rico without foreign direction and whose acts are directed at elements of the U.S. Government or its population, in the furtherance of political or social goals.
- International terrorism: the unlawful use of force or violence committed by a group or individual, who has some connection to a foreign power or whose activities transcend national boundaries, against persons or property to intimidate or coerce a government, the civilian population or any segment thereof, in furtherance of political or social objectives.

Combating Terrorism

Inherently, terrorism is an attack on the legitimacy of the established order, a negation of that system.[100] The Clinton Administration divided combative terrorism efforts into two major categories:

- Counter-terrorism, which includes *offensive* methods to combat terrorism (e.g., efforts to preempt and prosecute terrorists).
- Anti-terrorism, which includes *defensive* methods to combat terrorism (e.g., protection against and management of the consequences of an attack).

In order to keep terminology simple, both counter-terrorism and anti-terrorism are

addressed simultaneously and are termed counter-terrorism in this book, in order to explain the overall United States strategy to combat terrorism. Therefore "the goal of counter-terrorism is to prevent and combat it's use."[101] Thus the methods to prevent terrorist acts are inherently based on information operations due to the psychological aspects that even the *possibility* of a terrorist attack inflicts. Both sides (terrorists and policy makers) have a political purpose and the primary audience is a third party or the body politic.[102] In order to conduct successful counter-terrorism information operations against terrorist groups and to deter anti-American attacks, the credibility of the United States is crucial. Therefore "policymakers must above all demonstrate competence … the government may not always win, but it must show that U.S. policymakers, not terrorists, are in charge."[103]

This statement begs us to reflect on the dismal foreign policy failures involved with the Iranian Hostage Crisis. The capture of 55 Americans and the inexcusable duration of their internment had a vastly negative psychological impact on the American public. Since that horrible debacle, the United States has implemented retaliatory strategies against terrorists and their sympathizers that relied on its credibility in terms of international diplomacy and the use of military force. These include air strikes in 1986 on Libya in retribution for the terrorist bombings and the more recent strikes against Sudan and Afganistan in retaliation for the bombings of the United States in Africa. Secretary of State Madeleine Albright addressed critics of this course of action at an American Legion Convention on 9 September 1998,

> Some suggest that by striking back, we risk more bombings in retaliation. Unfortunately, risks are present either way. Firmness provides no guarantees, but it is far less dangerous than allowing the belief that Americans can be assaulted with impunity. And as President Clinton has said, our people are not expendable.[104]

So what is the official United States foreign policy against terrorism? It starts with a foundation that establishes that military forces will be employed where necessary and appropriate to prevent and punish terrorist attacks with four policy tenets that symbolize counter-terrorism rhetoric:

- Make no concessions to terrorists and strike no deals
- Bring terrorists to justice for their crimes
- Isolate and apply pressure on states that sponsor terrorism to force them to change their behavior
- Bolster the counter-terrorist capabilities of those countries that work with the United States and require assistance

Fundamentals of CTIO

Counter-Terrorism Information Operations builds on this verbal strategy and targets seven types of terror groups:

- State Supported
- Social Revolutionary Left
- Right Wing
- National-Separatist
- Religious Fundamentalist
- New Religions
- Criminal[105]

These types of groups are subject to misinformation campaigns, perceptions management

operations, and "coercive diplomacy," i.e. the threat of force as an influence on behavior, which requires the enemy to believe that force can be and will be used. [106] It is these IO activities that the United States employs to accomplish its military and political objectives. Specifically, a misinformation campaign intends to persuade perspective members from joining a group or influencing public opinion concerning a terrorist organization. A perceptions management operation consists of information manipulation similar to the Electronic Disturbance Theatre acts described earlier. Furthermore, the enormous growth of NGOs is a crucial tenet of any public perceptions management operation. For example, perception management operations backfired on the United States when horrific images of Army Rangers' bodies were dragged through the streets of Mogadishu. Finally, the United States uses "coercive diplomacy" to portray itself to be the defender of law and order to the body politic, both domestically and internationally through the United Nations, by condemning those states that support terrorism. International treaties or conventions or the actual funding for counter-terrorism operations also accomplishes this "confidence building" approach with its allies.

The use of misinformation campaigns, perceptions management operations, and "coercive diplomacy" rely on a systematic planning approach either to operate independently or as a combined information operation. To accomplish this, the Clinton Administration signed PDD-62 *Counter-Terrorism* on 22 May 1998. It is a much more systematic approach to combating the threat of terrorism than was previously directed in PDD-39, an earlier version of the counter-terrorism doctrine.[107]

PDD-62 *Counter-Terrorism*

This new doctrine provides a more defined structure for counter-terrorism operations as well as the tools necessary to meet the challenges posed by terrorists who may resort to the use of weapons of mass destruction.[108] Furthermore PDD-62 also serves as a focused attempt to weave the core competencies of several agencies into a comprehensive program.[109] Specifically, this new counter-terrorism doctrine clarifies the specific roles of the many federal agencies responsible for counter-terrorism, "from apprehension and prosecution of terrorists to increasing transportation security, enhancing response capabilities and protecting the computer-based systems that lie at the heart of America's economy."[110] Most importantly however, it also established the Office of the National Coordinator for Security, Infrastructure Protection and Counter-Terrorism. Currently occupied by Richard Clarke, the National Coordinator oversees a broad variety of relevant polices and programs including such areas as counterterrorism, protection of critical infrastructure, preparedness and consequence management for weapons of mass destruction. He works within the NSC, reporting to the President through the Assistant to the President for National Security Affairs. Each year the Coordinator produces an annual Security Preparedness Report, and he also regularly provides advice regarding budgets for counter-terror programs and leads in the development of guidelines necessary for crisis management. To show the importance of the National Coordinator position, as of the Fall of 2001, Richard Clarke has been retained within the new Bush Administration.

The Office of the National Coordinator for Security, Infrastructure Protection and Counter-Terrorism also acts as a facilitator and has created three senior management groups:

- The Counter-Terrorism Security Group
- The Critical Infrastructure Coordination Group

- The Weapons of Mass Destruction Preparedness Group

Each of these units works to improve the methods of response to terrorist attacks. However, the National Coordinator does not have the authority to mandate procedures to the FBI, FEMA, or any other agency. These organizations conduct most exercises with other agencies if asked or it is in their perceived interest.

As mentioned previously, the FBI's NIPC is the latest example of the government's interagency effort. This Center is a joint government and private sector partnership that include representatives from the relevant agencies of federal, state, and local government, as well as from the private sector.[111] Still, another proposed agency to improve coordination among federal agencies is H.R. 4210 the Terrorism Preparedness Act of 2000. This act establishes the Office of Terrorism Preparedness within the Executive Office of the President to coordinate and make more effective federal efforts to assist state and local emergency and response personnel in preparation for domestic terrorist attacks.[112] These activities include the FBI, DOJ, Federal Emergency and Management Agency (FEMA), DOD, DOE, Environmental Protection Agency (EPA), Alcohol, Tobacco, and Firearms (ATF), Secret Service, Office of the Vice President, offices under the Director of Central Intelligence (DCI), and the Department of Health and Human Services (HHS). Within each of these, there are various sub-departments that coordinate counter-terrorism and information operations issues. However, critics argue that the growth of federal programs to combat terrorism is excessive when compared to the relatively low number of domestic attacks.

While the number of domestic terrorism incidents is relatively small, the consequences of terrorism can have a great impact on the public. For instance, at the time of this report, lawmakers are concerned that a terrorist attack could destroy precious monuments such as the Washington Monument or the Vietnam Veterans' Memorial. These are national treasures, but in a democracy it is not possible to lock up everything that is sacred to the people. Therefore, the predicted recourse is the enormous build up of federal programs to combat the potential of terrorism.

Simulated Domestic Counter-Terrorism Operations

In the United States, the FBI is the lead agency for crisis management in the event of a terrorist attack and FEMA is the lead agency for consequence management when a threat has subsided and the task is to restore order and deliver emergency assistance. Other agencies also contribute when necessary as shown in the figure above. Although a recent proposal to build a National Homeland Security Agency was conducted by ex-Senators Hart and Rudman, many people feel that this new organization is too ambitious and will never occur. These federal agencies conduct simulated exercises to test and validate policies and procedures, as well as the effectiveness of response capabilities and eventually increase the confidence and skill level of personnel.[113] Furthermore, these tests are often conducted in a very public manner which in essence becomes an IO perceptions management operation directed at the general public. This is done to reassure the body politic that the government is doing a great deal of preparation against terrorist attacks, but more importantly, it is the impression that the government is doing something about terrorism. It is a verbal strategy as discussed before that demonstrates to the American people as well as to the rest of the world that the United States is engaged against terrorism just as the United States was against communism.

The United States conducts itself in this arena in a very similar manner as it did during the Cold War with the Soviet Union. Spending for counter-terrorism operations has nearly doubled in the last five years, and the budget for the lead federal agency for combating terrorism, the FBI, has also grown exponentially to prepare against the possibility of terrorist attacks. This growth in spending demonstrates that counter-terrorism is a top priority for the United States. It also reassures the public that the government is spending whatever it takes to prevent another Oklahoma City and it shows terrorists that the United States is not an easy target. This has also been accomplished by conducting exercises to put rhetoric into actual practice.

In May 2000, federal agencies conducted a ten-day response exercise designated TOPOFF, which stands for Top Officials. This operation brought together over 150 state and local emergency response planners and practitioners from across the nation, to identify the objectives used to design the $3.5 million TOPOFF exercise.[114] Agencies that participated in the exercise included the FBI, DOJ, FEMA, DOE, DOD, HHS, EPA, Department of Agriculture, the Department of Transportation, and the General Services Administration. To further test federal response, agencies performed National Capital Region 2000 (NCR-2000) in the District of Columbia and Prince George's County, MD. NCR-2000 tested the response to weapons of mass destruction events. Both events brought together a wide array of federal agencies to coordinate and practice a response to terrorism. The tests was successful, however there were still incidents where command and control issues plagued responders.

Partnerships for Counter-Terrorism: "Track Two Diplomacy"

United States counterterrorism policy is not formulated solely from reactive exercises and organizational changes in federal agencies. In fact over the past several decades, there has been growing evidence that unofficial actors, including NGOs are playing an increasingly important role in the development and implementation of government policies. To describe the efforts of ordinary citizens and unofficial organizations that resolve conflict, former United States diplomat Joseph Montville coined the term "track two diplomacy" in 1981.[115] The basic notion behind "track two diplomacy" is that government alone cannot achieve peace and conflict resolution. Unofficial informal behind-the-scenes contact, either with policy recommendation publications or by attending multinational conferences, plays a vital role in conflict resolution and in promoting regional security.[116] NGOs also play an increasingly important role in combating international terrorism. These organizations not only act to influence policy decisions, they are also able to place accountability to combat terrorism on national and international organizations, like the United Nations Security Council. NGOs have the ability to sway public opinion or more practically, offer congressional testimony. To date, the most important function of these groups is their ability to help foster multinational consensus concerning terrorism thus forming an international front against terrorism.

International Cooperation

"International terrorism threatens U.S. foreign and domestic security and compromises a broad range of U.S. foreign policy goals," according to Raphael Perl of the Congressional Research Service's Foreign Affairs and National Defense Division.[117] He also notes that, "Terrorism erodes international stability—a major foreign and economic policy objective for the United States."[118] Therefore, it is in the best interest of United States national security to seek

cooperation from our allies to combat terrorism. In this post Cold War era, the United States relies on its allies to ensure global and regional security by using existing partnerships and multinational institutions, such as the United Nations. While there have been relatively few cases of domestic terrorism in the last four years, attacks against the United States have increased drastically. The number of total anti-U.S. attacks to range from 73 in 1996 to 169 in 1999, which is an increase of 132% in four years.[119]

A prominent attack in the last three years were the terrorists' strikes on the United States embassies in Nairobi, Kenya and Dar Es Salaam, Tanzania on 9 August 1998. Following these tragic disasters, Congressman Frank Wolf introduced the National Commission on Terrorism Act on 9 September 1998. Before this act passed in early 1999, President Clinton addressed the opening session of the 53rd United Nations General Assembly in New York on 21 September 1998, to solicit international support to combat terrorism. President Clinton identified terrorism as the greatest threat to peace, not just to the United States, but to the world. He stressed that terrorism is not fading away with the end of the 20th century and that, "it is a continuing defiance of Article 3 of the Universal Declaration of Human Rights, which says, 'Everyone has the right to life, liberty, and security of person'."[120] This speech was one of many attempts to gain international support against terrorism.

Before the September 1998 speech to the United Nations General Assembly, a conference between the United States and the European Union (EU) was held on 18 May 1998. Its conclusions state, "The United States and the EU member states are strategic allies in the global fight against terrorism… we oppose terrorism in all its forms, whatever the motivation of its perpetrators, oppose concessions to terrorists, and agree on the need to resist extortion threats. The United States and the EU condemn absolutely not only those who plan or commit terrorist acts, but also any who support, finance or harbor terrorists."[121] From this conference, all parties involved agreed that to end state-sponsored terrorism, that international cooperation is necessary in the global economy.

Due to the success of the United States-EU summit, the State Department, as the lead federal agency designated to combat international terrorist threats, hosted an international counterterrorism conference on 16-18 June 1999. Each panel discussion included members from NGOs such as RAND, CSIS and government officials including Israeli Diplomats and leaders of NATO as well as 22 United Nations member states. This conference focused on the need to cooperate across borders in order to eliminate foreign and domestic terrorists' threats. If any state openly sponsored terrorism, economically or physically, economic sanctions will be imposed from all member states of the EU and the United States. To do this, the Secretary of State maintains a list of countries that have "repeatedly provided support for acts of international terrorism," and these include Cuba, Libya, North Korea, Iran, Iraq, Sudan and Syria.

PDD-63 *Critical Infrastructure Protection*

If *ER '97* and JV2020 are the bookends for this publication, then probably the defining moment for change in the United States government organizational architecture came with the promulgation of PDD-63. Although it has been touched on in earlier chapters of this book, we feel that it was of such importance as to merit a stand-alone section. This is because circumstances are forcing many military and government activities to develop defensive plans based on vulnerabilities rather than on the threat. The United States government is attempting to

help that coordination by adding CIP as a new PDD which was part of their overall NSS. Released on 22 May 1998, PDD-63 *Critical Infrastructure Protection*, this policy was also covered in the IO Organization section as a critical new element in the Clinton's Administration overall strategy. Much of the impetuous for this new policy, came from a series of well publicized terrorist attacks such as Ruby Ridge, Waco, the World Trade Center and the Federal Building in Oklahoma City. All of these incidents and standoffs by federal agents led to a feeling that there was a threat to our national infrastructures and, in turn, our national security. The Clinton Administration believed that if they could emphasize the need for public and private cooperation for infrastructure protection, then they could be successful from the current threats.

To that end, the Administration began working in 1996 on developing a series of plans and policy that ultimately culminated in PDD-63. The most important documents included Executive Order 13010 *President's Commission on Critical Infrastructure Protection (PCCIP)* and *Critical Foundations*. These reports laid the foundation for *Critical Infrastructure Protection* (PDD-63) and they are also tied very closely to another policy document, *Counter-Terrorism* (PDD-62). Both were released on the same day and both are headed by the same director at the NSC, Richard Clarke. This physical and symbolic closeness is good in that in allows the NSC to focus on all aspects of the issues for protecting the United States infrastructure. The goals of PDD 63 were to:

- Establish a national center to warn of and respond to attacks
- Address the cyber and physical infrastructure vulnerabilities of the Federal government by requiring each department and agency to reduce its exposure to new threats
- The Federal government will serve as a model to the rest of the country for how infrastructure protection should be attained
- Seeks voluntary participation of private industry to meet common goals for protecting our critical systems through public-private partnerships

To accomplish these goals, PDD 63 established the following institutions:

- The National Infrastructure Protection Center (NIPC) at the FBI which fuses representatives from FBI, DOD, United States Secret Service, Energy, Transportation, the Intelligence Community, and the private sector in an unprecedented attempt at information sharing among agencies in collaboration with the private sector. The NIPC also provides the principal means of facilitating and coordinating the Federal Government's response to an incident, mitigating attacks, investigating threats and monitoring reconstitution efforts
- Information Sharing and Analysis Centers (ISACs) are encouraged to be set up by the private sector in cooperation with the Federal government and modeled on the Centers for Disease Control and Prevention.
- A National Infrastructure Assurance Council (NIAC) drawn from private sector leaders and state/local officials provide guidance to the policy formulation of a National Plan;
- The Critical Infrastructure Assurance Office (CIAO) provides support to the National Coordinator's work with government agencies and the private sector in developing a national plan. The office also helps coordinate a national education and awareness program, and legislative and public affairs

In the original plan, two years after PDD-63 was released, an initial operating capability was supposed to have been achieved. Within five years (2003), PDD-63 was to have the operating capability to fully protect the nation's critical infrastructures would be assured. This

would include federal, state and local sector compliance as well as commercial cooperation. To this date, the authors are happy to announce that PDD-63 is on track. Numerous milestones have been released and with an increased guidance from the NSC, *Critical Infrastructure Protection* has significantly changed the public-private cooperation over the last two years. Admittedly it didn't hurt that there was a huge amount of attention paid to computer systems due to the Y2K rollover date, but much of the credit must be given to Richard Clarke and his staff. It was through their efforts that the success of PDD-63 over the last three years has been assured.

Summary

In conclusion, Information Protection is a huge area that needs from the United States government agencies and military to be effective. Officials have only recently in the last few years become aware of the true extent to which our nation is vulnerable to asymmetric attacks. As you have realized, a large number of programs have been covered in this chapter as the various governmental agencies have attempted to come to grip with the real-time threats imposed by IO. IA, CND, CTIO and CIP are all key elements of a defensive IO program, and significant effort has been made to increase funding and importance of these areas over the last few years. If we can emphasize only one thing out of this whole chapter, it would have to be that the best defense against IO attacks must be based on people and training. No amount of technology and policy can overcome a determined foe, but the proper training of good managers and administrators can often mitigate the effects of these attacks. And of course, only time will tell how effective these measures truly are.

Chapter 4 - Information Projection - Shaping the Global Village

"Iraq lost the war before it even began. This was a war of intelligence, electronic warfare, command and control, and counterintelligence. Iraqi troops were blinded and deafened . . . modern war can be won by informatika and that is now vital for the U.S. and U.S.S.R." [122]

Soviet Lieutenant General S. Bogdanov

The last chapter discussed the need for commanders to protect their information and information systems, however just or perhaps even more important is the need to plan military operations to exploit vulnerabilities in adversary information and information systems. JP 3-13 defines offensive information operations as:

> The integrated use of assigned and supporting capabilities and activities, mutually supported by intelligence, to affect adversary decision-makers to achieve or promote specific objectives. These capabilities and activities include, but are not limited to, operations security, military deception, psychological operations, electronic warfare, physical attack and/or destruction, and special information operations, and could include computer network attack.[123]

It is significant to note that this definition includes CNA, because before the publication of JP 3-13 in October 1998, this IO capability was classified. In addition, significant discussions of offensive information operations are contained in JP 3-13 under the following phrase: "Offensive information operations can support defensive information operations."[124] Although this may seem a subtle change, it does support the further assimilation of both disciplines into one, reinforcing a more proactive, rather than reactive approach. It also correlates well to the American penchant for the idea that the best defense is a good offense. In addition, offensive IO has also concentrated on the two main developments that have come to the fore in the last several years. Involving CNA and Perception Management, both of theses areas are where most of the focus for IO is currently being conducted.

Offensive Information Operations

The target for offensive information operations is the human decision-maker. We cannot emphasize this enough, to show the difference between the older disciplines incorporated in C2W. Whereas the earlier policy concentrated on nodes and links, IO has instead has a focus on influencing the commander or decision-maker. Commanders will plan to employ offensive IO capabilities and related activities with the goal of influencing their adversary's observation, orientation and perceptions, thus causing them to decide to act in a way that is advantageous to that commander's military objectives. As mentioned in Chapter 1, within United States doctrine, this is called Information Superiority, and IO is a sub-component of that theory.[125]

For offensive IO, there are a number of planning considerations. First, commanders need a range of capabilities in order to shape their broad operational environment. For example, the Commander-in-Chief of the U.S. Southern Command, General Charles Wilhelm, USMC, recognizes IO as a core competency and considers its employment as he would any other battlefield operating system when designing his TEP.[126] Since these plans are a tool for managing and shaping a CINC's AOR for a period of seven years, these documents are especially useful in the IO context. So much of IO is done before a crisis occurs, before a warning or an

execution order is issued, that it is the TEP and the collateral DOS reports that in essence constitute the IO attack plan. Therefore, IO can consist of offensive tools such as public affairs, civil affairs, psychological operations and CNA all of which can be conducted in a pre-hostilities phase of a potential conflict. In addition, offensive IO also considers both lethal and non-lethal weapons as means available to disrupt the adversary's information flow and services.

There are also some general principles for employing offensive information operations that must be considered in planning military operations. While offensive IO may be the main or supporting effort of a JFC's campaign or operation, it must also support the overall military objectives and have some form of observable measures of effectiveness (MOE). Finding such measures is often one of the most problematic issues, simply because some aspects of IO do not lend themselves to easily quantifiable observations. As mentioned repeatedly, IO is not something that can be done quickly or in a crisis mode. Therefore there is also a need for extensive lead time in preparing for offensive IO in order to ensure that the adversary decision maker is responding in the way one intends, thus raising the need for a thorough IPB prior to any offensive IO effort. Also, to be successful, offensive IO must fit with overall United States security objectives and be consistent with established rules of engagement. Furthermore, offensive IO must also be thoroughly integrated with all those non-DOD organizations throughout the interagency involved with the particular operation. In a regional context, the CINC – Ambassador/Country Team relationship is the most crucial for organizing and conducting an offensive IO strategy. The need for long-lead times, plus the required interagency involvement, has thus to some extent inhibited the successful use of IO as a strategy to shape the environment. However, there are indicators that as IO becomes more established within the United States government, these factors will become more accepted.

Therefore it appears evident that both doctrinally and operationally the distinction between offensive and defensive information operations is becoming increasingly blurred. This sentiment was communicated in January 1999 by President Clinton in an address to the National Academy of Sciences. Discussing the implications of the threats posed by terrorists (including cyberterrorists) and weapons of mass destruction, President Clinton noted that, "Because of the speed with which change is occurring in our society, in computing technology, and particularly in the biological sciences, we have got to do everything we can to make sure that we close the gap between offense and defense to nothing, if possible. That is the challenge here."[127]

By doctrine, IO is composed of six capabilities and two related activities. While we could discuss all of these mission areas in great detail, we chose instead to focus on the specific functions that are new or have changed significantly in the last three years. Therefore the first offensive IO capability that we would like to address is computer network attack or CNA. This will be followed by space-based applications of IO, Electronic Warfare (EW) and International Public Information. These four areas will be the focus of this chapter because this is where we as the staff of Information Warfare at the Joint Forces Staff College think that the biggest advances in IO will come in the future.

Computer Network Attack

"Computer Network Attack." The very term evokes thoughts of cyberwar and futuristic technology, with visions of precision accuracy and war without needless violence, perhaps even a kinder and gentler form of warfare. Yet perception does not equate to reality. Therefore, while

by definition CNA is a current warfighting capability of the United States, some would say that it is so limited by legal, political, and security constraints as to make it virtually useless to the combatant commanders.

Though this section discusses these issues and others associated with CNA, because much of this technology is classified, it cannot go into detail on some of the subtopics. In fact the very term Computer Network Attack was classified until October 1998 with the publication of JP 3-13. Before that time its use had been classified at least to the Secret level and even today, CNA cannot be associated with certain commands without immediately raising the classification level. For example, JP 3-13 gives only one sentence to CNA before referring the reader to the Secret supplement. So, unfortunately for the present volume, much of the discussion of CNA must be short and generic. This chapter instead focuses on what CNA can and cannot do and raises issues on some of its capabilities and limitations. It does not, however, describe how the United States is conducting CNA missions, or give examples of any recent CNA operations.

By definition CNA operations disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves.[128] While most people think CNA as being conducted over the World Wide Web or the Internet, in fact the physical destruction of a computer system or network by kinetic means also qualifies as CNA. Indeed, if a computer is not connected to a local area network (LAN) or the Internet and is a stand-alone system, then it will have to be physically destroyed or have malicious computer code physically inserted into its software program. That form of CNA might no longer be under the purview of uniformed military forces, but instead might fall to other organizations that have traditionally conducted such operations.

However, it is the ability to disable an enemy's computer system from afar, often from the safety of one's own command and control center, that makes this new form of warfare desirable. The safety and virtually risk-free concept of attacking from a distance has led some people to suggest that CNA is the "silver-bullet" that everyone wants in a new weapon. But, of course, there is no such thing as a "silver bullet." Thus, while CNA has enormous potential and capabilities, so far a variety of legal, political, and technological constraints have kept it from being fully exploited as envisioned.

In fact, the legal constraints alone may restrict the use of CNA by United States military forces. The caution is similar to the NBC (nuclear, biological, chemical) criterion of not using any weapon on an adversary that the user is not fully prepared to defend against. The United States is the most vulnerable of any country to a computer attack, so for us to initiate CNA would surely open the floodgates against it. Likewise, CNA can effect civilian as well as military targets with the same equipment. Should an attack target only military bases or should it try to cripple the economic base of a nation? If an attack targets financial institutions and spreads panic among an adversary's populace, is the attacker operating within the Geneva Convention and Laws of War, specifically those that require attacking only military targets, while minimizing collateral damage and avoiding indiscriminate attacks?

The specter of CNA is so large that Russia has attempted to limit its use by the adoption of new international laws. A proposal has been submitted to the United Nations to ban the use of Information Operations. While the White House under the Clinton Administration successfully deflected their proposal, it could gain strength and develop a life of its own, witness the worldwide movement to ban land mines. In addition to the legal constraints, there are also

technological challenges in conducting CNA. To be effective, a CNA operation is aimed at a single computer or a system of computers that conducts a specific mission. The intelligence needed to conduct a computer network attack is an order of magnitude greater than what may be needed for a bombing mission. Some of the following questions need to be answered to prepare adequately for a CNA operation:

- Where is the system that is to be the target? What room on what floor of which building?
- What kind of hardware is hosting the system?
- What software is resident on the computer and which version is currently installed?
- Is the computer connected to the World Wide Web or is it "air-gapped," i.e., a stand-alone system?

Once these and other questions are asked, the "painless" claim for CNA proves wrong, and these operations become as difficult or perhaps more so than other types of attacks that are more familiar. In addition, the targeting aspect of CNA is extremely difficult. Once intelligence has narrowed the list to a system or perhaps a single unit, the attacker must be sure that the targeted computer is in fact the right machine and not an intermediate Internet Service Provider (ISP).

While CNA is defined by the big four "D" words - disrupt, deny, degrade, and destroy, another facet of these types of missions is actually gaining access to a computer. That activity is often referred to as Computer Network Exploitation (CNE) and, more often than not, is the hardest part of CNA. Once in and having gained access, anyone can mess up a system, but getting past the security systems is definitely tricky. To confuse matters even more, while only certain organizations are allowed by law to conduct CNA, that same restriction does not necessarily apply to CNE.

What are the signs that a CNA operation is occurring? Does a computer explode on the desk? Or does it simply stop working? In fact, both instances may be signs of an attack, or may also be signs of operator error. Yet CNA can often be more subtle. The attack may occur without the adversary's realizing that it has been attacked. Since computers are often viewed as office rather than military equipment, they tend not to have the technical documentation or personnel support of a major weapon system. For example, suppose a computer system stops working. What does the operator do? Most will try to logically troubleshoot the computer by looking for obvious faults, and then, failing that test, try to reset the software. Perhaps they will hit the ESC key a couple of times or maybe try CTRL ALT DEL and end the particular task, or in the worst case, simply use the ON/OFF switch to reboot the system. This process probably takes about 10-15 minutes, and then the frustrated operator calls the system administrator, who, with luck, can respond to the trouble call soon. The administrator often goes through the process again, trying to reboot the system and checking its configuration. The whole process can take time, during which a vital message may have arrived, or an action taken place that has gone undetected because the computer was off-line. If IO is simply an integrating strategy that creates effects from different warfare areas, the denial of computer service is no different than jamming or destroying the same equipment. If one can safely affect that computer system from afar, and guarantee that one can control its effects, then maybe perhaps CNA is the weapon of choice.

By law, the four uniformed Services are required to recruit, train, equip, and support the armed military forces and provide those forces to the CINCs for their use around the world. Therefore weapons procurement becomes the responsibility of the individual Services, a major

political and financial issue depending on the system. But suppose the CINC directly acquires a "weapon" from outside sources, without service testing. The services may also have issues concerning control over software programs that have not gone through the typical acquisition process. Yet if a CNA program is used by a CINC, at some point it must be "weaponized". These can be major problems when Services are not involved in the procurement or training of these CNA weapons and do not maintain them in any sort of inventory. Questions will arise about who owns them and who can use them. Other problems may arise, namely concerning the deconfliction of CNA operations. The services have developed the Joint Force Air Command and Control (JFACC) system to deconflict air missions among the different Services, and it has worked reasonably well in a multitude of operations during the last decade. However, there is no comparable system for CNA operations. Instead, a number of classified groups meet to deconflict computer operations.

The current perceived lack of use of CNA weapons can also be attributed to the fact that many senior officers are not familiar with them. They grew up in a military filled with kinetic solutions, and unless they are educated on the potential effects of these new weapons, their first decision is often to not use them. Likewise if a CNA program is kept behind the green door in a compartmented cell and brought out only in a moment of crisis, its use will often not be approved. Senior leaders must be educated and read into programs that allow them to understand the capabilities of CNA. Only then can they appreciate its capabilities and be more inclined to use these weapons when the opportunity arises.

There are thus many complicated issues involved with CNA, that make it hard to discuss at an unclassified level. Needless to say, this is a new and important warfare area of IO, one that will need time not only to evolve but also to prove itself to a whole new generation of military leaders for its use to become commonplace. The potential for the future use of CNA is great and with proper education, research and development, we may be able to eventually realize that potential.

Space and its Relationship with IO

Space has become an important factor in the arena of IO. What today is termed the "information age" is largely a result of the use of space as a catalyst in this very significant evolution. While many people today think of space as a far away place of the future, they forget to realize that satellites are passing overhead at a mere distance of 100 miles and that the benefits of space are as close as their TV remotes, a cellular phone, the nightly news and a number of other daily conveniences. Space plays an integral role in all aspects of military operations as well as becoming an ever-increasing part of all government departments. The far reaching impact of space use has had the significant result changing the very world in which we live by providing an apparent shrinking and in some cases dissolving of international boundaries, compression of time and the ability to have near instantaneous insight into happenings around the globe.

While benefits of space derived information have played a significant role since the early days of the space program, there has been a remarkable change in the last few years that promises to revolutionize how we look at space in the future. This change involves the greatly increased availability of space derived data to the public and the implications that free access to space systems can have upon governments and their respective militaries. This distribution of power away from the military and official government agencies to NGOs and individuals has also

considerably altered the access to this information. This idea ties directly to the themes discussed in the first chapter that the power of information is now no longer in the hands of the military and government alone, but has instead been distributed more to the people.

For the majority of time since the dawning of the space age, access to space derived information has been limited to a very elite few. These early space systems provided an immense information advantage to leaders of owning countries. The consumers of these systems benefited by being able to see into other's backyards, to eaves drop on conversations, and provide early warning of potential attack. The diplomatic and military value of this information is clear in a quote by Lyndon Johnson who is reported to have said, "We've spent thirty-five or forty billion dollars on the space program. And if nothing else had come out of it except the knowledge we've gained from space photography, it would be worth ten times what the whole program cost." [129]

Today, the availability of space system information has greatly increased with the advent of numerous commercial systems that have made available space derived data to the public. This commercialization of space in recent years has brought astounding results as the application of space data finds its way into more and more aspects of daily life. Today, the commercial market provides high-resolution imagery, precision navigation, highly accurate timing signals, remote sensing data, telecommunications support and a host of other applications. The commercial application of space information is so great that indeed, the information age has come about largely as a direct result of capabilities provided by these systems. But, in this case, the availability of information is a double-edged sword that is effectively whittling away at the advantage enjoyed by the United States as one of the historical few that has in the past controlled space system information.

One recent event in the commercialization of space systems involves space imagery. High-resolution imagery of less than three meters was not publicly available before the 1990's. With the September 1999 launch of the Ikonos imagery satellite, one-meter resolution imagery is now available to the public at a cost of $30 - $300 per square mile. The impact of this increased availability is rapidly becoming apparent as new commercial applications of space imagery are identified. It also provides an excellent intelligence-gathering tool to any country that wants to have a better look at its neighbors or for terrorist groups to identify and monitor potential targets. Instead of government officials dictating the appropriate time to release information gleaned from a space surveillance satellite, the media, NGOs or even individuals can now "beat them to the punch" by ordering and analyzing the appropriate images. There is even now the potential for government decisions and policies to be challenged by anyone armed with the appropriate surveillance information.

Space based navigation is another example of recent changes in regards to the commercialization of space. The Global Positioning System (GPS) provides unprecedented accuracy and timing information as a free service, available to anyone with relatively inexpensive receive equipment. Developed and deployed by the military in the 1980's, this system has obvious military and civilian applications. While GPS was initially designed to provide commercially available navigation, the overwhelming number and breadth of commercial applications is unprecedented. Commercial GPS systems allow manufacturers to track the status of deliveries, farmers have improved land management applications, outdoor enthusiasts depend on them, police keep tabs of dangerous criminals on parole, rental cars provide them as an option

to assist customers to locate their destinations, schools provide advance notice to students as busses approach their respective bus stops, and fishermen can find their favorite fishing holes. While the number of navigation applications continues to grow at a phenomenal pace, arguably the greatest commercial benefit from GPS is derived from the highly accurate timing signal broadcast from each GPS satellite. This timing signal plays a critical part in telecommunications, electrical generation and other technologies. Even with this extraordinary commercial demand, the most accurate GPS signals were historically reserved for strictly military use before the year 2000. On 01 May 2000, under new policy guidance from President Clinton, these highly accurate navigational signals were now made available to all commercial users resulting in an immediate 10-fold improvement for all commercial receivers. [130] Of issue was the availability of GPS navigation data, which under this proclamation now changed the advantage that our military forces had previously held with exclusive access to this system. The military applications of GPS data are very extensive from precision weapon delivery and force movement to tracking of logistics and supplies. This advantage is now slipping as other countries realize the value of GPS and begin to acquire, field and use ground receivers themselves. While the United States military reserves the capability of selectively degrading the commercial GPS signal, it will never again enjoy the unchallenged availability to high precision navigation that was available with the initial GPS deployment.

As commercial capabilities continue to grow, the United States needs to develop a strategy for handling the availability of space technology overseas while maintaining the national's domination in space. This issue became increasingly complex as new international consortiums enter the space arena and the number of commercial space based sensors increase. This issue is further complicated as the capabilities of commercial satellites increase to the point that they rival or surpass national and military capabilities. This could lead to the loss of advantages enjoyed during previous conflicts such as:

- The practice of deception will be complicated. The left hook tactic during Desert Storm worked because the opposing side did not see it coming. With commercially available satellite imagery, this type of maneuver will become harder.
- The practice of hitting critical nodes to eliminate adversary C2 and lines of communication has now been greatly complicated. For the price of a low-end computer, anyone can purchase a handheld cellphone that uses ground and/or space based cellular technology. Utilization of this capability can provide a robust command, control and communication infrastructure that is difficult to counter.
- Proliferation of the GPS has for all practical purposes eliminated advantages associated with space based navigation. Integration of this technology into theater ballistic missile systems can greatly improve accuracy and place armed forces at greater risk.

Yet as recently as May 1999, the United States military, which possessed a tremendous intelligence and space-based photography capability, was still deceived by the camouflage tactics used by the Serbians. So to say that access to one-meter resolution pictures will negate the traditional military capabilities of the armed forces is a bit premature we believe. However the importance of space with relation to IO is emphasized by the shift in mission areas of CND and CNA to USSPACECOM over the last two years. As mentioned in Chapter 1, UCP '99 directed this shift and the CINCs staff has worked very hard during this period to operationalize and institutionalize both space and IO as warfighting disciplines. To the extent that they become

effective and synchronized in the future will be interesting to witness.

The Relationship Between EW and IO

When JP 3-13 was published in 1998, it was generally thought that confusion over the controversial subject of IO would subside. However as has been illustrated elsewhere in this book, that is certainly not the case. One area still causing problems is the relationship between EW and IO. In this chapter, the authors hope to clear away some of the confusion. We will do this by defining the architecture of EW and then use examples to show when EW is IO, and also when it is not. As mentioned in Chapter 1, the joint definition for IO is so broad that at times it can encompass nearly anything but the attempt of this section is to give you concrete examples of what IO is and also what it is not.

JP 3-13 defines IO as "Actions taken to affect adversary information and information systems while defending one's own information and information systems."[1] Given this definition, the question arises: “When we conduct electronic warfare, are we affecting adversary information and information systems or defending our own?” Perhaps the definition of EW will offer a clue. JP 3-51, Joint Doctrine for Electronic Warfare, defines electronic warfare as "Any military action involving the use of electromagnetic (EM) and directed energy to control the electromagnetic spectrum or to attack the enemy.” The three major subdivisions are:

- Electronic Attack (EA)
- Electronic Protection (EP)
- Electronic Warfare Support (ES)"[2]

Which brings us to another question, namely, are the electromagnetic spectrum and the enemy considered information systems? Before we answer this question, we need to know what an information system is. JP 3-13, defines an information system as "The entire infrastructure, organization, personnel, and components that collect, process, store, transmit, display, disseminate, and act on information."[3] So for most people, this means that the electromagnetic spectrum is an infrastructure or conduit that facilitates the reception and transmission of information. JP 3-51 defines the electromagnetic spectrum as "The range of frequencies of electromagnetic radiation from zero to infinity."[4] This definition alone certainly doesn't clarify anything, however the doctrine further expounds on the concept of the EM environment. "Today, electromagnetic (EM) devices are used by both civilian and military organizations for communications, navigation, sensing, information storage, and processing, as well as a variety of other purposes."[5] The spectrum is an infrastructure over which EM devices transmit or receive information! So if we think about this logically, any military action to control the electromagnetic spectrum affects an infrastructure which is part of an information system!

To show the specific advantages of EW, the next few paragraphs delineate some current doctrinal questions that are arising concerning relationships between EW and IO. Electronic attack is "that division of electronic warfare involving the use of electromagnetic energy, directed energy, or antiradiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability."[6] A good example is if an antiradiation missile destroys a radar antenna and the radar is an information system, then this is a case where EA is IO. If on the other hand, we use a laser to destroy a ballistic missile, many would argue that this unguided missile is not an information system, and in this case EA is not IO.

Electronic protection is "that division of electronic warfare involving passive and active means taken to protect personnel, facilities, and equipment from any effects of friendly or enemy employment of electronic warfare that degrade, neutralize, or destroy friendly combat capability."[7] If the personnel, facilities, and equipment are part of an information system, then EP is IO. For example, let's say we reprogram our radar warning receivers to recognize an enemy wartime reserve frequency. In this case, we've protected our information system and therefore, EP is IO. However if we put a lead shield around Army tank engines to protect them from an enemy radio frequency weapon, this would certainly fall under EP, but many would argue that a tank is not an information system and in this case, EP is not IO.

Electronic warfare support is "that division of electronic warfare involving actions tasked by, or under direct control of, an operational commander to search for, intercept, identify, and locate or localize sources of intentional and unintentional radiated electromagnetic energy for the purpose of immediate threat recognition, targeting, planning and conduct of future operations."[8] ES is not a part of IO. Collecting, processing and disseminating information falls under one of the three components of information superiority called "relevant information." The other two components are "information systems" and "information operations."

Earlier, we made the case that EW and IO overlap. We started out by looking at the definition of IO and EW to see if we could clarify the relationship. Once we got beyond the overall definitions and delved into the subdivisions, we could clearly see that there are cases when EW is IO and when EW is not. The authors believe this whole discussion is important because it shows how a particular capability relates to IO. It is also meant to show that while there are eight capabilities and related activities, just because you conduct a certain capability in this case EW, that does necessarily mean that you are doing IO as well.

PDD-68 *International Public Information*

Why in this new era, in this information age do we not have a single point or executive agency to coordinate and control the flow of information within the United States government? It is most likely since information is a tool that organizations use and because its control is no longer singularly in the hands of the government, it is understandable that no one single agency or unit owns the sources or means of delivery, nor the production as well.

These changes in technology alter, and in some sense diminish, the importance of the traditional role of the executive departments. Likewise, NGOs and other players have become more important in the last 10 years because of their ability to move with speed and agility to the different crisis areas of the world. Therefore in this post Cold War era, the fungibility of information and the use of “Soft Power” by the United States has greatly increased the need for a mechanism to coordinate a coherent message.[131] Yet at the same time, the drastic downsizing of the DOD and State Department agencies that coordinate these activities have forced the need for a reorganization and reconstitution of United States government public diplomacy capabilities. The unfortunate result of all this is that at this time, no single agency is empowered to coordinate United States efforts to sell its policies and counteract negative publicity. Therefore, the promulgation of PDD-68 *International Public Information* (IPI) was an outgrowth of efforts by the Clinton Administration to tackle the public relations portion within the greater issue of managing complex contingencies. However after two years in place, this new policy guidance has only recently begun to receive the predicted positive response that was expected when it was

signed.

History of IPI

The history of PDD-68 and IPI within the Clinton Administration is relatively short. During Operation Desert Storm, an Information Coordination Cell (ICC) was set up at the Pentagon. The NSC played a major role in this unit and many people within that organization clearly recognized how important this ICC was and that it should be a continuous feature, not an ad hoc creation. Therefore in 1993, the DOD requested that the NSC create an ongoing information coordinating body. Although nothing came of this initial effort, personnel, including Walt Slocomb who was the USD(P) under the Clinton Administration, were involved in this initial request, and were still a part of the civilian infrastructure at the DOD to help with these developments of IPI.

Fast forward a few years. The Clinton Administration is becoming heavily involved in complex contingencies like Haiti and Rwanda, where questions are beginning to arise within the White House and the NSC concerning information's ability to intervene in order to change the power structure in a crisis situation. Basic ideas such as "all crises starting with information", or "is one group controlling the information" began to be seen as possible methods for exploitation by the United States. Following these complex contingencies, a new policy document was issued entitled PDD-56 *Managing Complex Contingency Operations*.[132] The idea behind this new guidance was to build an executive committee (EXCOMM) that could coordinate interagency issues concerning complex contingencies around the world. It was realized that these problems could not be solved by military, economic or diplomatic power alone and thus other essential agencies were needed to be brought into the decision process.

Concurrently with this development in mid-1997, a number of mid-grade White House and NSC staffers began to write a PDD on information as a public diplomacy tool. They wanted to use the PDD-56 construct of Complex Contingencies and build a permanent working group at the deputies level that could meet on a regular basis to formulate public information policy. Their goal was to assess the information projection capabilities of the different government agencies and evaluate their usefulness. By the spring of 1998, the IPI group completed its five-month assessment concluding that a central coordinating body is necessary to integrate various federal departments' information projection capabilities. The IPI working group then drafted a rough PDD document and routed it through the various agencies for review.

Throughout the rest of 1998, the IPI group was busy working information issues within the interagency process. Due to budget cutbacks and a restructuring of the State Department, it was announced in late 1998 that by 1 October 1999, the premier public diplomacy organization in the government, the USIA was to be merged with the DOS. Thus, concurrent with the review of the IPI PDD came a need to build a home for this group within the restructured State Department. Therefore, a key component of the State Department Reform and Restructuring Act of 1998 was to form a new Under Secretary of State for Public Diplomacy and Public Affairs. This new office was proposed to be the key component and champion for IPI and would chair the interagency core group once the policy document was signed.

Outside Influences on IPI

Finally on 30 April 1999, PDD-68 was signed by President Clinton, but without the usual

fanfare. It was not detailed in a major policy speech or statement and in fact to this day, you cannot download a copy of the whole document off the World Wide Web like some of the other PDDs. The document is not considered classified but has remained for official use only in the last year of its use. It is a decidedly low-key policy statement compared to other PDDs issued by the Clinton Administration, and there are a number of reasons for this. First, IPI is a controversial issue. Anytime that you talk about trying to conduct psychological operations or perception management issues on a foreign audience, you are bound to attract controversy. Second, IPI became a victim of bureaucratic change within the State Department. Because PDD-68 was handed over to a cabinet agency to coordinate vice kept at the NSC level, it is influenced by the department politics more than perhaps other policy documents have. The fact that the IPI Core Group was assigned to State, which while the main diplomatic agency for the United States government, is not necessarily an operational command has somewhat prevented IPI from shaping the environment using information as was originally intended. A good example of this is seen in the actions of the IPI Core Group. This activity is supposed to be the main interagency body that coordinates information issues has only met once in the last year and is not the tool that was originally envisioned. Key IPI visionaries have not been able to remain concentrated on this issue due to a number of circumstances including bureaucratic and organizational politics.

In addition, there have been outside influences that have also affected the operation of PDD-68 in the last year. These were evidenced mainly in two articles that were written about IPI in August 1999 and published in the Washington Times newspaper. Both of these articles criticized IPI as simply a smoke screen by the Clinton Administration to try to conduct psychological operations against the American people. It also did not help that PDD-68 was considered to be somewhat sensitive, it was not generally available to the American public therefore a much-needed general debate did not subsequently occur. These negative stories were released concurrent with the appointment of a new undersecretary was to take office, so altogether they tended to cast a pall over the whole issue. In addition, a final issue that has delayed the implementation of IPI has been the slowness of the reorganization at the Department of State, which has also prevented an essential piece of PDD-68 implementation from occurring. According to the policy document, a DOD liaison officer should have been assigned to DOS to work solely IPI issues, yet that billet was gapped for the first 15 months of IPI's existence.

Therefore as you can see, the history of PDD-68 is relatively short. Much of the interest and heavy involvement from interagency officials has all occurred in the last three years. While one cannot speculate on the future of IPI and the use of information as tool for preventing complex contingencies, it will be interesting to see how this policy fares in the future.

What is IPI?

As stated earlier, the current phrase in use by the United States to affect the public opinion of foreign audiences is IPI and it is defined in PDD-68. It includes a combination of public affairs, international military information and public diplomacy. In reality, it is about the power of information.[133] Public diplomacy is the open exchange of ideas and information. It is an inherent characteristic of democratic societies and is central to United States foreign policy initiatives. Public diplomacy remains indispensable to achieving our national interests, ideals and leadership role in the world. Since the end of World War II, the United States has attempted to use public diplomacy as a tool to influence foreign audiences around the world. Thus, the

development of PDD-68 is the latest in a long line of attempts by the United States government to harness the power inherent in information.

Public affairs and International Military Information (IMI) comprise the other parts of IPI. Traditionally these two disciplines have not normally been associated with each other. Public affairs is often considered a support function. If you look at doctrine, public affairs is portrayed as a coordinating skill or relevant activity. It is not often seen as an offensive weapon or enabler that the military can use. IMI on the other hand, is a useful acronym for psychological operations. Also known as PSYOPS or perception management, this warfare area has a long and distinguished military history. It has successfully been used by armies throughout the world to create conditions mutually advantageous to combat conditions. It has also been discussed previously to describe the importance of counter-terrorism operations.

A highly sought after capability by military forces, PSYOPS are not a property normally associated with the State Department and the United States government. In addition, public affairs officers are often loath to associate themselves with PSYOPS in order not to "taint" themselves. This is because public affairs officers are always supposed to tell the truth and they should not be seen as trying to manipulate any audiences. PSYOPS on the other hand is all about trying to manage the perception of people, especially the adversaries' mind. As demonstrated in Operation Desert Storm, a properly conducted PSYOP campaign can be a huge force multiplier, inducing thousands of Iraqi soldiers to surrender to coalition forces. Thus, the use of information to manipulate the adversaries' mind goes directly against many of the principles inherent in the public affairs profession. Yet the two disciplines have many similarities and if coordinated correctly, there are huge gains to be made by an organization that integrates information across the board as a part of an overall campaign.

What was the Clinton Administration attempting to do with IPI?

Thus stated, IPI is the Clinton Administration's attempt to not only combat negative propaganda by other nation-states but to also show in a truthful and united front, the policies of the United States. As a policy, it is designed to:

- Prevent and mitigate foreign crises around the world
- Collect and analyze foreign public opinion on issues vital to the United States
- Enhance the use of information assets

As mentioned earlier, public diplomacy is not new. An important factor of United States policy in the Cold War, information was disseminated throughout this period to foreign audiences by television and radio broadcasts, in a form of state-to-state dialogue. And we were not alone. Nations throughout history and to this present day have tried to use information to influence other countries as well as their own citizens since time immortal. How successful they were in those attempts often depended on a number of factors including cultural and psychological bias' as well as their means and methods of technology used to transmit that information.

Therefore as envisioned by its writers, PDD-68 is important because it is an attempt to develop another tool that can be used in shaping and preventing complex contingencies. As outlined in their earlier policy of PDD-56, the Clinton Administration recognized that they needed to do a better job of promulgating the truths about the United States to the world. While public diplomacy had worked relatively well in the Cold War era using USIA officers and policies, the environment had changed drastically in the last decade. Without the overwhelming

threat from the Soviet Union, that agency had lost much of its raison d'être and thus by the late 1990s, there was a move afoot to absorb the independent agency into the State Department. Likewise, the incredible advances in technology and the explosive growth of NGOs have drastically changed the methods of state-to-state contact over the last few years. Therefore, methods that had been effective for conducting public diplomacy during the Cold War were no longer considered viable in this new era.

With the promulgation of PDD-56, the Clinton Administration was attempting to develop an organization that could form in a crisis and help could coordinate across the interagency and coalition boundaries to help prevent more debacles like the massacre in Rwanda. There was a belief that an EXCOMM would develop the trust and mutual understanding among the key principals and deputies of the executive branch. While communication and compatibility are essential ingredients, the ability to promulgate that information to the world was another one as well. If the United States could prevent contingencies by using information to shape the environment, then that would help out the United States government in many ways. PDD-56 is consistent with the NSS and current DOD doctrine, specifically the NMS and IO, as outlined in JP 3-13. These documents stress that with the downsizing of the United States military forces in the last decade, it is imperative that attempts be made to minimize the need to deploy them around the world. If crises or contingencies can be contained, minimized or perhaps even avoided through the skillful use of information, then that is usually the preferred option. However, PDD-56 is limited in the fact that the EXCOMM is only stood up at the start of a contingency. What was really needed was a standing organization, one that could use information in the pre-crisis phase to shape the environment and perhaps prevent a crisis from ever occurring. That was the rationale and grand theme for the PDD-68.

Therefore IPI is an outgrowth of the earlier doctrine and is in fact, a required follow-on piece to the *Managing Complex Contingency Operations Policy*. It was written to fill that void for dealing with foreign audiences that was addressed by PDD-56. The objective was to improve the ability to prevent and mitigate foreign crises while at the same time promoting understanding and support for United States foreign policy initiatives around the world. Specifically, the Clinton Administration wanted to avoid mistakes like those in Bosnia and Rwanda that may have been prevented if an effective information policy had been in effect. A device or group was needed to address the misinformation and ethnic incitement that had characterized these two regions. This group had to be interagency in character, in order to maximize its ability to develop a sound program, and it is called the interagency IPI Core Group (ICG).

PDD-68 is not a stand-alone product but instead part of a larger product. The broader theme for IPI is PDD-56 *Managing Complex Contingency Operations*. There are a lot of components that are involved with this process and IPI is only one of them, yet the idea was to form a group to attempt to integrate information as part of the interagency process. The founders of IPI wanted to make IPI a standard way of doing business, a regular part of the political military plan, not an "extra" that was added on at the last minute.

Why has IPI been "less than successful?"

Why has the State Department and other interagency organizations been slow to adapt the IPI structure? Mainly because there are two important sensitivities connected with PDD-68. First off, because the ICG has a connection with the intelligence community through the National

Intelligence Coordinating Committee, the information group can draw on foreign intelligence sources. That means at the present time, they are one of the few activities that has access to all-source intelligence. Therefore the ICG will be in a very unique position, although other units like the State Department Intelligence Bureau also attempts to conduct all-source intelligence analyses through open-source material. The second sensitivity involves the interface between Public Diplomacy and Public Affairs. The professionals that conduct Public Affairs are very wary of both IPI and PD in general, and the PDD-68 initiatives in particular. There is concern that the PA community could be tainted or affected by a close association with these other warfare areas. This line of reasoning was explained in two Washington Times articles that theorized that PDD-68 was a Trojan horse vehicle to PSYOP the American public favorably to various Clinton Administration foreign policy initiatives.

These are all noble ideas. Nevertheless, it still does not detract from the concept that IPI involves PSYOP elements, which concerns many people. As reported in the Washington Times article "Professor Albright goes live" by Helle Bering (8/4/99), the State Department has not given up on educating the American public. The author indicated that she believed that PDD-68 was just the latest attempt by the Clinton Administration to educate or "persuade" the citizens of the United States. The stated purpose of the IPI system was to coordinate and vet all PA output from the different United States government agencies. Clearly that is an unrealistic requirement and far from doable, but because it was reported in the Washington Times, it gained credibility.

During the Cold War, most American citizens understood who the enemy was and why we were conducting military operations or foreign policy initiates. When the United States government strayed from the course of Containment or belabored the point too long as in Vietnam, public opinion would rise up to influence the politicians. However, the post-Cold War era is different. The United States has no peer competitor and therefore much of the American populace does not understand why the government is involved in these small nations in Africa or the Balkans. Therefore the State Department often feels that it must demonstrate why this particular cause is important or is need of attention, vice that many others to chose from. Moreover, it is often a hard sell.

The State Department can only do so much educating of the American people. By law, the Smith-Mundt Act of 1948 prohibits the United States Government from targeting Americans with information that is aimed at foreign audiences, i.e. you cannot conduct public diplomacy on your own people. While that may have been relatively easy to separate via different media channels 50 years ago, today with the merging of the telecommunications, computers and media technologies, it is much harder to ensure that information aimed at foreign audiences will not be consumed by the American populace.

Detractors of IPI do not believe that the United States government is trying to abide by the Smith-Mundt Act and instead state that PDD-68 is merely a tool to propagandize the American public. What this and the other critical article in the Washington Times fail to realize is that the Clinton Administration, while made up of some political appointees, is mainly supported by a vast bureaucracy of civil servants and professional government officials who do not owe their allegiance to any particular party. They are the backbone of the United States government, and for good or bad, they will survive any political administration. The civilian bureaucracy is divided into many different agencies and activities and as is typical throughout the world, these departments all compete for budgeting dollars with each other. Therefore, in a

sense, within the interagency process it is extremely difficult to reach consensus much less to produce this Orwellian conspiracy against the American people. The career civil service personnel are often influenced more by internal department politics than the larger domestic agenda and therefore not only will it be hard to manipulate them, they also will be acting within an organizational and bureaucratic context.

For an IPI campaign to succeed, you cannot wait until hostilities have begun but instead you must begin earlier, to mold and shape the political environment. Unfortunately in the case of PDD-68, they probably meant that IPI was written to the lowest common denominator. The policy document that ended up being published was very vague and contained no lashup, or mechanism to coordinate with the Department of Defense. PDD-68 right now is a concept without a structure. Although it is supposed to be a component of PDD-56, that policy document is only a process that is to be used in contingencies. What is really needed for IPI to work is a coordinating group that can meet all the time.[134]

However, the most important thing that PDD-68 has done within the last year is that it has created an interagency dialogue during peacetime. While this may seem as a relatively easy task, it is in fact not al all. By trying to force the government to be proactive instead of reactive, IPI may have more success than many people realize. It is forcing staffs to try to integrate information into the TEP, as well as work the horizontal integration issues across the board. Who knows, maybe in the future, PDD-68 can even do what it was designed to do to look into the future at potential hotspots, and to use IO as a shaping tool.[135]

Conclusion

These four areas: CNA, Space, EW and IPI are the largest growth areas for offensive IO in the last three years. Yet, there are still many challenges to the successful application of IO for offensive operations. Since military planners still organize their staffs along operational lines and continue to think of military operations as either offensive or defensive, information operations are causing many to challenge these traditional conceptions. The need for increased integration and cooperation among the diverse members of the interagency community, as well as the private sector, academia, and others, will eventually force those within the DOD to come to terms with the limitations imposed by traditional military planning methods and procedures. The nation, which best develops a coherent national security strategy and thoroughly integrates both offensive and defensive information operations into all aspects of its diplomatic, informational, military, and economic policy will be best positioned to gain information superiority. In pluralistic democratic societies like the United States, the ability to develop such an approach may be illusive, given the many competing interests of all the players. Only time will tell how successful the United States will be in utilizing the offensive capabilities of IO in the future.

Chapter 5 - Organize, Train, and Equip

"*If a man does not know to what port he is steering, no wind is favorable"*

Seneca

IO Planning

Planning is the essence of military operations. Behind most military operations lie countless man-hours of planning and rehearsal. Military organizations at the tactical, operational and strategic level have organizational structures and detailed procedures for planning. These planning structures vary greatly in size and composition, but all have one thing in common, a desire to predict every possible outcome of an operation and to plan for every possibility. This chapter examines the utility of IO in support of peacetime engagement planning and in the deliberate and crisis action planning processes and discusses the DOD organization for IO planning.

Peacetime engagement is one of the principle missions of every regional CINC and this mission is derived from the United States' NSS. The December 1999 NSS states that peacetime engagement activities by the military, "…help to deter aggression and coercion, build coalitions, promote regional stability and serve as role models for militaries in emerging democracies."[1] The military accomplishes this mission through means such as forward stationing or deployment of forces, defense cooperation and security assistance, and training and exercises with allies and friends. Until fairly recently, the regional CINCs established their own direction for peacetime engagement in their respective theaters. This all changed in 1997 when the CJCS issued planning guidance to the regional CINCs directing them to develop multi-year plans for theater peacetime engagement.[2] Originally these TEPs were five years in length, but in 2000 they were lengthened to seven years.

The Chairman of the Joint Chiefs of Staff Manual (CJCSM) 3113.1, *Theater Engagement Planning*, published in February 1998, formalized the theater engagement planning guidance issued by the CJCS in 1997. This manual causes the regional CINCs to formulate their peacetime engagement strategies and to submit them for approval to the CJCS. Nowhere does CJCSM 3113.01 direct the CINCs to use an IO approach for peacetime engagement, but an IO strategy offers a logical means of accomplishing the CINCs peacetime engagement objectives.[3] Given that one of the principle attractions of IO is its potential to deter conflict, one would expect to see IO play a major role in the TEP process. In fact, this is not so simple. While a regional CINC may wield significant power in a theater or a country during a conflict, most of the authority lies in the hands of the United States Department of State during peacetime. It is therefore incumbent upon the regional CINCs to coordinate with the State Department and a host of other United States Government agencies when planning peacetime engagement activities, especially ones involving the employment of IO. In particular, a regional CINC's staff may find themselves coordinating information operations with any of the following organizations:

- The Drug Enforcement Agency (counter-narcotics)
- The FBI (counterintelligence)
- The DOE (nuclear weapons counter-proliferation)
- The DOC (foreign technology transfer)

Managing the details of an operations plan is becoming increasingly difficult, as

technology has multiplied the number of information planners involved in the operations plan. The pathway for the United States' military described in *The Concept for Future Joint Operations: Expanding Joint Vision 2010* describes how the United States must gain and maintain information superiority over its adversaries. Information superiority as you may remember consists of three components, information systems, information operations, and relevant information. Relevant information is "all of the information of importance to the JFC in his exercise of joint command and control. It includes information about friendly forces, the enemy, and the operations area. Therefore it is incumbent upon the J-3 to so organize the IO cell so it has the necessary balance of talent and expertise to sort through the profusion of information available to the average military staff today.

JP 3-13 provides little substance to guide planners in the integration of IO in the planning process. The joint planning process is documented in the manuals of the Joint Operations Planning and Execution System (JOPES). To incorporate IO into military planning, the DOD has added a number of special units and organizations as mentioned in Chapter 1. At the highest level, the Joint Staff J-39 provides guidance, direction and support of IO planning at the unified commands. Likewise, the IO cell at a unified command performs similar functions for any sub-unified commands, joint task forces, and/or service component commands subordinate to it. In addition, as covered earlier in the first chapter, all services have formed component IO or IW centers to support all aspects of information warfare. Although each differs in organization and mission, all provide support to IO and IW planning. The following discussion examines the approach each military service has taken towards IO and IW planning.

Military IW Service Centers

The Land Information Warfare Activity (LIWA) at Fort Belvoir, Virginia supports deployed Army units, both operationally and during exercises. LIWA teams support the Army Commander's goal of achieving Information Dominance with the other JTF components or organizations. LIWA's purpose is to provide Army commands with technical expertise that is not resident on the command's general or special staff, and to exercise technical interfaces with other commands, service components, and National, DOD, and joint information centers. When deployed, LIWA field support teams (FST) become an integral part of the command's IO staff. To facilitate planning and execution of IO, LIWA provides IO operational support to land component and separate Army commands, and reserve components commands as required. LIWA has had FSTs deployed in the Balkans since 1996 and has gleaned innumerable lessons learned.[5] The LIWA also provides the Army's Computer Emergency Response Team (CERT).

The Fleet Information Warfare Center (FIWC) at Naval Amphibious Base Little Creek, Virginia supports IO and IW planning for the Navy and the Marine Corps. The FIWC provides naval and joint commanders with deliberate and crisis action IO and IW planning support, ranging from strategic level planning through tactical execution. FIWC personnel are integrated into the staffs of numbered fleets, aircraft carrier battle groups, and amphibious ready groups with their accompanying Marine Expeditionary Units. The FIWC also provides the Navy's CERT capability. In addition to its headquarters in Virginia, the FIWC also maintains a detachment in San Diego, California to support operations in the Pacific.

The Air Force Information Warfare Center (AFIWC) in San Antonio, Texas supports IO planning in the Air Force. The AFIWC is part of the Air Intelligence Agency and currently

works for the Air Combat Command (ACC). The AFIWC reorganized its deployed structure into IW flights, which are assigned to numbered air force, air expeditionary forces, and air component command headquarters. The AFIWC is uniquely positioned to provide IO and IW support due to its being co-located with AIA and JIOC, mostly because the commander of the AIA also commands the JIOC. Until recently, the AFIWC provided the Air Force's CERT (AFCERT) capability. This has since changed as AFIWC has built a separate organization within the 67th IO Wing that actually commands the AFCERT.

The JIOC is the key organization in the DOD specifically designed to support offensive and defensive IO planning. Located at Kelly AFB in San Antonio, TX, the JIOC evolved from the Joint Command and Control Warfare Center (JC2WC). The JC2WC in turn evolved from the former Joint Electronic Warfare Center (JEWC), transitioning from purely EW to encompass C2W. It is the designated DOD "center of excellence for information operations." Falling under USSPACECOM, the JIOC provides the combatant commanders and JTF's with teams of information operations specialists. The JIOC also provides dedicated teams to each regional CINC and USSOCOM, while the remaining CINCs received matrixed support. These JIOC teams thus provide technical and operational specialists to support IO planning, operations, and exercises.

An additional command that is essential for IO planning is the Joint Warfare Analysis Center (JWAC) located in Dahlgren, VA. Normally teamed with the JIOC, these planners usually work in partnership with the CINC IO Cell to assist the CJCS and commanders of unified commands in their preparation and analysis of joint operational plans. Specifically, the JWAC provides combatant commands, the Joint Staff and other customers with information in order to carry out the national security and military strategies of the United States across the spectrum of operations. Falling under USJFCOM, JWAC also provides direct support teams to assist Unified Commands with planning and these teams usually work in conjunction the CINC's JIOC team.

IO Planning Tools

Moving from IO planning organizations, this next section reviews a number of IO planning tools that are currently available to the military operator. Computerized planning tools to support IO are ubiquitous. Many of these are legacy systems from C2W and do not fully support full-spectrum IO planning. A number are also stand-alone systems, however, there have been a number of attempts to develop software applications to support planning for all of the IO capabilities and related activities.

The IO Planning Tools (IOPT) is an advanced concept technology demonstration (ACTD) that has been ongoing at the United States Central Command since it was funded in fiscal year 1997.[6] However at this time, this program appears to be unfounded and will probably never go beyond the ACTD phase. Its original purpose was to demonstrate how IO planning, modeling and analysis tools can aid in the effective execution of a CINCs battle objectives. These automated tools were to provide capabilities supporting the planning, development, synchronization, deconfliction and management of an integrated IO campaign involving HQ Central Command's J3 staff and the CINC components. The ACTD also was supposed to support the modeling and analysis tools for the Integrated Air Defense System (IADS) target recommendation development that is aligned with CINC IO taskings. Finally, the IOPT ACTD was to provide automated capabilities to enhance horizontal collaboration between multiple

CINC components in planning and implementing CINC IO taskings. If fielded, the IOPT was also expected to facilitate synchronized J3 and component IO planning & operations activities. Yet as mentioned earlier, to date the IOPT is for intents and purposes cancelled.

The Information Operations Planning System (IOPS) program will develop, field, and sustain an IO planning and decision support capability for the US Air Force. The IOPS effort will include concept exploration as well as large-scale C4I system development, integration, and sustainment. This will include both systems architecture and planning tools and applications that must support all aspects of IO planning. The IOPS is planned to provide enhanced IO decision support capability, which must augment and interface to existing intelligence and operations systems.[7] Currently under development at AIA, IOPS developers are considering the feasibility of integrating an IO planning support application called the IO Navigator (ION) into the IOPS.

The ION is a new software application being developed at the JIOC. Amongst the services ION will eventually provide are:

- Developing IO and IW strategy
- Objectives and tasks
- Developing IO and IW target lists
- Creating synchronization matrices for the planning and execution of IO and IW
- Creating and inserting text for IO and IW annexes and appendices into operations plans using the formats found in the three volumes of the DOD's JOPES.[8]

ION incorporates a planning process called the Joint Information Operations Attack Planning Process (JIOAPP). The ION software was specifically designed to support this process. The JIOAPP methodology used in the ION software is derived from the strategy-to-task planning methodology discussed later in this book and is an important component of IO planning. A defensive planning process is currently under development.

Strategy-to-Task Planning

The RAND Corporation developed the strategy-to-task (sometimes called objective-to-task) methodology for the DOD. In this context IO and IW tasks may trace their origin all the way to the NSS. Therefore IO and IW tasks are derived from a specific mission assigned to a regional CINC by the Joint Strategic Capabilities Plan (JSCP). To understand IO planning, it's essential to understand this linkage. The President publishes the NSS, which as mentioned earlier establishes broad strategic objectives to protect the national security interests of the United States and describes the President's strategy for accomplishing these objectives.

The NMS is the DOD's plan for implementing the NSS, and flowing from the NMS are two key documents: the UCP and the JSCP. The UCP provides guidance to all unified combatant commands, establishes their missions, responsibilities and force structure, delineates the general geographic area of responsibility for CINCs and specifies responsibilities for functional commanders. Complementing the UCP, the JSCP provides guidance to the combatant commanders and the Joint Chiefs of Staff to accomplish tasks and missions based on current military capabilities. It apportions resources to combatant commanders, based on military capabilities resulting from completed program and budget actions and intelligence assessments. The JSCP provides a coherent framework for capabilities-based military advice provided back to the President.

Each CINC develops a strategy explaining how he intends to accomplish his assigned missions. This is called a theater strategy for CINCs or a TEP. The theater strategy enumerates objectives the CINC wants to accomplish in the execution of this strategy. For every objective the CINC develops, the staff planners will develop supporting IO objectives and sub-objectives. The planners then associate available IO capabilities and related activities with each IO sub-objective. Finally, each IO capability and related activity is assigned specific tasks to support the accomplishment of the IO sub-objectives. These tasks, after much coordination and orchestration by the staff, eventually appear on a daily IO task execution list. Thus, the daily IO tasks, if properly planned and formulated, are directly linked to the NSS.

Tying Together Strategy-to-Task Planning and IO Planning Tools

With an understanding of strategy-to-task methodology, it's easy to see the logic in the JIOAPP methodology used in the ION software. The JIOAPP consists of five steps for planning offensive IO and IW. It facilitates planning at the unified command level and at subordinate components or joint task forces. The first step is identifying the IO objectives and sub-objectives. This flows from the mission analysis process, during which the staff develops a restated mission and the CINCs objectives. As stated previously, the CINC's objectives answer "what" the CINC desires to accomplish. For the purpose of our book, we will focus on the IO sub-objective to "lower the morale" of our adversary.

The next step of the JIOAPP is generating IO tasks. These will be very broad tasks associated with the individual IO capabilities and related activities available to the planners. For example, lets look at only the PSYOP tasks. Elements of a campaign may be to conduct a leaflet campaign, conduct PSYOP radio broadcasts and to place PSYOP messages in the foreign press, which may be done by having a third party purchase column space in newspapers, magazines, etc. Then the planners identify IO targets associated with the individual IO tasks. Looking again at the PSYOP tasks, our example identifies the Redland military forces, national politicians, and chief executive as PSYOP targets. In the fourth step, the planners associate IO sub-tasks with each IO target. In our example, the PSYOP campaign will target the Redland military forces with leaflet drops from MC-130 aircraft, Commando Solo radio broadcasts, and public information articles on U.S. military capabilities places in selected foreign newspapers, magazines and other media that one might expect members of the Redland military forces to have access to. Finally, the planners conduct an equity review of the IO attack plan. This include an analysis of the operational gain versus the potential intelligence loss, electromagnetic frequency deconfliction, an OPSEC review of the plan, and other considerations as determined by the command. The JIOAPP utilization in the ION software is an excellent example of how the strategy to task methodology is adaptable to computer-based IO planning tools.

IO and JOPES

The DOD conducts all joint planning within the framework of the JOPES, which is a system of policies and procedures, combined with automated data processing systems, that is designed to provide joint commanders and planners with a method for planning joint operations. JOPES is well suited for strategy to task methodology and ideally supports IO and IW planning. There are three basic manuals in JOPES, and at the time of this writing, they were undergoing extensive revision.

JOPES Volume I (CJCSM 3122.01) describes the DOD planning policies and procedures. It offers broad guidance and background information and is essential reading for all IO planners. *JOPES Volume II* (CJCSM 3122.03) establishes formats and offers guidance for preparing an operations plan (OPLAN). This volume has a secret supplement entitled CJCSM 3122.04. The final basic manual of JOPES is CJCSM 3122.02, *TPFDD Development and Deployment Execution*.

As mentioned above, *JOPES Volume II* provides the basic formats for the various annexes and appendices in an OPLAN. The following section describes those portions that are important for IO planners. There has been much discussion in the IO community regarding the need for a separate IO annex to each OPLAN. Thus far, the general consensus is that since IO is an integrating strategy, it should be integrated throughout the various portions of the OPLAN, not lumped into a single annex. The wisdom behind this becomes clear when we look at just how many annexes in an OPLAN must address IO. Theoretically, each annex should address both the offensive and defensive aspects of IO. A complete description of JOPES IO appendices, annex's and tasks are enclosed at the back of this book.

OPLAN, TPFDD and the IO Cell

Planners generally view the development of time-phased force deployment data (TPFDD) as a logistics function. However, it is important for IO planners not to overlook this aspect of JOPES. The TPFDD is a database containing time-phased force data, non-unit related cargo and personnel data, and movement data for an OPLAN. It is important for IO planners because certain IO capabilities and related activities are specifically associated with units. As an example, most of the active component CA capability in the DOD resides within one unit, the 96th CA Battalion. Likewise, most of the active duty PSYOP capability resides in the 4th Psychological Operations Group (POG) and both of these units are based at Fort Bragg, North Carolina. To a lesser extent, the same holds true for units providing EW support. IO planners will be interested in the arrival times of CA, PSYOP and EW units in theater, as their arrival will signal the IO planners as to when a particular IO capability or related activity will become available for employment. As a general rule, commanders will want CA, PSYOP and EW units available early in a deployment. IO planners may need to leverage the system to ensure these units are included early in the flow of forces into a theater.

Finally, all of planning staff's efforts will eventually result in an OPLAN. But the work isn't over yet. The most important part of any operation is the execution. From the planning that was conducted during the OPLAN development process, the IO cell will have a multitude of tasks that must be executed in a highly coordinated, synchronized and time-phased sequence in order to support the accomplishment of the CINC's objectives. This is accomplished by producing a series of mission synchronization matrices through the course of the planning process. Initially, one matrix is produced depicting the major functions of the IO capabilities and related activities for each phase of the operation. Eventually, as more details develop, the IO planners will prepare separate synchronization matrices for each IO capability and related activity. Again, as more details are developed these matrices will be transposed into daily execution checklists for each IO capability and related activity. Daily execution checklists will be reviewed at each meeting of the IO cell and revised as necessary as the operation proceeds.

So planning becomes the life of the IO cell. Even as a plan is executed, the cell must

constantly revise and adjust the IO particulars to ensure that the CINC's objectives are met. The high degree of detail required to successfully execute IO places the onus on every "IO warrior" to take full advantage of the information technology available to assist in planning. As new computer-based IO planning tools emerge, it is essential that these be integrated into the planning process. Additionally, published planning procedures and guidance are essential to ensure that the diverse IO planning effort conducted throughout the staff is coordinated and complementary. Just as sweat in training prevents blood in battle, sweat in planning will help prevent the unexpected during execution.

IO is considered a conceptual approach to military planning and operations, including their support functions, rather than a new area of military specialization. IO in current doctrine is the responsibility of operations staff assisted by other functional groups. Planning staffs also need to consider IO as part of future operations when conducting deliberate and contingency planning. At present within Joint headquarters, a dedicated operations staff member is normally responsible for IO. At the tactical level, IO responsibility is met by command direction, awareness of IO, and representation on formation level IO planning cells if required. The manner by which the IO planning function is met must be appropriate to the headquarters and ensure that IO are considered and integrated with the maneuver plan.

IO has the following staff responsibilities:

- Operations: Inclusion of IO in current operations plans with policy on IO, deconfliction and synchronization of IO including direction of IO related assets on behalf of the commander and providing friendly force updates for the commander’s situational awareness
- Plans: Inclusion of IO in future plans and contingencies and developing long/short term shaping strategies for the operations staff to implement
- Intelligence: Through the joint intelligence preparation of the battlespace process provide intelligence on adversary critical vulnerabilities that may be exploited by IO including advice on the threat from IO and countermeasures as well as targeting intelligence on the specific characteristics of selected targets and technical control of intelligence collection operations and activity (including counterintelligence operations)
- Communications: Coordinating the electromagnetic spectrum management and the management of friendly communications architecture with technical control over communications assets and their security, as well as technical control of information assurance measures and advice on the vulnerability of friendly information systems, given input from intelligence processes
- Logistics: Provide for IO related assets and resources as well as advice on logistics infrastructure and plans, given input from intelligence processes

IO planning as mentioned earlier needs to be involved at the earliest stages of a potential conflict. At the strategic level, military IO planners need to engage relevant government departments as early as possible to develop overarching shaping strategies. At the theater level, IO planning must be integral to the planning process, which brings a range of activities that can be synergized within the traditional maneuver of major force elements to achieve decisive points. IO is not a separate planning activity, nor can IO be considered as a separate maneuver element, force element or battle operating system.

IO as an Integrating Strategy

Commanders will remain central to the operations planning process. Their guidance on IO will naturally include an assessment of how the commander views friendly and adversary vulnerabilities. This may translate into a priority of targets and priorities of effort for scarce resources. The commander may also indicate the level of acceptable risk to be sustained and the perceptions to be manipulated. Commander's guidance may also include direction as to the deception target and deception objective and those key elements of information, personnel and materiel to be kept secure. Central to the development of commander's guidance in relation to IO and targeting is the continuing balance between the implications of the Laws of Armed Conflict (LOAC) and the principles of war. Offensive IO will be conducted as a legitimate response, and hence, the selection of targets, the means of attack, the level of force applied, and the risk of collateral damage will all be in accord with national and international law. Development of protocols relating to emerging IO disciplines is expected to occur in the next few years.

It is the nature of IO that much of the effort to achieve related effects can be detracted from or confused by other IO-related activity. For example, thematic based message efforts such as deception, public information, operations security, and PSYOPS often conflict. Therefore, the IO planner will be required to ensure that each activity works to achieve suitable outcomes in accordance with set priorities. Moreover, IO activity can often conflict with other efforts such as targeting, maneuver and the desires of subordinate commanders. Again the IO planner will seek to plan for and avoid such conflict. As well as being deconflicted, each IO effort must be synchronized with other IO efforts and wider operations efforts to achieve maximum effects. This process is fundamental to IO and is captured on a synchronization matrix or on a time/event-sequenced chart. One of the most difficult features of IO planning and staff-work will remain evaluating the effectiveness of IO measures. Increasingly, commanders will demand advice on the levels of risk of collateral damage and will need to be provided with a clear evaluation plan. The basis for evaluation lies in establishing and monitoring measures of effectiveness. It includes: maintaining an effective reporting system to identify degradation in information assurance; steerage of the efforts of the intelligence system; linkage to the combat assessment aspects of the targeting process; and integration with the security validation and reporting process. During planning, the measures of effectiveness for each IO element will need to be defined. These are subsequently further developed and monitored as part of current operations. Measures of effectiveness are considered in an offensive context (for the targeting outcomes of offensive IO) and in a defensive context for the security aspects of defensive IO. These determinations ideally rely on such data as mathematical models, ongoing practical weapons testing and historical analysis, all of which combine to enable staff to predict the effectiveness of IO activity. In PSYOPS this process may include 'pre-testing' types of product to guarantee an appropriate effect.

In the future, when incorporating IO into operations, commanders will be offered an expanded range of options which may include an ability to deceive, degrade, destroy, manipulate, or confuse an adversary's information and information systems. Hence, IO forms part of the wider operations process that feeds targeting related processes and activity. While recognizing the IO input to operations planning, the majority of the IO planners' daily work is related to current operations and hence such staff officers usually resides in the operations area of headquarters. Especially in cases where a TF is operating independently, an IO cell of specialists

and involved parties is required to regularly meet to assist in the prosecution of IO staff responsibilities noted above.

Legal Issues Connected with Information Operations

Throughout this book, the message is clear that the capabilities, opportunities, and threats involved with information operations are significantly different than have been the case in the past. It is also clear that, in many cases, the legal landscape is uncertain. Domestic laws within the United States and in other nations are changing in an effort to strike a balance between the needs of the law enforcement, national security and business communities and the civil liberties of the populace. In many ways the situation is a hydra – rather than settling issues, each inquiry into a legal matter raises more questions. Both as a matter of law and of policy there is uncertainty as to where IO fits. In each case, the question is asked whether what is being faced is a criminal act or a national security threat. It is not clear whether what is involved is a new form of mischief, a new example of the keen competition between businesses and nations, or at some point, an act of terrorism or an armed attack.

Over the past decade, the legal community has been paying increasing attention to the field of information operations. What used to be limited to discussions of computer crimes and more traditional forms of electronic warfare now looks at all of the new capabilities and techniques and attempts to divine the legal constructs which apply. In this attempt, we see two perspectives on the issues. First, what are the laws, policies, and rules of engagement affecting the potential use of IO concepts and tools in wartime, in operations other than war and during peacetime operations? This is the perspective most often voiced by the client, the military commander and his staff charged with execution of a discrete mission. Just as importantly in the long run, though, is the second perspective, namely that of the legal community and policy makers attempting to develop a comprehensive IO capability and strategy. From this perspective, the important question is how must the law evolve to strengthen United States interests, policies and capabilities with regard to IO?

An Overview of the Legal Landscape

In the space allotted for this chapter it would be impossible to cover the landscape in depth. Other sources exist which address these questions in great detail.[136] What we will do, however, is sketch the outlines of the legal issues in terms of the underlying principles which operational planners need to take into account in their planning – issues which must then be presented to the chain of command and their legal advisors so that these issues can be resolved to some degree before the planning concludes and execution of the mission begins. In this regard, the process now in place for developing the Rules of Engagement (ROE) for an operation allow the means by which operational planners can address the legal questions which may arise. Staff officers will encounter issues of both international and domestic law in planning any operation. What is important for the planners is an understanding of the underlying principles and issues rather than the specifics of the legal analysis.

International law addresses the relationship between nation-states and, rather than a collection of rules, should be seen as a system by which the international community seeks a stability of expectations in their interactions. As with any other system of law, international law represents a struggle between the individual sovereign interests of the members of the

community. The principle that each community member has certain sovereign rights and interests which can and should be advanced is balanced by the principle of reciprocity – that successful existence within a community requires members at times to subjugate individual interests so that the collective will can be advanced and through this coexistence, an environment created which fosters individual sovereign interests.

The basic document which governs this reciprocal effort in the current international legal environment is the Charter of the United Nations. It was written to advance three interests:

- International peace and security
- International human rights
- Economic and social development[137]

Military operations are generally raised in the context of protecting international peace and security and it is from this context that the discussion will flow. The generally accepted view is that the UN Charter establishes a balance between deterrence of aggression and promotion of defense. In this regard, Article 51 of the Charter recognizes the inherent right of a nation state, or a collective group of states, to protect their interests against armed aggression. The recognition of the inherent right to use force defensively is balanced by the prohibition contained in Article 2(4) against the aggressive use of force. This balance, recognized well before the Charter was developed, can be accomplished unilaterally by individual states or groups of states or on behalf of the international community as a whole by the Security Council.[138] Established as the enforcement arm of the international community working through the United Nations, the Security Council has a great deal of authority. [139] Because of this, the Security Council can authorize action which would constitute a violation of Article 2(4) if undertaken unilaterally by a state or group of states.[140] If the Security Council does act in a given circumstance, all member nations are obliged to support that effort – there can be no neutrals in the case of a Security Council enforcement action.[141]

Peacetime Treaties Impacting IO

The analysis above is important, not simply in the decision whether or not to employ the use of force in an international context, but also in determining whether or not there are treaty obligations which should be taken into account in IO planning and execution. In this regard, there are two basic types of treaties involved – those such as the 1982 Law of the Sea Convention or the Outer Space Treaty, which address operating in a particular environment, and those such as the various International Telecommunications Conventions, which address the use of a capability. Both sets of treaties contain language which IO planners should be prepared to address. First, these treaties generally require that use of the environment or capability be reserved for "peaceful purposes." Secondly, each of these treaties contain some version of a requirement that a party operating within the environment or using the capability do so in a manner which does not interfere with the legitimate use by another.[142] Clearly, military operations at any scale of intensity implicate these provisions. For many, the mere use by the military for the conduct of military operations seems to violate the treaty provisions referred to above. Similarly, the use of certain capabilities (jamming for instance) are designed to deny others the use of a capability or environment. Under the aggression/defense analysis described above, the proper legal approach is to ask whether the operation being planned is being undertaken for a purpose or in a manner which is "consistent with the principles of the UN

Charter." If so, then the action is generally going to be permissible, at least in concept.

This is not to say that this approach resolves all potential issues of treaty law. There may be other issues which arise from our treaty obligations. Many of these treaties do, however, contain some sort of exemption for military communications, requiring compliance with the treaties "to the extent feasible." [143] Finally, it is generally accepted that treaties such as the various telecommunications pacts are intended to guide peacetime relations and would be suspended during a period of armed conflict. [144] Of course, as our military continues to be tasked with Military Operations Other Than War (MOOTW) it will not necessarily be clear whether the particular operation qualifies as an armed conflict. In this regard and based on the discussion above, one critical question for planners at the operational level to ask of the chain of command would be the extent to which treaties such as telecommunication conventions will be considered to apply in the context of the planned operation.

In addition, another treaty which will have to be taken into account in the planning stages of an operation will be any Status of Forces Agreement (SOFA) or comparable diplomatic arrangement which may have been made concerning the basing of troops and operations in another nation. These agreements may limit the operations which can be conducted from within the host nation or be launched from the host nation, they may require coordination in the planning and execution of operations and will also affect the imposition of criminal justice on visiting forces. If civilian technicians will be a part of the IO cell, their status needs to be considered. Host nation laws will have to be considered, much as United States domestic law is taken into account, when operating from within the nation's borders. Again, these factors will vary from situation to situation and should be considered in the early stages of planning in order to avoid distraction at a later time.

Law of Armed Conflict

Ultimately discussions on legal issues connected with the planning and execution of IO touches on the Law of Armed Conflict (LOAC). At first blush, we are faced with a situation which will require the application of traditional LOAC principles to a new set of capabilities and threats. From the perspective of the operational planner, the issues need not be that different, again so long as the underlying principles remain the focus. All of the LOAC boils down to a societal balance between two objectives. First is the legitimate need to protect the ability of a sovereign, acting through its military commanders, to use force in order to successfully accomplish legitimate military objectives. The second is the equally legitimate need to protect the innocent from unnecessary suffering. All of the LOAC reflects the struggle to strike this balance in the context of differing societies, cultures, and levels of conflict. Each advance in warfare technology has resulted in an evolution of how these principles are applied. [145]

The principle of distinction requires a commander to be able, in his choice of targets and of weapons, to be able to distinguish between combatants and other legitimate military objectives and civilian objects. The principle of necessity requires the commander to be able to demonstrate a definite military advantage in the contemplated action. The principle of proportionality requires the commander to consider the effect of the attack and the weapons used on the safety of civilians and other noncombatants.[146] These interrelated principles suggest the areas of concern in using IO capabilities or preparing to defend against IO threats.

It is also important to note that the ground rules by which these principles are evaluated

differ significantly. The United States considers legitimate military objectives to include combatants, defended places, and those objects which, by their nature, location, purpose or use make an effective contribution to military action.[147] Clearly military targets are simple in this regard; other infrastructure, including infrastructure relied upon by the civilian population, is more problematic. Many of our allies have adopted the Protocols Additional to the Geneva Conventions. These set forth a more narrow definition for military objective by adding the requirement that the total or partial destruction, capture or neutralization of the objective must offer a definite military advantage.[148] Other language contained in the relevant sections of Protocol I clearly reflect an unwillingness to countenance the attack of infrastructure and other objects which, although arguably part of the war sustaining effort, are not a clear part of the adversary's war-fighting capability. While the United States takes the position that the definition contained in the Additional Protocol is reflective of customary international law, it also holds strongly to the position that infrastructure which indirectly but effectively supports and sustains the war-fighting effort may also be attacked.[149]

Much of the international community, then sees a fairly bright line between the legitimate targeting of war-fighting capabilities and the presumptively illegitimate targeting of infrastructure considered to be part of the war-sustaining capability. The United States takes the position that proper application of the balance between necessity and proportionality appropriately guarantees the safety of the innocent from unnecessary suffering – by seeking to the extent possible under the circumstances the least amount of collateral damage, so the argument goes, we maintain adequate flexibility for the military commander while protecting the innocent. Many others, though see the issue as a slippery slope.

However it could be argued, doesn't the very nature of IO capabilities help the United States resolve this issue? After all, a discrete IO capability is sure to be more discriminating and less likely to result in unnecessary innocent suffering than high explosives. To date, however that argument has not been persuasive. First, there is a lack of trust that these capabilities are in fact as discrete as the sales pitch suggests. We are often reminded that there exists a "law of unintended consequences", ie you never truly know what the effect will be until you use it, and in the current societal context, there is more comfort in reliance upon tried and true capabilities than in the use of a new capability without a track record.

Conversely, there is also the concern that even if the IO capabilities lived up to their billing, they represent a capability which we, as the most prosperous and technologically advanced nation on earth, enjoy and which other poorer nations do not. In this context, there is concern that the use of our very discrete weapon against infrastructure relied upon by the civilian community will legitimize that infrastructure as a target even by adversaries who must rely on much less discrete weapons. These adversaries would argue that they were using the best they had and so ought not be held responsible for the collateral damage which results. The solution for the international community is to ultimately tend towards a "lowest common denominator" approach to a greater degree. This unfortunately may in the end result in greater harm to the United States and its allies.

There are also a number of other issues that the LOAC regulates. One of these warfare areas concerns the use of deception. An ancient facet of warfare, new computer-based plans or media operations have not changed the basic rules of deception. [150] It still remains unlawful to target the civilian population as such with any weapon, whether that weapon is a high explosive

or a falsehood designed to cause confusion or civil unrest. In a similar vein, it is also unlawful to use a protected symbol or character as a means of deception. False identification as a medical or religious person, site, or other platform remains unlawful perfidy, regardless of the means of deception used.

Domestic Law

So far the discussion has been centered in the field of international law, identifying the context in which issues of the legitimacy of the use of force, of obligations under treaty law and under the LOAC must be considered in IO planning. But what of the field of domestic law? To what degree do domestic legal issues affect IO planning? In this area, there are two basic questions we ask.[151] First, does domestic law adequately permit defense of IO capabilities? Secondly, does domestic law restrict offensive IO operations and action taken in self defense? To answer to these questions, there are a number of major federal statutes which have been passed to protect national security, to protect the property of the private sector as well as the governments and to protect the privacy and civil liberties of the citizenry.[152] These statutes both provide the basis for prosecuting crimminals as well as the necessary checks and balances which our society feels are necessary to ensure against wrongdoing by the national security and law enforcement mechanisms.

In many ways, these checks and balances make the national security role more difficult. Those who are trained to act immediately in self-defense of their unit chafe at the requirement to use complex, cumbersome and time-consuming processes such as exist in the criminal investigative arena. And yet, these checks and balances are a reminder that the democratic processes are by design inefficient and this exists to protects, however imperfectly, against governmental tyranny. Throughout our history of criminal justice, the struggle has been to design structures which allow identification and prosecution of wrongdoers without infringing on the rights of those who have not done wrong. Even more than in the past, the use of the electronic environment has meant that attribution is the key and it is very difficult. First, we must recognize that the overwhelming majority of computer intrusions and attacks have been made for personal, rather than national gain. Added to this, the fact that the criminal investigative processes, though relatively slow and filled with procedural checks and balances, are nonetheless reliable and accurate in the long run. From these ideas, we can then understand the current DOJ perspective, which is to treat all intrusions/attacks as criminal unless clear evidence exists of hostile state involvement. This point should be a reemphasis of the lessons learned in the organization section of Chapter 1.

Because this is the perspective taken, great effort is being made to ensure that processes are streamlined. Taking analogies from other areas of the law, from decisions made earlier in other contexts, the DOJ is working to ensure that the courts and legislatures strike the most effective balance between efficient identification, investigation, prosecution and civil liberties. In his article *The Critical Challenges from International High-Tech and Computer-Related Crime at the Millenium,* Michael A. Sussmann, Senior Attorney for the Computer Crime and Property Section of the U.S. Department of Justice, notes that the Attorney General has identified four areas where progress is critical:

- First, the enactment of sufficient laws to appropriately criminalize computer and telecommunications abuses

- Second, commitment of personnel and resources to combating high-tech and computer-related crime
- Third, improvement in global abilities to locate and identify those who abuse information technologies
- Fourth, development of an improved regime for collecting and sharing evidence of these crimes, so that those responsible can be brought to justice[153]

In the planning of Offensive IO missions, planners have been similarly obliged to keep in mind that these statutes have clear requirements for approval/coordination, without which the planned action is very likely illegal. While the DOJ would in all likelihood be reluctant to prosecute a well-intentioned service member, the investigation necessary to determine the motive of the member and make this decision would represent a major distraction of resources and time. Not only domestic laws of the United States, but also host nation and target nation laws represent potential sources of distraction at the least or individual criminal liability at the worst. For example, Mr. Sussman theorizes that the situation could arise where a searching country took the view that a particular transborder search effort was permissible, while the searched country took the position that the execution of the electronic search is not only prohibited but constitutes unauthorized access to its computers and therefore is a criminal offense.[154]

The Solutions for the Operator: IO ROE Planning

It is clear from the foregoing and from the discussions found elsewhere in this book, that the legal landscape where IO is concerned is anything but certain. How then can military operators be expected to plan anything? That is where ROE and the IO planning process mentioned earlier in this chapter can help. ROE are defined as policies and procedures which govern the actions to be taken by United States forces during military operations. In general, ROE for peacetime operations or MOOTW are defensive in nature and address the decisionmaking process in determining the proper response to a Hostile Act or the demonstration of Hostile Intent.

It is important to keep in mind that the ROE are designed to be developed or modified by the NCA and the CINCs to fit the strategic and operational needs of particular events and operations. There is no desire for a "one size fits all" approach, but rather an iterative approach whereby the higher levels of the chain of command provide initial guidance and then respond to submissions from below to amplify, explain, modify or substitute other ROE provisions based on the needs of each component or subordinate division. The ROE requirements of the naval component will vary from those of the SOF component and each is expected to advocate for their required guidance. In this regard, over the last several years the operational planning process has spawned an ROE planning process which contemplates a cell – the "Knights at the Round Table" -- gathering to discuss mission tasks and requirements in order to ensure all operational views are explored and appropriate ROE is requested. The approval process set forth in the ROE ensures higher headquarters review and allows for interagency coordination prior to or as a component of any ROE approval. This process provides the CINC some measure of certainty in what response is permitted (or restricted) and under what circumstances.

This forum allows a process whereby the legal issues of IO can be identified and addressed. So long as the right questions are asked and incorporated into the ROE requests, a Commander will be provided much of the guidance he/she needs to determine what legal issues

are raised in IO planning. For example during one exercise, the following matrix was developed:

- Who/What is perpetrator/adversary? Criminal? Terrorist? State? Combination?
- Where is perpetrator located? U.S.? International waters/airspace? Third Country?
- State of perpetrator?
- What is impact on U.S.? Minor disruptions or Damage to national security?
- Who should respond? Law Enforcement? Host Country? Flag State? U.S. Military?
- Is Interagency Coordination required?

Summary of IO Planning and Legal Concerns

From the foregoing, we have discerned that IO is a legal political-military tool and a means of warfare and while existing law, regulations and policies and do not prohibit IO, the degree to which the law affects this warfare area will depend on the factual circumstances. Likewise the premium placed on planning for IO is crucial to the success of a campaign. It is incumbent upon the operator and planner to coordinate the various portions of IO methodology that were mentioned in this chapter. In addition, the importance of state custom and practice on the development of the law requires close involvement of legal advisors in development of IO capabilities and doctrine. Thus the ability of the IO Cell to properly plan and execute using IO tools and methodologies will be symptomatic of the success rate for a campaign. To conclude, if you get nothing else from this chapter, please remember that IO Cell and other staff planners must get early legal advice and integrate their operations in the master operations plan early on. That is the key to success.

Chapter 6 - Recent Information Operations Campaigns

"China has realized from the outcome of the Gulf War several years ago that unlike the human wave tactics of the agricultural age and the iron and steel warfare of the industrial age, air raids and precision strikes from long distances are decisive factors in the outcome of wars. It also realizes that information warfare and electronic warfare are of key importance, while fighting on the ground can only serve to exploit the victory."[155]

Jen Jui-Wen, Chinese Military Leader

This chapter is an attempt to update the reader on events and activities that have occurred over the last several years concerning IO, on real-world operations and how it has been used during this period. Specifically we will cover updates to Russian doctrine, IO aspects of the NATO coalition in Operation Noble Anvil in Kosovo, Chinese writings on IO, and most recently the Australia Defence Forces' campaigns in Bouganville and East Timor. This chapter will analyze these operations, focusing on the use/misuse or inaction of IO in each of these geographic areas.

The Growing Role of Information in Russia

The operations of the Russian military offers many fascinating examples of how important information has become in modern combat, especially with the glaring eye of global television ever present. Some of these changes are reflected in Russia's current national security documents that reflect an increased concern over information security issues more than earlier versions. The most recent (October 1999) military doctrine draft stated that the exacerbation of the information opposition/confrontation is an important feature of today's international context, a destabilizing factor used to achieve destructive military-political goals and affect current operations and the overall security environment. The draft included information-technological (attacks on computers, nets, infrastructure, etc.) and information-psychological aspects of the external threat to Russia, and stated that the greatest internal threat were actions to disrupt or disorganize the Russian Federation's information infrastructure.

The military-strategic features of the new draft doctrine focused on the features of modern war, namely indirect strategic operations, means of IW and the development of a massive information preparation (information blockades, expansion, aggression) operation. Confusing public opinion of certain states and the world community (aka IPI) and achieving superiority in the information sphere in either wartime or during the initial period of war were also other important missions. This new draft will elevate information security up to a basic military mission and ensure that information support remains a constant priority in the realm of information-economic principles.

The Concept of National Security that was approved by the Russian Security Council in October 1999 also addressed the country's information security and technology needs. The chapters titled "Russia's National Interests," "Threats to the Russian Federation's National Security," and "Ensuring the Russian Federation's National Security," included the following information specific interests:

- Observing the constitutional rights and freedoms of citizens to obtain and use information
- Developing modern telecommunication technologies

- Protecting the state information resource against unauthorized access to political, economic, science and technology as well as military information
- Preventing the use of information for manipulating the mass consciousness of society
- Attempts by a number of countries to dominate in the world information space and to crowd Russia out of the foreign and domestic information market
- The development of "information warfare" concepts by a number of states envisaging the creation of means of exerting a dangerous effect on the information spheres of other world countries, means of destroying the normal functioning of information and telecommunications systems, and means for the safekeeping of information resources or of gaining unauthorized access to them
- Implementing citizens' constitutional rights and freedoms for information activities
- Improving and protecting the domestic information infrastructure and integrating Russia into the world information domain
- Countering the threat of the initiation of opposition in the information sphere[156]

For Russian security specialists examining the national security environment on the verge of the new millennium, no issue is more important or more fraught with uncertainty than that of the current and future information environment. There are several good reasons why this is so. First, the free flowing, cross border exchange of information has offered people and organizations in the former Soviet Union unstructured access to fresh information never before available. This relatively unfettered environment permits citizens and decision-makers alike access to a wide variety of ideological, political, religious, and other information, to what was once forbidden by strict internal and external barriers. Second, the Russians now perceive that information itself has developed into a very important type of national or strategic resource. Compare this to the ideas that the authors discussed in the first chapter on the power of information. This is because information can potentially increase the precision and effectiveness of both traditional (missiles and rockets) and non-traditional (non-lethal and psychological) types of munitions which could thus upset parity in strategic arms. Third and finally, many Russians believe that a single global "information space" is emerging. If they are correct, then a country can exploit this space to alter the global balance of power.

Information Superiority

The Russians also believe that countries that possess information superiority may be more inclined than ever to employ military force. This is so because military objectives may now seem more attainable without significant loss of life and with no apparent risk. This is what for many Russians provides an explanation for the recent NATO intervention in Kosovo. The Russians have also realized that few legal restraints exist which that can regulate the use of an information attack. They are convinced that this actually encourages the growth of concepts such as cyberterrorism, which includes the use of terrorism against information processing systems. Finally, many Russians also understand that they are far behind in the global race for information superiority and are beginning to appreciate and fear the potential consequences. These three final reasons have prompted the recent Russian attempts at the United Nations that we mentioned earlier to limit the development of information operations procedures.

It is because of these considerations, that the subject of IW/IO has become almost as significant and important to Russian military planners as the issue of nuclear proliferation.

Russian theorists warn decision-makers not to submit to external forms of coercive information diplomacy. At the same time, subcommittees of the State Duma are commissioning studies on both IW and psychotronic warfare, while the Kremlin advisors and the security community are studying how information security issues may affect the country's political, technical, economic, and military policies. Some members of the Russian academic community are also engaged in studying the potential impact of information operations. The analyst E. A. Belaev, a member of the Russian State Technical Commission (under the President of the Russian Federation) believes that the *informatizatsiia* of society has led to the collection, processing, maintaining, and exchange of information between actors-people, organizations, and governments-in the single information space. As Belaev defines them, the most critical information technologies within this space are those that support:

- Governmental and military command and control organs
- The financial-credit and banking structure
- Command and control systems of various types of transport, energy, and ecologically dangerous industries (nuclear, chemical, biological, and others)
- Warning systems for emergency situations and natural disasters

Any underestimation of the information security of these systems, Belaev argues, could lead to unpredictable political, economic, ecological, and material consequences, and perhaps even turmoil. This analysis sounds very similar what the United States doctrine espoused in PDD-63 *Critical Infrastructure Protection*. It shows that nations today must protect their national information resources as strategic resources. In addition, the burgeoning access to global information networks such as the Internet have only underscored the necessity for protecting information resources from manipulation, corruption, deception or even outright theft. Furthermore, the Internet has also become an arena for potential conflict, especially over modern information concepts and unauthorized access to databases, witness the recent Solar Sunrise and Moonlight Maze incidents.[157]

Information Space

The recent conflict in Kosovo has done little to assuage Russian concerns about the significant role information will play in national security issues in the 21st Century. In the case of Kosovo, for the first time, the United States and NATO justified military activities by different geo-strategic principles other than simply national interests. In fact, writing in *Foreign Affairs*, Joseph Nye asked if it is possible to define interests conventionally in the information age, especially in light of humanitarian concerns, that due to the impact of the mass media, divert public attention away from real strategic issues. He summed up his views stating:

> The Canadian media guru Marshall McLuhan once prophesied that communications technologies would turn the world into a global village. Instead of a single cosmopolitan community, however, they may have produced a conglomerate of global villages, each with all the parochial prejudices that the word implies, but with a greater awareness of global inequality... all in the presence of television cameras and the Internet.[158]

Nye noted that the United States now has an interest in the use of outer space and cyberspace similar to the language once used by the British to express freedom of the seas. Notably, both are the channels through which words and ideas pass and democratic principles can be promoted.

However, the same medium of cyberspace has also been used to promote the advancement of democratic interests, such as humanitarian affairs to the level of a state interest at a startling pace. The Clinton Administration clearly appeared to agree with this assessment based on their justification for the use of force in Kosovo. In summary, Nye added, "a democratic definition of the national interest does not accept the distinction between a morality-based and an interest-based foreign policy."[159] From this it is clear that new geo-political principles are beginning to emerge in response to the influence of information.

This concept of information space has two dangers; first it can be used to monitor the state's information resources, thus becoming a conduit for information espionage, and second the information interaction can destroy or disorganize the information resources of elements of state structures. These effects can be realized in peacetime, especially if critical application systems are affected, thereby distorting or destroying information used for state management or decision-making. IO protection is what many theorists contend is the greatest promise for this new warfare area and also it's weakest link. Just as the Russian federation is attempting to develop information security, the current inability of the United States government to effectively capitalize on this capability will ultimately determine the true effectiveness of IO. Information space has no recognized boundaries, no institutions to protect state interests such as border or customs checks. The nation is transparent to information resources and analysts believe that one day, states may try to regulate the movement of information flows. This is because there are currently three ways that information impacts national security. The first is the security of vital state information resources and information systems, counters to which are being actively developed by countries all over the world. Second is the predominance of the information approach as the emerging primary scientific method of solving national security problems.[160] Finally, information can impact on a state or person's social awareness by manipulation of reality or fact, which in turn can have a deep impact on a state's national security decision-makers.

Russian IW Terminology and Theory

Many Russian theorists differ over the elements that comprise IW. Listed below are two of the different variants, both of which are the products or thinking of either theorists or practitioners who could be considered Russian information warriors. The first theory is from former First Deputy Minister of Defense and National Security Chief Andrei Kokoshin, who was ultimately responsible for research and development of these information systems. He divided information warfare into the following five subcategories:

- Electronic warfare
- Intelligence
- Communications
- Operational command and control systems
- Facilities for the protection of command and control systems against enemy influence[161]

The second theory comes from the civilian Russian Minister of Defense V.I. Tsymbal who wrote of additional categories. Information Warfare, in his view, must be considered as an integrated whole of systems working together that includes the following eight subcategories:

- Intelligence and counterintelligence gathering
- Maskirovka and disinformation
- The use of EW systems

- The debilitation of communications and scrambling of enemy data
- A determination of to which state a military objective belongs
- The destruction of an enemy's navigational support
- The use of psychological pressure on the enemy
- The destruction of enemy computer nets and software programs[162]

However whatever the number of groupings a theorist might believe in, just as in the United States, until IO has been extensively tested in combat, there will be continual doctrinal development.

General Major N. A. Kostin, Chairman of the Radio-Electronic Department, General Staff Academy has written a general theory of IW. He listed both *informatsionnoy bor'boy* and *protivoborstvom* as simply the same definition offered to the United Nations, "a form of struggle between sides that involves the use of special methods and means for impacting the information medium of the opposing side and protecting one's own side in order to achieve the assigned tasks." Therefore his goal was to provide information security for one's own side and lower the information security posture of the opposing side. If you compare that to the current United States military doctrinal for IO espoused in JP 3-13, you will notice many similarities. He noted that the battle over information is now so important that the battle for ore, oil and markets could fade in comparison. General Kostin added that the information struggle is a special category of war because it is an independent type of war, a component element of any other form of war, and it is waged constantly in peacetime and wartime. Once again, compare to United States doctrine.

Kostin also believes that political factors have the greatest impact on the substance of IW, driving their goals, tasks, and issues. This idea is comparable to the development of PDD-68 by the NSC and State Department. Therefore it is the political factors that also determine the means, methods, and characteristics of conducting the battle, its scope and duration, and also provide the necessary material support and financial resources. On the other hand, economic factors determine the scientific and technical development of the computerization of society and the state. Kostin has described information factors as influencing both the political and economic readiness by determining the scope of the struggle, the procedure and methods of its conduct, and the capabilities for utilizing them when influencing the enemy's information environment.

The logical elements according to Kostin's general IW theory that form the foundation are categories, laws, patterns, and principles. Categories objectively reflect the essence and core characteristics of the most important manifestations of IW. They also represent a body of military-theoretical thought that includes general terms such as information and IW, and in particular terms such as protecting information and attacking information. Categories can reflect the structure, substance, and requirements of IW. The laws of the materialistic dialectic also present themselves as well, according to Kostin, as objective laws and patterns of military activity valid for IW. These include:

- The law of the defining role that politics plays in IW
- The laws on the course and outcome of war and IW

These laws depend on the economic, socio-political, scientific-technical, and military capabilities. Recognizing the patterns that are inherent in IW are where the current primary efforts have been conducted. Therefore the effectiveness of IW is determined by the proportionality among the goals, tasks and systems used, including means available, which take into account the enemy's countermeasures.

Informational-Psychological

Probably the most interesting and neglected Russian element by Westerners is the information-psychological component of IO. The Russian military excels in the study of these areas especially over Western theorists. To date, the United States has not conducted extensive analysis in this area of IW except for those personnel involved in psychological operations. On the other hand, the Russia military scientists have been studying not only the ability of information warfare to affect the values, emotions, and beliefs of target audiences (traditional psychological warfare theory), but also methods to affect the objective reasoning process of soldiers. That is, Russia is interested in ascertaining how to affect not only the data-processing capability of hardware and software but also the data-processing capability of the human mind.

Three books published in the Russian Federation during the last two years serve as an example of this fixation on the mind. Endorsed by the State Duma's Security Committee, the first book was appropriately enough entitled *Informatsionnaya voina* (Information War).[163] This book examined how to manipulate the mind by toying with the algorithms (to include how to model them) that define human behavior. Humans, the author noted, like computers can have a "virus" inserted in their information system (reasoning process) if the proper algorithms of mental logic can be affected. The authors dubbed this human information virus a "psycho virus," which according to mathematical formulas could perhaps be inserted as a "suggestive influence" to alter the mind's algorithms or prevent objective reasoning. The second book, entitled *Psikhotronnoe oruzhie i bezopasnost' rossii* [Psychotronic Weapons and the Security of Russia][164] bore the endorsement of the State Duma's Information Security Committee. It was co-authored by Major Vladimar Lopatin, the Chief of the Information Security which is a subsection of the Security Committee of the Duma.[165] Lopatin and his co-author V. D. Tsigankov, defined psychotronics as an inter-disciplinary area of scientific knowledge, which when mediated by consciousness and perceptual processes, investigates distant (non-contiguous) interactions among living organisms and the environment. Another book that was recently published (1999) handling information-psychological problems was titled the *Secret Weapons of Information Warfare*. Focused squarely on the psychological impact on the mind by information issues, the chapters of the book are listed below:

- Basic directions in the Development of IW under Modern Conditions
- Understanding Phenomenology in Man and Controlling his Behavior
- Education on the Use of Psycho-Physical Weapons
- Methods for the Precise Orientation of Covert Effects on the Human Psyche
- Psychotronic Means of Subconscious Effects on the Human Psyche
- The Integral Method of Psycho-Physical Weapons

These two books plus another book *Psychotronic Weapons and the Security of Russia* also written by Lopatin and Tsigankov are part of a series known as the "Informationization of Russia on the Threshold of the 21st Century." What is important here is that these three books underscore the Russian belief that informational and psychological matters should be of concern to civilian and military alike as valid subjects for close scrutiny and that their effects, both positive and negative can and should be experienced both in peacetime and wartime. Colonel Igor Panarin of FAPSI, speaking at a conference in 1997, stated that there is a need in Russia to develop information-psychological subunits in government and military directorates. The role of these departments would be to develop strategic and operational measures to prevent or

neutralize attempts to control the psyche of Russian society (what he termed the "strategy of psychological defense"). If formed, this main directorate in support of psychological security could ensure the psychological component of Russian national security. All of these efforts by the Russians are understandable when you look at how they define an information weapon. They view it as a specially selected piece of information capable of causing changes in the processes of systems (physical, biological, social, informational, etc.) according to the intent of the entity using the weapon. Information weapons not only are aimed at hardware and software systems as listed below, but also at wetware or the mind.

In a addition, methods of persuasion are considered another Russian IO tool. The primary information weapon in this regard is a concept known as reflexive control, which is also called "intellectual IW." Reflexive control is defined as a means of conveying to a partner or an opponent specially prepared information to incline him to voluntarily make the predetermined decision desired by the initiator of the action. There are scientific and mathematical components as well as the varied military and technical uses. Russian academics have often noted that goals of reflexive control are to distract, overload, paralyze, exhaust, deceive, divide, pacify, deter, provoke, suggest or pressure an opponent with information. Other less known but reported information-psychological related activities include:

- Military unit 10003, which studies the occult and mysticism, reportedly to understand the recruiting and "brain washing" techniques of these groups
- Anti-ESP training in the strategic rocket forces, designed to enable missile launchers to establish mental firewalls in case someone from the outside attempts to take over their thoughts
- Astrologers in the Ministry of Defense, who predict ambushes, plane crashes, and other phenomenon
- Practice with the "25th frame effect," which tries to insert a subliminal message into every 25th frame of a
  movie or computer generated scene
- Applying electromagnetic impulses to the head of a soldier to adjust his/her psychophysical data
- Remote viewing and psychotronics

Russian military researchers have focused on the informational and psychological stability of individuals and society as a whole for a variety of cogent reasons, but the primary reason is the psychological security of Russian citizens. This is due to the striking change that has occurred in the country's dominant ideology, a change that did not occur in the West. Understandably therefore, the absence of a similar ideological shock in the United States and Europe has prompted less attention to this subject. However that may change in the West as the trend is for the proliferation and use of computer games, which can influence the youth, who are increasingly interested in the subject. As a special note, more American researchers are now pondering the influence of information technology on the minds of its citizens, a phenomenon accelerated by the sort of youth violence that has taken pace more frequently in the past few years.

Military-Technical

According to Marshall Igor Sergeyev, Russia's Minister of Defense, the war in Kosovo demonstrated that a new phase of the revolution in military affairs is upon us. The United States,

he noted, is in the midst of a significant military-technical breakaway in the sphere of information support of combat operations that must be countered in the future. Sergeyev's comments in a December 1999 issue of the military newspaper *Red Star* devoted to military-technical issues on the eve of the 21st century, also discussed the main domestic and foreign threats to Russia, and the primary missions and problems of Russia's military-technical policy.[166] Sergeyev used the term "information" fourteen times in his discussion of military-technical issues, and his emphasis is not surprising. Over the last few years, Russian specialists have studied and written about information issues profusely.

Sergeyev also noted that the NATO campaign in Kosovo signified the beginning of "contactless" or virtual information-technical warfare. The biggest advantage the coalition possessed came from information-support systems, such as reconnaissance platforms, which contributed mightily to the overall success in this operation. Unable to compete at the present time, Sergeyev believes Russia must look to asymmetric options. This recognition is important because the theorists believe now that Russia can not support both the military-strategic and military-technical parity with the leading military powers of the West on a 'symmetrical' basis, especially in the area of non-nuclear armaments. Therefore, some theorists state it may be necessary to search for a reasonable combination of evolutionary and 'revolutionary' paths and more effective asymmetrical directions for the development of weapons and military technology as well as technologically outfitting the Russian armed forces.

The emphasis noted by Sergeyev should be on reconnaissance, command and control systems, with the latter specifically at the operational-tactical and tactical levels. The goal is to create an integrated information environment and a single system of military standards to transmit data. Other requirements would be to universally equip a force that was information-oriented, that could essentially make use of miniaturized computer systems. Sergeyev wrote for the need to closely integrate information systems and nuclear weapons, stating that information-technical developments of both support and defensive systems would help to guarantee the effective use of nuclear weapons and could be a "new aspect of nuclear deterrence." Weapons based on these new physical principles signifies a qualitative leap in the forms and means of armed conflict and would definitely change the parameters of "parity." Sergeyev also noted that Russia's main priority in the field of prospective weapons should be concentrated on guided and electromagnetic energy weapons, cyber-weapons, and stealth unmanned combat platforms. His final conclusion remark was that a new phase of the revolution in military affairs has begun and Russia must not lose time. Time frames were of such importance that any further delays in starting a full-scale modernization of the armed forces could lead to a fatal and insurmountable disadvantage to the Russian military forces.

Systemological Aspects

Russian scientists in recognizing the increased importance of information systems, have also adjusted their emphasis on the growing influence of information on the military-technical aspect of military doctrine. Therefore they have focused more attention on the interaction of combat systems instead of the old reliance on simple force on force ratios. According to this logic, warfare is now viewed as the interaction among the military systems vice forces in a confrontation. This idea has been extended to the modeling and simulation conducted at the General Staff Academy, where Red versus Blue is no longer the only war game played. Today, high tech systems are also modeled against other high tech systems.[167] To place this emphasis in

context, within Russian military systemology, information is viewed as the "nourishment" that gives life to all elements of the system. In particular, this applies to reconnaissance, command and control, support and strike systems. To put this in perspective, IW can be viewed as a system, according to this view which includes three components:

- Information support of the functioning of one's own combat systems
- Information counteraction against the functioning of the enemy's combat systems
- Information protection or defense of one's own combat systems against the informational counteraction of a possible enemy.[168]

Therefore under modern conditions, the skillful use of one's information potential and information resources, including information means and systems, will increase the force combat potential many times and the effectiveness of using weapons, combat equipment and combat systems on the whole. This definition and its implications are similar to how the United States views the potential of IO. At the same time, the vulnerability of command and control systems with respect to deliberate and random activity in the information sphere, continues to increase. Therefore, the Russians just like the Americans now understand that it is necessary to protect or defend one's information potential - to protect it everywhere and continually - not only in peacetime and wartime, but also from a probable enemy and also against unexpected changes in the current situation including social, economic and diplomatic conditions, as well as from a lack of skill and/or professionalism on the part of subordinates and chiefs.[169] Of course not all Russian forces have accepted IO as the future of warfare. While there is a growing interest in military systemology, not only in modeling information warfare but national security in general, there are still some in the military forces who look at it as not much more than witchcraft.

What has been approved recently is, however, a very definite change in the Russian military and federal government doctrine and policy for the future of warfare. The writings that have been promulgated over the last few years indicate a shift from the previous emphasis on technological developments to a huge interest in what IO can do for their forces. Especially with the extremely tight fiscal situation that the Russian military finds itself in today, it is no wonder that asymmetric warfare and IO have assumed a much larger role in their recent doctrinal publications. While the Russian military forces have tended to be written off in the last few years, one cannot discount their capabilities.

As mentioned earlier, the Russians have not organized their forces like the United States and they have also focused on different aspects of IO. The emphasis on psychological aspects are entirely different than where other military forces have decided to orient their attention. This is a whole new area of study and the Russian Federation is known for employing many highly trained academics including mathematicians and scientists who have now concentrated their attention on investigating all aspects of IO. Just because the Russians do not organize their operations along the same lines as allied nations, does not necessarily mean that they are wrong. For, as many people have recognized, IO has many aspects and not all the answers are necessarily known.

IO in Kosovo

If the Russian doctrinal debate shows how information and its use in war is evolving in this new revolutionary period, then an alternate example could be the use or misuse of IO in the planning for the Kosovo campaign. This was a massive air campaign conducted by a coalition of United States and NATO air forces against the former Yugoslavia over its policies of genocide in

the Serbian province of Kosovo. The coalition flew over 34,000 combat sorties in a 78-day period of bombing, inflicting massive destruction on Serbia's economic infrastructure.[3] Rather than bringing stability to the region, as IO doctrine dictates, NATO's operation actually created greater regional instability and the potential for future conflicts. What caused this problem? It was due, at least in part, to the fact that no concerted peacetime IO campaign was implemented to deter conflict with Serbia. Once the conflict began however, IW was successfully executed to help bring the conflict to a peaceful conclusion. The problem here is that IW tends to rely heavily on physical destruction supported by other IO capabilities and related activities. Failing to execute a concerted peacetime IO campaign against Serbia, the United States and NATO were unable to avoid inflicting severe damage that ultimately makes a post-conflict period much more difficult to manage both politically and economically.

The Use/Misuse of IO in Operation Noble Anvil

The strategic bombing campaigns first described by the renowned Italian air power theorist General Giulio Douhet and executed by the Allies against Germany in World War II are a thing of the past for the United States. Douhet envisioned a total warfare where a nation's military, industry, and population were attacked to bring about a swift and total defeat. IO doctrine, on the other hand, does not advocate attrition bombing attacks and wholesale destruction against an adversary. Indeed, the advent of precision-guided munitions and effects-based targeting has added a whole new dimension to using physical destruction as an information weapon.[6] The mere ability to destroy one of an adversary's high value targets while leaving the surrounding area virtually unscathed sends a very potent psychological message. First, it demonstrates the precision, lethality, and superiority of American weapons technology. More importantly from an IO perspective, limiting collateral damage and physical destruction gives the adversary less ammunition for hostile propaganda directed against the United States. Second, the United States military has now so conditioned the international media to low collateral damage and precision engagement that when the occasional accident occurs and a nonmilitary target is hit, the media will tend to amplify the effects of the accident. By its sheer excellence, the United States' recent aerial campaigns have inadvertently set an inescapable standard for minimizing collateral damage. However, there is much more to IO than just a targeting or destruction campaign.

Therefore, both the domestic and foreign publics expect United States to avoid inflicting massive collateral damage and civilian casualties since it has the technological means to do so. Failure to accomplish this strategy makes the United States a target of criticism by domestic and foreign media and politicians alike. The very manner in which the United States uses physical destruction may in fact provide an information tool for an adversary. When the United States uses physical destruction to manipulate the behavior of an adversary, it must defend itself against the hostile propaganda of that adversary and strive to maintain absolute credibility. Therefore, it is critical that the public affairs and PSYOP messages describing the use of physical destruction be absolutely accurate. Here is an example of a press statement that was published during the Kosovo conflict with Serbia:

> The Serb air force is a shadow of its former self. Former Republic of Yugoslavia garrison capability has been severely compromised. Air defense systems have been degraded and destroyed. Some 637 heavy weapons and 268 other military vehicles have been destroyed. Fourteen command posts have been hit. Thirty-eight percent of radio

relay sites have been destroyed or damaged. Two-thirds of surface-to-air missile systems have been destroyed.[4]

While sounding impressive, this lofty list of NATO achievements later proved fairly inaccurate. In what may have been an overzealous desire to demonstrate positive results from a two-month-old air campaign that was beginning to draw considerable international criticism, NATO put its credibility on the line with statements the Serbian military knew to be inaccurate. Given that the National Army force in Kosovo was the target of United States IPI and PSYOP efforts, any loss of credibility with the target audience ultimately harmed these operations. In addition, besides using just PSYOP leaflets, the United States also uses public affairs to inform an adversary of its military's destructive capabilities and to dissuade them from behavior that is contrary to national security goals. A good example of this was the large amount of media coverage given to the arrival of the Apache attack helicopters in Macedonia during the Kosovo conflict with Serbia. The United States intended the presence of the lethal Apaches to have a psychological impact on the Serbs. The Apaches received great amounts of media coverage due to their awesome destructive capabilities. However, this backfired when one crashed during a training mission, generating a rash of bad press regarding the poor state of training of the Apache aircrews. Whether or not this was true, it somewhat negated the intended psychological impact.

An IO After-Action Report

The bottom line is that an overall information strategy was never attempted against Yugoslavia, despite almost seven years of warning. As emphasized throughout this book, IO is a long-term strategy that must be put into motion during peacetime. The failure of the United States to implement an information plan was largely attributable to the lack of political direction. To be effective, there must be national-level direction to ensure that the required interagency coordination takes place early in the planning process. Another major problem was the lack of coordinated United States and NATO strategies. In addition, the absence of a United Nations resolution signaled a lack of international support, and the failure to recognize the significance of Russian participation also caused unnecessary turmoil for the coalition. Since there was no clear link between military and political strategy of United States and NATO, impatience with the diplomatic process inhibited the execution of an IO strategy.

At the operational level, serious blunders were made that precluded the long-range planning of an IO campaign. The ruling out of ground forces violated the principles of operation security and deception. There was also an absence of a contingency plan to address the public relations aspects of military failures, i.e. the Chinese embassy bombing. The confusion that followed that incident greatly damaged NATO's credibility. Furthermore, the public information campaign never connected the Danube bridges' destruction to protecting the Hungarian minority in Vojvodina. In addition, NATO did not produce a military "video" comparable to the Yugoslav capability, which quickly led to their credibility being questioned when "ground truth" failed to match the press releases, i.e. where are the destroyed tanks? The absence of the NATO Secretary General in the beginning of the campaign in the United States media also caused a perception of lack of unity in the coalition. These and other mistakes collapsed any concept of conducting a viable IO campaign against Milosevic and his forces.

How an IO Campaign may have succeeded

To better understand the concept of IO as an integrating strategy, let's look at an example

of how an information plan might have been employed from the start in Kosovo. Imagine that NATO forces in Kosovo as part of the regional stabilization strategy, are engaged in helping restore normalcy to the lives of the Kosovar citizens. Many of the NATO activities would consist of coordinating projects to restore economic infrastructure, restore public works and reestablish the local governments. The pre-conflict demographics indicate that the population of Kosovo was approximately 90 percent ethnic Albanian and 10 percent ethnic Serbs. NATO would expect the ethnic Serbs to distrust NATO intentions, as the Serbs were the primary target of NATO hostilities during the short conflict. It would therefore be imperative for NATO to appear even-handed in assisting the different ethnic groups. This would mean that the Serbs should enjoy the same benefits and security that the NATO operation affords the ethnic Albanians.

Now imagine that part of the plan would require a NATO mechanized infantry brigade to establish its command post in a town having an ethnic Serb majority and a mostly Serb local government. How might NATO employ information operations to help stabilize this area, reduce friction, and deter hostile actions towards the NATO force? First, NATO would employ its intelligence system to conduct an intelligence preparation of the area, which could be called an intelligence preparation of the battlespace. This would occur through a variety of means, including ground and aerial surveillance and reconnaissance, signals intelligence, human intelligence and open-source intelligence. PSYOP studies, if available, would contribute valuable information on the social, religious, and ethnic characteristics of the area. NATO Civil Military Cooperation (CIMIC) personnel would coordinate with any nongovernmental, private volunteer and international organizations present in the area before the conflict to help gather information about the area. After developing a preliminary intelligence estimate and conducting PSYOP or CIMIC assessments, NATO would begin planning for the operation in earnest. The intelligence community would also continue to develop intelligence on the area.

NATO would then begin an information preparation of battlespace as mentioned in Chapter 2. This would help prepare the area inhabitants and particularly the ethnic Serbs, for the arrival of NATO forces. Planners could choose from a number of different means to convey this information. NATO public information personnel would prepare media releases to inform the populace of the details of the employment, including answering when, why and how many NATO forces would be introduced into the area. NATO might also disseminate the media releases to the local Albanian and Serb media, drop PSYOP leaflets, conduct radio and television broadcasts, distribute NATO-produced newspapers in the Albanian and Serbo-Croatian languages and use any other means available to get the desired information to the people. While the public information releases would focus on informing the populace, the PSYOP releases would focus on very specific facts and themes aimed at influencing the Serbs to accept the NATO presence. These PSYOP themes might stress the economic or security advantages of having coalition forces in the area and would encourage Serb cooperation.

With the information preparation of the battlespace completed, NATO could begin introducing forces into the area. The initial force would have a security element and would probably be accompanied by CIMIC and PSYOP troops, who would establish contact with the local Albanian and Serb leadership in addition to any NGOs in the area. The aim would be to help assist in the introduction of additional troops and to further assess the geographic area. NATO would continue a gradual introduction of forces to avoid giving the impression that an occupying force was entering the area. As the mechanized infantry brigade headquarters became

operational, CIMIC troops would identify projects that NATO could coordinate to help gain the acceptance of the Serb population. Within the limits of force protection requirements, the NATO mechanized infantry brigade personnel would conduct activities to increase the direct contact between NATO soldiers and the local populace, which usually tends to help gain acceptance. The brigade commander would periodically conduct personal meetings with the local Albanian and Serb civilian and military leadership and any other influential members of the community, in order to clarify NATO's intentions, help resolve any issues or misunderstandings, and make personal assessments of the local attitudes.

The NATO public information and PSYOP troops could also furnish information to inform and influence the local populace to cooperate with NATO. This information would be disseminated by a variety of means, which might include public information releases to any local Albanian or Serb media and public information broadcasts in the Albanian and Serbo-Croatian languages over radio KFOR. In addition, public information broadcasts over local civilian radio with purchased broadcast time, radio and television broadcasts either commercially or from COMMANDO SOLO aircraft, handbills, and any other media available to disseminate information to the people. While all of these activities were underway, NATO would employ operations security to deny potential adversaries any critical information that would indicate the plans and activities of the NATO forces moving into the area. Deception might be employed to mask the arrival of a NATO force into the area and to deny potential adversaries the ability to accurately assess the size and strength of the NATO force. This sort of approach to informing the local populace would continue as long as the mechanized infantry brigade remained in the town.

While this scenario obviously did not occur, it shows how an integrated IO campaign may have been successfully implemented in Kosovo. Ultimately it was the lack of an overall information plan in this political war that probably led to the relatively unsuccessful conduct of this campaign. One would think that the United States military would have learned more in the last few years about how to conduct a proper IO campaign, but that was not the case in Kosovo during 1999. This is especially egregious considering the advanced state of IO doctrine in the United States. However as many people understand, just because a country publishes doctrine, it does not necessarily mean that they understand or employ it. The United States is a case in point. While we may not be studying our own doctrine, that is certainly not the situation for IO. What is especially interesting is the huge amount of interest in IO doctrine by other nations, especially China, who are studying this new warfare area at a feverish pace.

Information Warfare and the People's Republic of China

Given the Chinese military leadership's continued fascination with the United States conduct of the Gulf War, there is little doubt that in the next conflict, the PRC is likely to employ its own version of the information-based warfighting techniques. Just how strongly has the PRC's military establishment been persuaded about the lethality of the information warfare techniques, was described by Lt. General Huai Guomo in his book on information war. Describing a series of techniques that could be used by the PRC in a future conflict, Guomo relates:

> Before a battle begins (sometimes dozens of hours in advance) and proceeds, commanders will first use offensive information-war means (precision guided weapons, electronic jamming, electromagnetic pulse weapons, and computer viruses) to attack

> enemy information systems, affecting or destroying their decision-making mechanisms and procedures, thus forcing an end to the fighting in line with the aspirations and terms of the offensive sides. And meanwhile, to protect their own information and information systems from enemy destruction, they will set up in combat space among all targets and weapons real-time detectors--links among shooters. Such offensive-defensive information warfare will become the focus of coming wars. The struggle for information supremacy will gradually become the crux of the battle, in a sense as strategic deterrent.[170]

Consider how that quote compares to the discussion from Chapter 1, in which the United States tacticians have also stated that Information Superiority is the key to success in future conflicts. The other significant influence on the thinking of the Chinese military analysts is their conclusion that the People's War under modern conditions has undergone an irreversible change. Much of that analysis came from observing the United States led coalition effort in the Gulf War. Soldiers equipped with low technology, like the soldiers of Iraq and the PRC, will encounter a decisive tactical disadvantage when faced with high tech-equipped American and European forces. Consequently, it has been argued in the latest PRC doctrine, that new technology is particularly important especially in local wars.

The Chinese military establishment is also very preoccupied about emerging as a high technology-based force in the 21st century. A recent examination of the writings of its military analysts underscores the fact that they are avid readers of American professional military journals and the futurists, much of whose work has deeply influenced the thinking of senior United States military leaders. One scholar, Su Enze believes that the military revolution has already happened. "Guided and represented by information warfare," he writes, "a military revolution is also taking place in military ideology, military theory, military establishment, combat pattern and other military fields on a global scale."[171]

The PRC scholars are also quite sensitive to the notion of information as a prime strategic source in warfare and the importance of intelligence in contemporary warfare. One author writes:

> In strengthening the information concept as a multiplier of commanders, we must take information as a multiplier of combat effectiveness and see it as a strategic resource more important than men, materials, and finances, so that it can be properly gathered, employed in planning, and utilized. We must make efforts to raise our capacity to obtain, transmit, utilize, and obstruct warfare information and must include these elements in the whole process of command training.[172]

Chinese defense specialists, like their American counterparts, are looking for the "perfect weapon" in information warfare. One hears the echo of Admiral William Owens's advocacy for "a system of systems." Cai Renzhao advocates that the PRC, "should try to gain insight into the development situations of foreign military forces, to try to understand future warfare by accurately recognizing the differences between ourselves and foreign military forces to fully bring our own superiority into play and explore the “perfect weapon” on a digitalized battlefield."[173] He recommends that the PRC follow the European Union's example in a "focused way," and learn lessons from the United States and Europe in developing information-related research. According to Cai Renzhao, the PRC should, "fully bring into play the guiding role of information warfare research in building the military… to seek measures by which to launch vital strikes in future warfare, so as to damage the enemy's intelligence gathering and transmission

abilities and weaken the enemy's information warfare capacity."[174]

Chinese IO as a Warfighting Network

Similar to what we discussed in the first chapter, conventional organizations in the information age are undergoing major changes and the notion of hierarchy has become outmoded. In its place are emerging multi-organizational networks, with the United States military performing a trail-blazing task of undergoing radical changes in response to the radically divergent techniques of warfighting in an information age. Called “joint warfighting,” this term serves as an umbrella phrase under which a multitude of changes are taking place. Under the auspices of the Goldwater-Nichols Act of 1986, the United States military has not only been busy converting the task of joint warfighting into an operational form, but is also continuing to do more with less. This means that different organizational and functional agencies have been formed to serve as a credible warfighting force. The fact that JV 2010 and its follow-on doctrine JV 2020 has emerged in an abbreviated discussion as the premier white paper of the United States military and the importance of IO within that doctrine has not been lost on the Chinese military.

These defense analysts also appear to understand that information warfare is at the cutting edge of military doctrine and all the implications that this means for traditional institutions like the military. Xu Chuangjie writes, "The revolution in information technology has increasingly changed with each passing day the battleground structure, operational modes, and concepts of time and space while dealing blows to the traditional 'centralized' and 'tier-by-tier' command structure."[175] He cites the United States Army's example of building a "ground force operational command system," which is an attempt "to organize various command control systems of the . . . ground forces into an integrated mutually linked network to realize ‘shared information' from the national command authorities on top down to a grass-roots unit."[176] He emphasizes the significance of strengthening, completing, and perfecting the building of a command and control system for the PRC. He also recommends that the command and control system "at and above the battalion level of various services and service arms" be turned into an integrated mutually linked network. In addition, the traditional vertical and tiered command system must be converted into a network command structure in order to meet the demands of time and flexibility in command, and finally the centralized type command system should gradually be developed into a dispersed type command.[177] Once again, this ties into the horizontal integration concept that we mentioned in the first chapter of this book.

The Chinese military establishment has also been quite conscious of its country's vulnerability to potential acts of sabotage during peacetime, as well as attacks during a military conflict and is taking steps to reduce this vulnerability. Wei Jincheng writes, "An information war is inexpensive, as the enemy country can receive a paralyzing blow through the Internet and the party on the receiving end will not be able to tell whether it is a child's prank or an attack from an enemy."[178] Discussing the use of viruses in a netwar or even a cyberwar, another defense scholar writes, "Computer viruses can be used to track down enemy's target system and the enemy's guided missiles may end up attacking the side which has launched them or deviate far from the intended target . . . After locating its target, a virus may replicate rapidly, erasing the normal operating database, thus overwhelming and crippling the computer system."[179] The same article discusses the variety of measures taken by the U.S. military in reducing its vulnerability to potential attacks, including sabotage attempts from terrorists and hackers.[180]

The military establishment in the PRC is watching the recent research and development of "virus warfare" in the West with rapt attention. The main focus of their interest, once again, is the United States military. One essay notes with interest a news item that the American military has developed a computer virus program that can destroy an enemy's computer circuits and control systems, "transmit internal information that mistakenly reports enemy's orders and distorts the computer satellite software that the enemy transmits to his combat units." The same essay discusses another "computer virus weapons plan" that the armed forces are in the process of developing. This program reportedly is aimed at planting viruses in exported computers and electrical equipment. The "virus source" implanted in such equipment can be activated during the time of military conflict, causing the enemy's electronic equipment to malfunction.

This section concludes that a number of suggested preventive measures are needed against a future netwar or cyberwar. First, it advocates raising the consciousness of military computer security throughout the Chinese armed forces. Second, it asks the PRC military establishment to pay special attention to removing "hidden perils to hardware and software security," by creating security filters and careful tests on all imported electronic equipment. Finally, it recommends the initiation of "special-topic research on computer viruses."[181] What is extremely interesting from a western viewpoint to these Chinese articles are how they tend to mirror similar concerns by United States analysts.

What of the Future of IO in China?

So as one ponders the future dynamics of United States-PRC relations in the context of information warfare, at least three observations come to mind. First, even though the Chinese military establishment wishes to emerge as a high tech-based warfighting machine, based upon current intelligence, it will likely take time for this to occur. Second, this reality should not let anyone forget that the current commitment of the Chinese armed forces to high-tech-based warfare, if continued with the same zeal, will likely pose a serious challenge for the United States in the coming years. The state of readiness of the Chinese armed forces in the realm of information warfare at the present time may be at a very primitive level compared to the United States armed forces, but they are writing doctrine and experimenting with IO on a constant basis. Some of America's leading information warfare specialists, like Martin Libiki, postulate that:

> Militaries, especially those of widely different nations, cannot prosper by copying each other… Their endowments, circumstances, and strategies differ greatly. Each must adapt the general to the specific. We know the Chinese can copy our thoughts, but whether they can innovate in pursuit of their own objectives is not yet obvious.[182]

Third, China's smaller neighbors must not only watch the Chinese military preparedness closely, especially in the realm of information warfare, but also try not to remain too far behind in this field. This is not to suggest that the PRC and its neighbors are likely to fight one or more wars in the near or distant future. Rather, it is to suggest that the military establishments of a number of countries of that region are in the process of being equipped with state-of-the-art weaponry and they are well-served to emulate the United States military preparedness in the realm of information warfare-related technologies as much as possible.

The Chinese have a very long history of adapting different technologies for their own use. They view information warfare as a tool to counter the overwhelming military superiority of the United States. If they can influence world opinion through international public information, PSYOP, electronic warfare, etc., then the PRC will try to shape the environment to facilitate their

goals. IO is all about perceptions management, as discussed in a number of areas in this book, and the side that can best influence the adversary decision-maker will be in the most advantageous position to ultimately affect the final outcome.

Introduction to IO in Australian Defence Forces

One of those nations that will be affected by China and its growing capability within the IO arena is Australia. This section, we will discuss how this nation is developing its own doctrine and force structure. What is very interesting about Australia is that it is a nation with a very large in land mass but a small population and even smaller in its military forces. Therefore, IO would seem to be a great tool for it to use to maximize its effectiveness in the region and around the world.

In common with the armed forces of many other states, one of the most important operational concepts adopted by the Australian Defence Force (ADF) in the last half decade has been IO. In particular, over the last several years, IO has been incorporated into Australian Defence Organization (ADO) policy and into joint/single service doctrine as well. Instruction on IO has been introduced into the curricula of a variety of courses taught at generalist and specialist single-service schools, as well as in the joint training establishments. IO doctrine and training has been tested on exercises and most importantly, it was recently used during real-world operations. In short, the ability of the ADF to conduct IO in concert with other operational activities has become a fundamental part of the ADF's approach to warfighting.

This section is intended to outline the ADF's approach to IO and recent Australian experience in the conduct of IO in operations. The intent is to focus on developments within the ADF at primarily the operational and tactical levels. This is not to say that there has not been significant policy activity at the strategic level for which a case in point would be the significant activity outside of the ADO regarding the protection of the Australian National Information Infrastructure. However, it is at the operational and tactical levels that developments with respect to IO in Australia are perhaps the most readily apparent.

The Evolution of IO and Related Concepts in Australia

Tracing the development of any form of military doctrine is inevitably a difficult task. Descriptions of the adoption of particular concepts or approaches will tend to focus on official announcements encapsulated in policy documents. In practice, this approach reflects the end or outcomes of doctrinal evolution and innovation rather than the realities of the doctrine development process. It ignores or marginalizes the significance of less formal influences on doctrine development such as the observations and experiences of exchange officers and the modification or outright copying and adoption of overseas ideas. It also tends to disregard the influence of individuals from outside the military establishment, be their influence direct or second-hand via the pressure that they may exert on service personnel. With those caveats in mind, the following section provides a broad overview of the development of IO doctrine within Australia.

Like most other defense forces across the globe, serious thinking about the implications of an information-based Revolution in Military Affairs for the conduct of operations commenced as the result of observations of the Coalition's performance in the Gulf War. Key observations included the increasing military value of attacking or manipulating an adversary's information and information systems, the need to deny an adversary the ability to do the same, and the

requirement to integrate such activities with other military operations. A further key factor noted was the rise of the so-called "CNN effect", the pervasiveness of global electronic media and the influence that it exerts on public opinion, thereby shaping political and (therefore) military decision making.

The conclusions drawn from the Gulf War were reinforced by Australia's operational experiences in Somalia and Rwanda as well as by observation of overseas experiences in Haiti, Bosnia and elsewhere. Experience and observation of peace operations demonstrated the utility of influencing the information environment at all levels of conflict, not just the middle to high end of the conflict spectrum. In particular, it was noted that a technologically inferior adversary might still have the ability to influence the information environment in their own favor, by exploiting the vulnerabilities and weaknesses of high technology systems.

The Australian response to the above observations was gradual. Through the mid 1990s, a variety of capabilities that had languished since the end of the Vietnam War were resurrected, in particular PSYOPS and to a lesser extent CA. Between 1995 and 1997, there was extensive discussion of a variety of information-related operational concepts including terms such as C2W and IW, in professional military journals and conferences organized by the ADF. But it was not until late 1997 that information-related concepts were clearly articulated in an official ADF document.

At that time, the Australian government released the document *Australia's Strategic Policy* (ASP97), which identified the achievement of a Knowledge Edge (KE) as Australia's highest priority in defense policy. ASP97 described a KE as being the product of three elements of capability – intelligence, C4 systems, and surveillance/reconnaissance capabilities. As has been noted by Air Vice Marshal Nicholson, this provides a rather limited account of the role that information-related activities can play in the context of armed conflict. However, this account of the KE provided a basis for further conceptual development, in that it left open the possibility of other means by which a KE might be achieved.

In early 1998, the Commander of the newly formed Headquarters Australian Theatre (HQAST) released the document *Decisive Maneuver*, which for the first time articulated an Australian approach to warfighting at the operational level of war. The capstone concept of Decisive Maneuver is composed of five core concepts, and three supporting concepts. Underpinning these core and supporting concepts is the concept of Decision Superiority, which is defined as the ability to make and implement more informed and accurate decisions at a rate much faster than an adversary. This is very similar to the Information Superiority concept espoused by the United States. In addition, shades of the OODA loop are seen in these Australian doctrinal writings. In turn, Decision Superiority is enabled by four broad sets of activities:

- Information management
- Intelligence
- Protective measures for C4I systems and processes
- Offensive C2W directed at adversary C4I systems and processes

Hence, whilst the Decisive Maneuver concept precedes the adoption of IO by the United States per se, it goes well beyond the KE concept articulated in ASP97. This is because it includes measures to shape the information environment, as well as the collection, processing, management and dissemination of information. Significantly, it also functionally divides information-related activities into three broad categories:

- Offensive
- Defensive
- Supporting activities

As will be seen later, this division of effort is also reflected in the IO construct adopted by the ADF.

The formal doctrinal adoption of IO by the ADF occurred during 1998. An initial draft version of the *Information Operations Staff Planning Manual* (IOSPM), was circulated throughout the ADF by the Australian Defence Force Warfare Centre (ADFWC). This became and still is the doctrinal basis for the planning and conduct of IO within the ADF. In addition, at the departmental level, IO was finally given official recognition in the document *Defense: Our Priorities*, which noted that the development of IO capabilities was a key priority for Defence. Hence by the beginning of 1999, IO had formally become part of the ADF's approach to warfighting.

Now that IO was formally been adopted as part of the Australian approach to warfighting, there still remains the issue of linking IO to other warfighting concepts. In a presentation given in early 1999, a model was demonstrated to connect IO with other information-based warfighting concepts at the Defense Communications Development Seminar held in Canberra. The model, noted that while a combination of IO and C4ISR systems might provide IS, this in itself, did not guarantee Decision Superiority (DS). The KE which led to DS was seen to be a product of both IS and superior intellectual capital within the Defence Organization.

The above approach to DS implies the possibility of a warfighting concept which could be referred to as Knowledge Operations (KO) or Knowledge Warfare (KW). Such a concept would include not only the activities which are currently encompassed within IO, but would also incorporate other measures centered around the attack and defense of the organizational intellectual capital that transforms IS into a KE, and thence to DS. These ideas extend well beyond the concept of IO as it is presently understood within the ADF and elsewhere. In particular, it implies a far closer functional relationship between the operational conduct of IO-related activities and the development and maintenance of capability, in particular the human dimension of capability than is presently now the case. The full development of a coherent KO/KW concept that can be readily employed in an operational setting is probably some time off. Nevertheless, the conceptual possibility of KO/KW highlights the dynamic nature of operational concepts relating to the information domain.

The Australian Doctrinal Approach to IO

Having examined the evolution of IO within the ADF, attention will now be focused on the details of the current doctrinal approach to IO as accepted by the ADF. In present (draft) Australian doctrine, IO is defined as: "Actions taken to defend and enhance one's information, information processes and information systems, and to affect adversary information, information processes and information systems." It should be noted that, unlike in United States joint doctrine, there is no separate definition offered in Australian IO doctrine for IW, as the activities and effects encompassed within IO are held to be applicable at all levels of the conflict spectrum. In addition, the term C2W has fallen into disuse within the ADF, which was formally regarded as the employment of IO at the operational and tactical levels against a particular target set, normally the adversary command and control systems and processes. Hence, in the Australian

approach, C2W was originally regarded as an application of IO rather than as a separate operational concept in its own right, but that too has now however changed.

Current ADF doctrine resolves IO into three distinct but interdependent components of Offensive IO, Defensive IO and IO Support. These three components can further be broken down into specific IO capabilities or activities, as shown above. It should not be inferred from this doctrinal model of IO that all the capabilities listed are currently possessed by, or are intended for future procurement by either the ADF or the ADO as a whole. However what the model does acknowledge is that the increased integration of high technology computers with communications equipment into the everyday business practices of the ADO represents a source of potential vulnerabilities that can and will be exploited by adversaries. Accordingly, there is a need to understand how adversaries might exploit these vulnerabilities, and to incorporate the means that an adversary might employ against the ADO into the Australian doctrinal account of IO.

The range of capabilities or activities incorporated in the Australian model of IO is essentially similar to that which is offered in the JP 3-13, although there are some differences. Australian IO doctrine does not include any direct equivalent of the United States term Special Information Operations (SIO), though Australian doctrine does recognize that some IO capabilities or activities are sensitive, and will require special authorization for their employment. Similarly, Australian IO doctrine does not recognize Counter-Deception as a discrete part of Defensive IO. In addition, the number and range of activities listed under IO Support in Australian doctrine is somewhat more extensive than the two (CA and Public Information) listed under IO related activities in JP 3-13. In the Australian model, these two activities are incorporated within the IO Support area.

At present, the draft IOSPM remains the capstone doctrine for IO within the ADF. IO has also been incorporated into single service capstone doctrinal documents for both the Australian Army and the Royal Australian Air Force (RAAF). IO is not mentioned in the current interim Royal Australian Navy (RAN) capstone doctrine, though it is likely that IO will be incorporated into subsequent editions of the work. At the present time, the IOSPM is in the process of being revised, with the intention of publishing it as an Australian Defence Force Publication (ADFP) in the near future. The details of the model of IO that is finally articulated in future doctrine may vary somewhat from that which is shown in the figure above, however, it is likely that the fundamentals will remain essentially the same.

The Australian Experience of IO – Two Case Studies

As mentioned earlier, Australia is included in this chapter because not only are they a smaller force that is attempting to add IO doctrine within their services but the ADF has also used IO in two recent operations over the last three years. While there are obviously many portions of these missions that remain classified, we will, over the next few pages, discuss the operational IO issues pertinent to these two task forces.

Bougainville – Background

The first case study on the operational employment of Australian IO doctrine is Australian involvement in the Truce Monitoring Group (TMG), and leadership of the Peace Monitoring Group (PMG) to Bougainville, codenamed Operation BELISI. A map showing Bougainville relative to the rest of Papua New Guinea is shown below:

In July 1997, the various PMG and Bougainvillean, less the hard-line BRA faction of Francis Ona met in New Zealand, signing the Burnham Declaration. This called for the various leaders to bring about a cease-fire and for an international peacekeeping force to be deployed to Bougainville. In October 1997, the Burnham Declaration was followed up by the signing of the Burnham Truce. This established an immediate truce between the conflicting parties on Bougainville and recommended to all parties that a TMG should be deployed to Bougainville. The technicalities of monitoring the Burnham Truce were resolved in meetings in Cairns, Australia, between the PMG government and the Bougainville factions in November 1997.

At the same time in Cairns, an agreement was signed by the governments of Australia, New Zealand, PMG, Fiji and Vanuatu, regarding the terms under which the TMG would operate. Under the terms of the agreement, the TMG had responsibility for:

- Monitoring the compliance of the parties with the terms of the Burnham Truce
- Promoting and instilling confidence in the peace process
- Providing people in Bougainville with information on the truce agreement and the peace process

It is understood that the latter two responsibilities clearly indicated the need for the conduct of IO to support the TMG's activities. The TMG deployed to Bougainville in December 1997 under New Zealand command. The bulk of the TMG personnel, both military and civilian, were provided by Australia and New Zealand, with some participation from Fiji and Vanuatu. The operation of the TMG and later the PMG will be dealt with below.

In January 1998, the various parties in the Bougainville conflict signed the Lincoln Agreement. This extended the truce period to 30 April 1998, whereupon a permanent cease-fire would come into effect. At the same time, the TMG would be replaced by the PMG, the terms under which the PMG would operate being contained in the so-called Arawa Agreement, which was an annex to the Lincoln Agreement. Finally, the Lincoln Agreement provided for free and democratic elections for a Bougainville Reconciliation Government (BRG). As the Arawa Agreement came into force on 30 April, the TMG was re-roled as the PMG and at the same time, command of the force shifted from New Zealand to Australia, where it has remained since.

As of September 2001, the PMG remains in place in Bougainville. While it is the case that the future status of Bougainville with respect to Papua New Guinea remains unresolved, the PMG has been very successful in enhancing the peace process and providing an environment in which the reconstruction of Bougainville can proceed. At present the total strength of the PMG remains at about 250, though the force is currently in the process of being reduced in size. However, it is likely that the PMG will remain in place for the immediate future, until the status of Bougainville and the PNG is resolved.

IO Contributions to Operation BELISI

Having provided the background to Operation BELISI, attention will now be focused on how IO has contributed to the operation. However before doing this, it is necessary to provide a brief overview of the structure and operations of the PMG. The
PMG is divided into a headquarters (with supporting elements) located at Arawa, and a number of Monitoring Teams (MT) or Liaison Teams (LT), each of which are allocated a distinct area of operations (AO). Within their respective AO, each MT/LT conducts regular patrols to monitor the peace agreement, and to maintain contact with the local population.

As was been noted above, IO plays a vital role in the achievement of the PMG mission, as mandated by the Arawa Agreement. IO achieves this by the provision of information about the peace process to the various parties on Bougainville. Furthermore, as an unarmed force, the PMG is critically dependent upon the support and goodwill of the people of Bougainville. The principle means by which the PMG achieves this popular support, and performs this role is by the dissemination of information products produced by the Military Information Support Team (MIST). The primary responsibility of this team is the production of a variety of printed media of which the most notable are the newspapers titled *Nius Blong Peace* (Peace News), which is supplemented by the glossy monthly magazine *Rot I Go Long Peace* (The Road to Peace). In addition to these two printed products, the MIST is also responsible for the development of a wide variety of other products. This includes other printed products such as posters and handbills as well as other products such as T-shirts, hats and soccer balls bearing messages.

Beyond printed products, the MIST has also developed radio scripts and a cassette featuring local music. Collectively, these products supported the achievement of the PMG's objectives, as mandated by the Arawa Agreement. They have also been used for information campaigns centered on themes to support the peace objectives, including preventing domestic violence against women as well as the production and consumption of *hombru* (home-brew liquor). While the MIST does perform some dissemination of the product that it produces, the bulk of these efforts fall to the MTs, from both their static locations, as well as during their patrols. In addition to disseminating MIST product, the MTs were also able to provide feedback to the MIST on the effectiveness of their products. The products produced by the MIST have been well received by all the factions on Bougainville and represent a key means by which the PMG has performed its mission. More than that, it could be argued that Operation BELISI represents an example of IO being the main effort of an operation, with other military elements being in support of these operations. IO has been the means by which the Bougainville population has been kept informed of developments in the peace process and its support for the PMG maintained.

East Timor - Background

The second case study on the operational employment of Australian IO doctrine is the Australian led peace-enforcement mission to East Timor, code-named Operation STABILISE. The roots of the present UN intervention in East Timor date back to 1974. Following the collapse of the government in Portugal, civil war erupted in East Timor between factions favoring independence and those supporting integration with Indonesia. In December 1975, following the withdrawal of the Portuguese administration, Indonesia intervened militarily in the territory, and the following year they integrated East Timor as their 27th province, an act which was not recognized by the United Nations. Intermittent guerrilla conflict continued off and on between the Indonesian security forces and pro-independence groups (principally FRETLIN and its armed wing, FALINTIL) throughout the intervening period until the late 1990s. Concurrent with the on-going guerrilla conflict were extensive human rights abuses conducted by the Indonesian security forces against the East Timorese population. Estimates of the total number of deaths in East Timor for a 23 year period ending in 1999, range well above the 100,000 mark, out of a pre-1976 population of about 680,000 for the territory.

The 1997-98 economic collapse in Asia sparked political turmoil throughout Indonesia. In mid-1998 this culminated in the forced resignation of President Suharto with a replacement

B.J. Habibie, prior to the outcome of general elections to be held later in 1999. As part of the measures to deal with political disorder, Habibie floated the idea of an autonomy ballot for East Timor. This eventually led to the signing of the May 5 1999 agreement between Indonesia and Portugal, for the conduct of a ballot on future status of East Timor. Despite on-going sporadic violence and intimidation by pro-Indonesian militias, some 446,000 voters registered to take part in the ballot. This culminated in the actual ballot on 30 August 1999, with results announced on 3 September 1999. Some 78.5% of the East Timorese electorate voted against special autonomy within Indonesia, or in other words, for East Timorese independence.

In the immediate wake of this announcement, widespread violence and destruction was instigated by pro-Indonesian militia groups. Thousands of East Timorese were killed, and well over 150,000 were displaced from their homes. Despite the declaration of a state of emergency, Indonesian security forces prove either unwilling or unable to stem the bloodshed. As international pressure mounted, evacuation operations were mounted to rescue United Nations personnel and some East Timorese from the unfolding carnage. On 15 September 1999, the UN Security Council adopted Resolution 1264, which authorized the deployment of the Australian-led INTERFET force to East Timor in order to restore peace and security.

INTERFET deployed into East Timor on 20 September as Operation STABILISE, and immediately commenced securing the immediate vicinity of Dili. By late-October, the INTERFET force had taken control of all of East Timor, including the Oecussi enclave located in the middle of West Timor. During the subsequent months, INTERFET restored peace and security to East Timor, though the prospect of armed clashes with pro-Indonesian militia infiltrating from West Timor remained a constant threat. In mid-February 2000, INTERFET commenced the hand-over of its responsibilities to a United Nations force and completed the hand-over on 28 February 2000. Operation STABILISE is now officially concluded.

IO Contributions to Operation STABILISE

Having provided the background to Operation STABILISE, we would now like to focus on the conduct of IO during the operation. However, it must be noted that as of the summer of 2001, much of the details pertaining to the planning and conduct of Operation STABILISE still remains outside the public domain. Not the least hidden, in this respect, is the aspects relating to the planning and conduct of IO during the operation. Accordingly, this account of the role played by IO in Operation STABILISE is far from complete, and will concentrate on that one element of IO that of necessity is in the public eye namely Public Information (PI).

From the information that is readily available from open sources, it is clear that IO played a significant role in the overall conduct of Operation STABILISE. At a public address delivered in April 2000, Major General Peter Cosgrove, the Commander of INTERFET noted:

> "…the military operation plainly had an IO quotient to it. By that I mean that our military operations to provide a peaceful and secure environment in which the UN could conduct humanitarian assistance and nation building activity were to be seen in two dimensions: what we were actually doing and achieving on the ground; and what we were perceived as doing, its relevance, proficiency and legitimacy."

In his address, Cosgrove divided the parties whose perceptions were critical to the success of Operation STABILISE into four broad groups:

- The individual nations comprising the INTERFET coalition
- The INTERFET coalition itself and the broader international community

- Nations whose view of the INTERFET coalition mission, composition and leadership MG Cosgrove termed as ‘jaundiced’
- Parties within East Timor

These stakeholders and their perceptions were the crucial elements that the INTERFRET force needed to address, including the last group was comprised of the East Timorese population, the various UN agencies and NGOs.

From the outset, MG Cosgrove assessed that there would be an IO campaign by interests opposed to the INTERFET mission, such as the pro-integrationist militia groups to discredit the coalition operation. From this assumption it followed that such an IO campaign would have to be countered vigorously and effectively as a highest priority. Therefore in common with the leaders of many past coalition operations, MG Cosgrove identified that the center of gravity of the INTERFET coalition was the maintenance and legitimacy of the coalition itself. Furthermore, he also identified that the chief means by which the coalition center of gravity might be targeted was via adversary IO, namely the misinformation and propaganda disseminated via the global electronic media. Noting the media attention that the East Timor operation had generated, MG Cosgrove chose to embrace and encourage the presence of the global media in East Timor, rather than merely accept or acquiesce to it's presence. He emphasized that the INTERFET force would be transparent, accountable, available and very pro-active in dealing with the global media. MG Cosgrove felt that the most effective way of countering adversary propaganda and disinformation was to invite open scrutiny of INTERFET personnel, activities and operations by the media and to allow audiences to assess the lies for what they were.

A key example of this policy in action was the INTERFET response to claims that militia groups had infiltrated in strength deep into East Timor from West Timor. In the second week of October 1999, television footage was broadcast around the globe purporting to show militia leader Eurico Guterres, with 150 militia personnel, in the vicinity of Liquica. Guterres claimed to have crossed from West Timor into East Timor, and then driving some 100km to Liquica, without sighting or being sighted by any coalition INTERFET troops. The INTERFET commander dealt directly with the media and countered the claims by highlighting discrepancies and improbabilities in the militia leaders account, thereby extinguishing the credibility of Guterres’ claims. Had INTERFET not engaged the global media as thoroughly as it did, it is unlikely that the countering of such claims would have been nearly as effective. In short, INTERFET’s truthfulness and openness in dealing with the media were its greatest asset in countering militia propaganda.

Although the above account of IO during Operation STABILISE has focused on PI activities, this is primarily the result of the lack of open source information on other IO activities that have been undertaken in East Timor. There is little doubt that elements of IO were conducted during Operation STABILISE which have not been released as of the summer of 2001 into the public domain. That said, the significance of PI in establishing and maintaining the credibility of the coalition in the face of militia propaganda and disinformation should not be undervalued. For if it is the case that the legitimacy of the INTERFET coalition was its center of gravity, then it follows that efforts taken to protect that center of gravity are a core rather than peripheral part of warfighting. In this regard, the final words here will be left to MG Cosgrove who said, "I cannot stress enough this aspect of IO in its crucial contribution to a successful coalition mission. In this area of nurturing your constituencies, you can be figuratively just as damaged by a headline as a bullet.”

Lessons Learned and Directions Forward

Having now reviewed the employment of IO by Australia in two recent contingencies, an assessment will now be made of the effectiveness of the Australian approach to IO and the means by which this can be improved. In general terms, it can be clearly be stated that Australia's operational employment of IO has been effective. In both Operation BELISI and STABILISE, IO has contributed significantly, if not critically, to the success of both operations. In this sense then, both these operations can be seen as validating the Australian approach to IO. That said, certain caveats apply. In both cases, Australian forces were working in fairly unsophisticated, low intensity operational environments. In neither instance was the ADF faced with an adversary of the sophistication of either Serbia or Iraq. The full range of IO related capabilities were never fully employed. So leaving this issue to the side for the moment, how can Australia's ability to conduct IO be further enhanced? In broad terms, this question resolves down into two issues: doctrine and capabilities.

With respect to doctrine, the evolution of Australian IO doctrine into its present state has already been reviewed above. The current draft IOSPM is in the process of being converted into an ADFP, and it is likely that the final product will incorporate the lessons learned from Operations BELISI and STABILISE, as well as from observations of other nations' efforts. The 1999 NATO operations against Serbia also loom large. A particular issue for consideration in this regard is the conduct of IO within a coalition framework. It has been claimed by some commentators that most future military operations in the near future will be conducted by impromptu coalitions rather than traditional allies. Current Australian and United States IO doctrine barely touches on the issues involved in conducting IO in such a setting.

The second broad issue regarding the enhancement of Australia's ability to conduct IO is one of capability. Despite the successful employment of IO in Operations BELISI and STABILISE, Australia's IO related capabilities are modest and are principally oriented towards lower-intensity operations. In recent years, there have been calls for the enhancement of a variety of capabilities, including PSYOPS, CA and EW, particularly in regards to supporting air operations. Since the ADO, in common with many other defense establishments, relies heavily on commercial IT systems, it needs to enhance its ability to defend its own information infrastructure from both intrusion and disruption. This implies the need for an enhanced and dynamic IA or CND capability, especially for deployed networks. The same can be said for the other capabilities that fall under the umbrella of IO. It is expected that some direction regarding the capability and development of these other areas of IO will be articulated in the Defense White Paper to be released in the near future.

Summary

As shown in this chapter, there are a number of nations other than the United States that have conducted IO missions or operations and are currently writing doctrine but for this particular project, we chose to concentrate on the few preceding examples. First in the case of Russia and China, these two nations are the closest peer competitors to the United States and any new developments by these counties are watched with great interest by western military forces. Second, the operations in Kosovo gave the United States and the coalition a chance to use the new IO doctrine against a savvy adversary but unfortunately the advantages inherent in this warfare area were not properly utilized. An opportunity missed, Operation Noble Anvil also

demonstrated how a supposedly less sophisticated force (ie Serbia) was able to successfully deceive and manipulate coalition forces during this 78-day campaign. Finally, the section on Australia, including their doctrinal and operational use of IO over the last few years, is very illuminating for a number of reasons. A small force, the ADF is a great example of how the asymmetric capabilities inherent in IO used by forces other than the United States. Maybe it is these nations that will have thegreatest impact on IO in the future. It is also our goal, that this section demonstrates in an unclassified format, some of the unique characteristics that make up the power embedded in IO.

Conclusion: What is the Future of Information Operations

"We didn't give up when the Germans bombed Pearl Harbor…"
Bluto

Information is power, and how a nation uses that power determines how effective a country may be in influencing the world politic. Unlike in the past where the elements of power only included military, economic and diplomatic factors, in the 21st century, information is rapidly assuming a place of primacy in the conduct of foreign policy. It can be a force multiplier, a decision-tool, a central theme for an offensive campaign and so much more. But to be useful, information must be understood for what it truly is – a weapon, and if not used correctly, it can backfire just like any other kinetic device in your inventory.

The use of information to effect public opinion has a long and varied history within world politics. Often it was the government or leadership elite that could control that information, thereby exercising power over their people. Yet the tremendous advances in technology in the computer and telecommunications fields over the last decade have shattered their monopoly of control over information. In addition, the merging of these formally separate areas have given the power to use information to a much greater audience. This in turn has forced the government to work harder to control the dissemination and ultimately the use information as an element of power.

Yet in reality the government can no longer control information. This is because it does not owns the sources nor means of delivery of information to our modern society. Which of course begs the question, if you cannot control information, can you really control power? There are many other organizations outside the government that now have a much greater influence on the flow of information, and it is now the government more often than not that is on the defensive. Since it cannot control the information, it must therefore react, and because the government is a bureaucracy, it cannot act fast enough to stay on the offensive.

Therefore Information Operations is changing the way in which the worlds' militaries and governments conduct business. This includes military deterrence and peace-keeping operations, foreign policy and also world-wide economic development. No longer can these missions be conducted in isolation and so it is imperative that the organization structure adapt to these changing circumstances. That is precisely why you see so much turmoil in the governmental architecture that exists today. Will these changes even out as IO matures as a warfare area? Perhaps, but it remains to be seen as the United States and other nations continue to develop the weapons and capabilities of Information Operations.

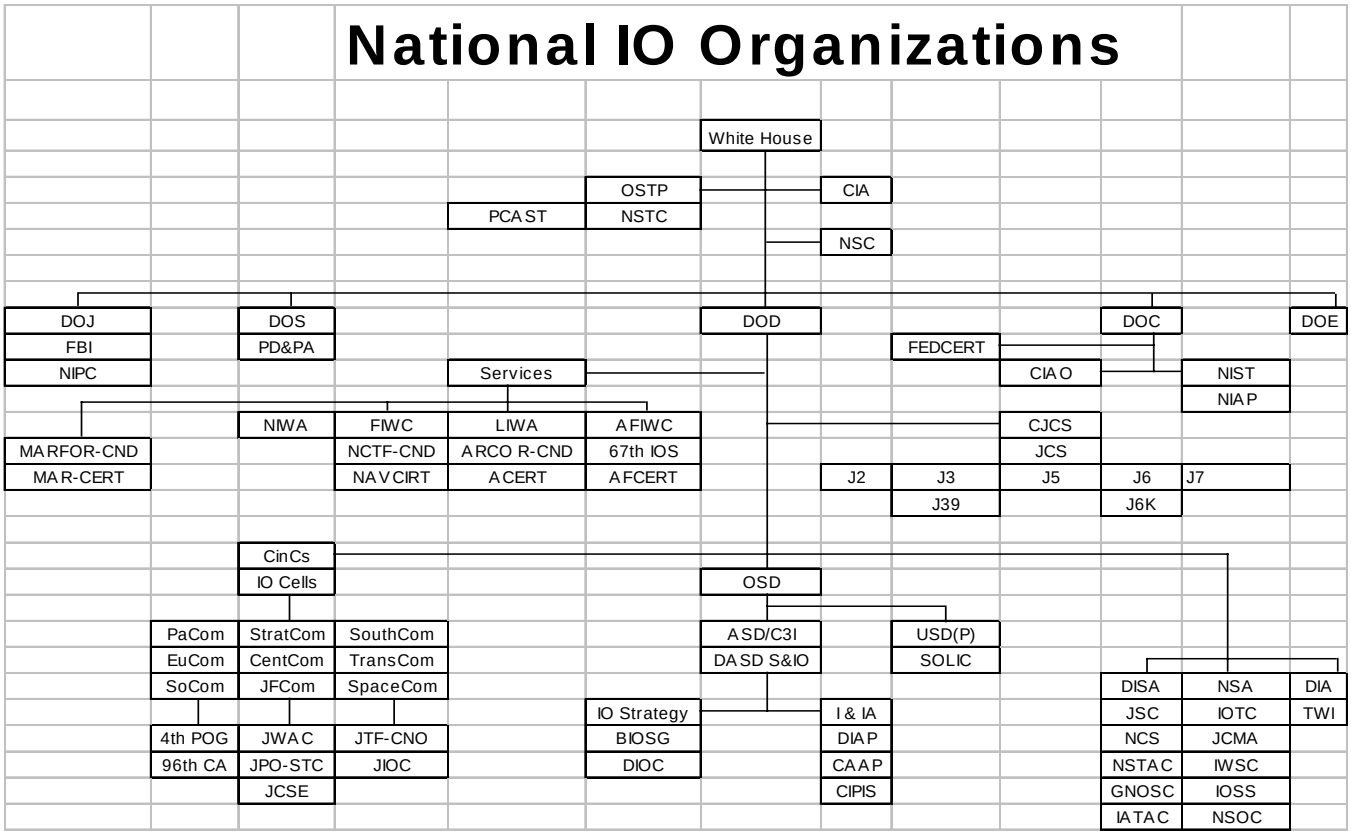
The use of information as a weapon and force multiplier is not likely to go away with a change in an administration or government. A fundamental shift has occurred and the world is now in the midst of a revolution, a new era in which information is now the most fungible of powers, and whoever uses it to their best advantage will emerge victorious. Unfortunately the fact that the dynamics of power has greatly changed is not widely recognized at this time. As we mentioned at the very beginning of this book, would you recognize a revolution if you were in it? Information Operations has forever changed the method of conducting warfare. Hopefully some of the more crucial concepts of this new warfare area have been covered adequately by this book and will be useful to you in your operations.

The authors hope that you enjoyed this publication. This book was meant to serve not

only in a teaching role, but also as an update for the millennium. We chose to highlight the critical time period from June 1997 to June 2000, with the bookends of *ER '97* to the incorporation of IO into military doctrine with JV 2020, as the highlights. In these last several years, much has changed within the IO community, both in organizational activity as well as doctrinal publications. However the delay in publication and the tragic events of 11 September 2001 are mentioned as well, to give you a better understanding of the power of Information. We have tried to address those changes as well as looking at what else was happening around the world concerning IO, concentrating on Russia, China, and Australia because that is where a great deal of activity has occurred. The original three-year period was also significant since that is two generations according to Moore's Law.

To conclude, the editors and all the contributors hope you enjoyed this book. We are using this book as a primary reference source for our students and therefore if you see mistakes or upgrades that need to be made, please feel free to contact us at jciws-iw@jfsc.ndu.edu. Our plan is to continue to use this publication in the future, so any help you can give us would be greatly appreciated. Once again, thanks and we hope you enjoyed reading this book.

APPENDIX A – IO Organizations



APPENDIX B – IO Acronyms

AFIWC	Air Force Information Warfare Center
AIA	Air Intelligence Agency
ASD/C3I	Assistant Secretary of Defense/Command, Control, Computers and Intelligence
ASD/SOLIC	Assistant Secretary of Defense/Special Operations and Low-Intensity Conflict
BIOSG	Bilateral Information Operations Steering Group
BIOWG	Bilateral Information Operations Working Group
CAAP	Critical Asset Assurance Program
CERT	Computer Emergency Response Team
CIA	Central Intelligence Agency
CIAO	Critical Infrastructure Protection Office
CINC	Commander in Chief
CIP	Critical Infrastructure Protection
CIPIS	Critical Infrastructure Protection Integration Staff
CIPWG	CIP Working Group
CITAC	Computer Investigation & Infrastructure Threat Center
CJCS	Chairman of the Joint Chiefs of Staff
CNA	Computer Network Attack
CND	Computer Network Defense
DASD S&IO	Deputy Assistant Secretary of Defense for Security and Information Operations
DCI	Director of Central Intelligence
DIA	Defense Intelligence Agency
DIAP	Defense-Wide Information Assurance Program
DIAPSG	Defense Information Assurance Program Steering Group
DII	Defense Information Infrastructure
DIRNSA	Director National Security Agency
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DIOC	Defense Information Operations Council
DOC	Department of Commerce
DOD	Department of Defense
DOE	Department of Energy
DOJ	Department of Justice
DOS	Department of State
FBI	Federal Bureau of Investigation
FEDCIRC	Federal Computer Incident Response Capability
FEMA	Federal Emergency Management Agency
FIRST	Forum of Incident Response & Security Teams
GNOSC	Global Network Operations Security Center
GSA	General Services Administration
I & IA	Infrastructure and Information Assurance
IA	Information Assurance
IC	Intelligence Community
ICC	Information Coordination Center

IMINT	Imagery Intelligence
INFOCON	Information Condition
IO S&I	Information Operations Strategy and Integration
IOSS	Interagency OPSEC Support Staff
IOTC	Information Operations Technology Center
IPI	International Public Information
IPIIWG	International Public Information Interagency Working Group
IPTF	Infrastructure Protection Task Force
IWSC	Information Warfare Support Center
JCIWS	Joint Worldwide Intelligence Communications System
JCMA	Joint Comsec Monitoring Activity
JCS	Joint Chiefs of Staff
JCSE	Joint Communications Support Element
JDISS	Joint Deployable Intelligence Support System
JIOC	Joint Information Operations Center
JIVA	Joint Intelligence Virtual Architecture
JPO-STC	Joint Program Office – Special Technology Counter Measures
JTF-CNO	Joint Task Force – Computer Network Operations
JSC	Joint Spectrum Center
JWAC	Joint Warfare Analysis Center
LIWA	Land Information Warfare Activity
MASINT	Measurement & Signature Intelligence
MPP	Mission Program Plan
NCA	National Command Authorities
NCS	National Communications Systems
NCTF-CND	Navy Component Task Force – Computer Network Defense
NIAP	National Information Assurance Partnership
NIPC	National Infrastructure Protection Center
NIST	National Institute of Standards and Technology
NIWA	Naval Information Warfare Activity
NSA	National Security Agency
NSC	National Security Council
NSIRC	National Security Incident Response Center
NSOC/IPC	National Security Operations Center/Information Protect Cell
NSPD	National Security Presidential Directive
NSTAC	National Security Telecommunications Advisory Committee
NSTC	National Science and Technology Council
NSTISSC	National Security Telecommunications and Information Systems Security Council
NTIA	National Telecommunications & Information Assurance
ONDCP	Office of National Drug Control Policy
OMB	Office of Management and Budget
OSD	Office of the Secretary of Defense
OSINT	Open Source Intelligence
OSTP	Office of Science & Technology Policy
PCAST	President's Committee of Advisors on Science & Technology Policy

PCCIP	Presidential Commission on Critical Infrastructure Protection
PDD	Presidential Directive Decision
PD&PA	Public Diplomacy and Public Affairs
PIR	Priority Intelligence Requirement
POG	Psychological Operations Group
POTUS	President of the United States
PSN	Public Switched Network
RPP	Regional Program Plan
TWI	Transnational Warfare Interests
UCP	Unified Command Plan
USD(P)	Under Secretary of Defense for Policy
USG	United States Government

APPENDIX C – IO and JOPES

Annex B of JOPES addresses intelligence. Though intelligence is not doctrinally a capability or related activity of IO, good intelligence is essential to conducting effective IO. JP 3-13 states that, "offensive IO requires broad-based, dedicated intelligence support." Likewise, good intelligence on a potential adversary's IO capabilities and interests is essential to conducting defensive IO and implementing effective information assurance programs. It is extremely important that this annex address the counter-intelligence aspects of defensive IO, as this information is critical to developing an effective operations security program. While not all of Annex B is dedicated to the discussion of intelligence support to IO, it is essential that the annex discuss support to IO in detail.

Annex C of JOPES addresses operations. In this annex, we find Appendix 3, which some people in the IO community are now calling the IO appendix. The appendix will always have the following five tabs:

- Tab A - Military Deception
- Tab B - Electronic Warfare (EW)
- Tab C - Operations Security (OPSEC)
- Tab D - Psychological Operations (PSYOP)
- Tab E - Physical Destruction

Additionally, there may be a Tab F, addressing CNA. This tab will only be used if the CNA tools discussed are not controlled through a compartmented or special access program. If compartmented CNA tools are used in a classified method, then they will be discussed in Annex S, which is a classified annex published separately from the rest of the OPLAN. Although Annex C does not address CND, it is addressed in Annex K, which is discussed later.

The IO related activities of Public Affairs (PA) and Civil Affairs (CA) have their own annexes. While these annexes are not dedicated entirely to discussing IO issues, it is important that at least a portion of each address how the IO related activity will be integrated into offensive and defensive IO. Annex F discusses PA. Besides addressing support to offensive IO, this annex should not neglect the defensive topic of PA in support of counter-propaganda. Annex G discusses CA. As with Annex F, Annex G must not neglect counter-intelligence and the hostile intelligence threat against CA personnel.

Annex K discusses command, control, and communications (C3) systems. The J-6 is responsible for developing this annex and is usually responsible for the IA program within a command. From the IO perspective, Annex K is largely defensive in nature, dealing with the protection of information systems. The discussion in Annex K will include both active and passive measures to protect information systems and respond to potential threats. This should include risk management, information security, physical security, personnel security, communications security and computer security. Though focusing on defense, this annex should not neglect to discuss the C3 support to offensive IO.

Beyond the defensive considerations in Annex K, defensive IO planners must consider OPSEC, counterintelligence, counter-deception, and counter-propaganda. As stated previously, the offensive and defensive aspects of OPSEC are addressed in Tab C to Appendix 3 of Annex C. Counter-deception should be addressed along with deception in Tab A to Appendix 3 of Annex C. Counter-propaganda should be included with PSYOP in Tab D to Appendix 3, Annex C. Counterintelligence should be addressed in Annex B (Intelligence). A recent change to

JOPES Volume II introduced Annex V, *Interagency Coordination*, to address the extensive coordination requirements needed in the interagency environment. The annex will essentially serve as a CINC IO Cell's "wish list" to submit requests for support to IO to agencies outside of the DOD.

Contributor's Biographies

Ehsan M. Ahrari, Professor of National Security and Strategy, JFSC. Dr. Ahrari contributed the section on Chinese IW efforts, as well as provided guidance for strategic IO interests. He has served as part of the senior staff at Joint Forces Staff College since 1994, working to build the IO curriculum for the Joint Command Warfare School. His previous teaching assignments include the United States Air Force Air War College, Mississippi State University and East Carolina University. A graduate of Southern Illinois University (1976), Dr. Ahrari has published widely with two books and numerous scholarly articles to his credit.

Edwin L. Armistead, Primary Editor for this book, LCDR Armistead is an E-2C Naval Flight Officer, with a number of staff and operational tours in AEW and C3 units, including VAW squadrons, USS *Nimitz* (CVN-68), MAWTS-1 and COMUSNAVCENT. Formerly an IW Instructor at JFSC, he is a graduate of the US Naval Academy, US Navy and US Air Force Command and Staff College, LCDR Armistead is currently entered in a Ph.D. program at Old Dominion University, where he is writing his dissertation on IO. He has written two books on AEW aircraft and a number of articles for professional journals.

Major Robert E. Blackington, USAF. Currently the Chief of Initiatives at the Space Warfare Center, MAJ Blackington was previously a student at the Air Command and Staff College at Maxwell AFB, and before that an instructor at the JFSC. He spent the majority of his career flying the MC-130E and AC-130E gun ship aircraft as a navigator and has over 3000 hours in type. While serving as an IW Instructor at JFSC, he was instrumental in upgrading the the US Air Force IO communities awareness of the role of the former USIA as well as IPI and PDD-68. In addition to providing guidance in these areas, MAJ Blackington, was the main contributor for the section on EW.

Byron Collie, former Federal Agent, New South Wales, Australia. Mr. Collie is recognized throughout the Australian Defence and governmental agencies as "the" expert on Information Assurance and Computer Network Defense issues. He was actively involved in the Eligible Receiver '97 exercise as well as coordinating with the FBI on the Solar Sunrise and Moonlight Maze cases. A graduate of the 1998 AFSC Information Warfare course, Mr. Collie has also served for the last two years as an instructor at the Australian Defence Force Warfare Centre Information operation course. Mr. Collie is currently employed as an Information Assurance analyst in the United States.

1LT Carlton T. Fox, Jr., Student, US Air Force Intelligence Officer. A recent graduate of the Virginia Polytechnic Institute and State University, 1LT Fox earned his Bachelor's degree in Political Science and a Master's Degree in history with a concentration in foreign relations. A key ingredient in the overall success of this book, 1LT Fox served as the assistant editor for this project in edition to writing the section on counter-terrorism and designing the cover. An essential player in bringing this book to print on a timely basis, 1LT Fox is currently enroute to his first assignment in the US Air Force.

Mark R. Goodell, C4I Instructor, JFSC. MAJ Goodell is currently attached to the JFSC, and

most of his prior billets were as a career Space Controller. Stationed in a variety of positions from Flight Commander at Falcon AFB, to Atlas II Launch Controller, Crew Commander at the 73rd and 16th Space Surveillance Squadron, MAJ Goodell also served as a Staff Officer, HQ USAF Space Command. A Graduate of the Air Force Institute of Technology and Brigham Young University, MAJ Goodell has also completed the Air Command and Staff College and Squadron Officer School, and contributed the section on Space and IO for this book.

Dave Harris. LTC, Australian Regular Army (Ret) served for 25 years in a variety of billets in the Royal Australian Armoured Corps including tank gunner/operator and regimental appointments in Tank, Reconnaissance, and Armoured Personnel Carrier regiments. He has also served with the Royal Canadian Dragoons and the United Nations (UNIIMOG), as well as instructing tactics and leadership at the Royal Military College Duntroon. His last posting in the Australian Defence Force was as the Information Operations planner in the Directorate of Joint Plans in Strategic Command.

Zachary P. Hubbard, LTC, US Army (Ret). Former chief of the Information Warfare Division, JFSC from April 1998 – April 2001, LTC Hubbard was a prime advocate for the publication of this book. Commissioned in the Field Artillery, he is also qualified as a counterintelligence and HUMINT officer. LTC Hubbard's operational experience includes service in operations Desert Shield and Desert Storm, Saudi Arabia/Kuwait; JTF Andrew , Florida; CJTF Kismayo, Somalia; Operations Sharp Guard and Deny Flight, Italy; and IFOR/SFOR in Bosnia-Herzegovina. He is currently working for Zeltech Corporation in Hampton, VA as an Information Assurance analyst.

Richard J. Kilroy, Jr., Information Warfare Instructor, JFSC. LTC Kilroy is an Army Intelligence Officer who has served in a variety of Tactical and Strategic Intelligence Staff Officer positions in the U.S. and in Europe. As a Latin American Foreign Area Officer, LTC Kilroy has also served in a variety of politico-military affairs positions in the U.S. Southern Command, to include serving as a Special Assistant to General Barry McCaffrey and General Wes Clark. LTC Kilroy attended the Mexican Command and General Staff College and has authored articles on civil-military relations in Latin America. He holds an MA. and Ph.D. in Foreign Affairs from the University of Virginia.

Dan Kuehl, Professor IRMC at NDU. Dr Kuehl is the Director of the Information Strategies Concentration Program, a specialized curriculum for selected students at the NWC and ICAF. Lt Col Kuehl (ret – USAF) served primarily as a Minuteman ICBM instructor crew commander, nuclear planner at HQ SAC, and on the Air Staff during Operation Desert Shield/Storm. He supported the landmark Gulf War Air Power Survey, and authored the "Air Campaign" chapter in the DOD's *Final Report to Congress on the Persian Gulf War*. He has numerous articles published in journals contributing to the IO and EW fields, and has also co-editing the pending book *Cyberwar 4.0: Information Operations: Applying Power in the Information Age*.

Jeff Malone, CPT, Australian Regular Army. A prior enlisted soldier, he was commissioned in 1992, and has served in a variety of regimental and staff appointments, including appointments in the Information Operations area. CPT Malone is currently posted to the Directorate of Strategy and International Engagement, Future Land Warfare Branch, Army Headquarters. He has a BA

(Honours) and a MA (Research) in Political Science from the University of Western Australia, Perth. At present, he is completing a PhD entitled 'Information Operations and Australian National Security Policy' at the Queensland University of Technololgy, Brisbane.

Robert J. Orr, CDR, USN, Staff Judge Advocate for Commander, Navy Region Mid-Atlantic. Previously he served as Assistant Fleet Judge Advocate Commander in Chief, U.S. Atlantic Fleet. A graduate of Heidelberg College in 1981, CDR Orr received his Juris Doctor from Ohio State University in 1984. He also holds a Masters of Law in International Law from the University of Virginia and is a graduate of the College of College of Command and Staff, U.S. Naval War College. CDR Orr has a strong operational background, with operational cruises on the USS *Midway* (CV-41), USS *Eisenhower* (CVN-69) and USS *Saratoga* (CV-60). CDR Orr is an adjunct instructor for the Joint Forces Staff College and the US Naval War College.

Neil Quarmby, LTC, Australian Regular Army. Commissioned into the Australian Intelligence Corps from the Royal Military College in 1984. He served regimental appointments in Australia's medium artillery regiment and electronic warfare regiment. He has served with the British Army on the Rhine and has been involved in a number of counterintelligence and counter terrorist operations and duties. With Masters Degrees in International Relations and Defence Studies, he has been active in Australian Defence capability development and is currently serving in the Defence Intelligence Organisation. LTC Quarmby contributed to a number of sections throughout the book and has been the driving force behind IO training and doctrine in the ADF.

Tim Thomas, Foreign Military Studies Office, Ft. Leavenworth, KS. LTC Thomas, US Army (Ret.) is a regular guest speaker for the JFSC JIWSOC and JIWOC sessions as well as a nationally recognized expert on Russia and Chinese IW doctrine. He was the featured speaker at the latest Information Warfare Convention 2000 in Washington, D.C. and contributed mostly to the Russian IW section.

Endnotes

[1] Floodnet is a JAVA applet that causes constant search queries of a site by the search engine every nine seconds. It monopolizes compute processor unit time and resources that may cause the server to overload.

[2] Hactivism is the use of Hacker or cyber attacks to promote activism in a particular cause.

[3] RAND. *The Zapatista Social Netwar in Mexico,* Washington, D.C.: RAND Corporation, 1996, Pg. 45.

[4] *Sneakers*, movie, director: Phil Alden Robinson, 1992.

[5] Robert Keohane and Joseph Nye, *Power and Interdependence*, (Boston: Longman, 1989), 23.

[6] John Arquilla and David Ronfeldt, "Looking Ahead: Preparing for Information-Age Conflict," *In Athena's Camp: Preparing for Conflict in the Information Age,* ed. John Arquilla and Daid Ronfeldt (Santa Monica, Ca: RAND, 1997) 441.

[7] Hans J. Morganthau, *Politics among Nations: The Struggle for Power and Peace* (New York: Alfred A. Knopf, 1967), xviii.

[8] Joseph S. Nye and William A. Owens, "America's Information Edge," *Foreign Affairs* 75 (March/April 1996): 22.

[9] Walter B. Wriston, "Bits, Bytes and Diplomacy," *Foreign Affairs* 76 (Sept/Oct 1997): 175.

[10] Barbara Haskell, "Access to Society: A Neglected Dimension of Power," *International Organization* 34 (Winter 1980): 94; Joseph S. Nye, *Bound to Lead: The Changing Nature of American Power* (New York: Basic Books, Inc., 1990), 8; Eliot A. Cohen, "A Revolution in Warfare," *Foreign Affairs* 75 (March/April 1996): 52; Robert O. Keohane and Joseph S. Nye, "Power and Interdependence in the Information Age," *Foreign Affairs* 77 (September/October 1998): 81; Joseph S. Nye and William A. Owens, "America's Information Edge," *Foreign Affairs* 75 (March/April 1996): 20; Walter B. Wriston, "Bits, Bytes and Diplomacy," *Foreign Affairs* 76 (September/October 1997): 172; Richard N. Rosecrance, *The Rise of the Virtual State: Wealth and Power in the coming Century* (New York: Basic Books, Inc., 1999), 16; John Arquilla and David Ronfeldt, "A New Epoch – And Spectrum – Of Conflict," in *In Athena's Camp: Preparing for Conflict in the Information Age,* ed. John Arquilla and Daid Ronfeldt (Santa Monica, Ca: RAND, 1997), 7.

[11] David C. Gompert, *Right Makes Might: Freedom and Power in the Information Age* (Washington, DC: National Defense University, 1998), 5.

[12] Joint Publication 3-13, *Information Operations* (Washington, D.C., Government Printing Office, 9 October 1998).

[13] Joint Chiefs of Staff, *Joint Vision 2010*, (Washington D.C., Government Printing Office, July 1996), Pg. 69.

[14] Information superiority

[15] The first known use of information warfare was in a briefing title and concept written by Dr. Tom Rona (then of Boeing) for Andrew Marshall, May/June 1976.

[16] Neil Munro, *The Quick and the Dead: Electronic Combat and Modern Warfare* (New York: St Martin's Press, 1991), 173.

[17] Department of Defense, DEPSECDEF MEMORANDUM, *Strategic Concept for Information Operations (IO),* by John J. Hamre (Washington, D.C.: 14 May 1999).

[18] Ibid, art. I, sec. 8 (11).

[19] National Security Council Organization Chart (accessed 14 June 1999); available from http:www.whitehouse.gov/wh/eop/nsc. Members include the Chairman of the Joint Chiefs of Staff, Director of Central Intelligence, Secretary of Treasury, Assistant to the President for National Security Affairs, Assistant to the President for Economic Security, United States Representative to the United Nations, and the President's Chief of Staff, in addition to the Attorney General and the head of the Office of National Drug Control Policy.

[20] These include: Council of Economic Advisers, Council on Environmental Quality, National Economic Council (NEC) National Security Council (NSC), Office of Administration, Office of the First Lady, Office of Management and Budget (OMB), Office of National Drug Control Policy (ONDCP), Office of Science and Technology Policy (OSTP), White House Office for Women's Initiatives and Outreach, President's Foreign Intelligence Advisory Board, United States Trade Representative (USTR)
Three of these offices, the NSC, OMB, and OSTP have a direct interest in IO policy, while others, such as the NEC, ONDCP, and USTR are involved on an ancillary basis.

[21] Specific duties assigned to the NSC by law include:
- "The function of the Council shall be <u>to advise the President</u> with respect to the integration of domestic, foreign, and military policies relating to the national security..."
- "...performing such <u>other functions the President may direct</u> for the purpose of more effectively <u>coordinating the policies and functions</u> of the departments and agencies of the Government relating to the national security..."
- "...<u>assess and appraise</u> the objectives, commitments, and risks of the United States..."
- "...<u>consider policies</u> on maters of common interest to the departments and agencies of the Government concerned with the national security..."

[22] This is spelled out explicitly in their list of official functions:
Provide information and policy advice to President; Manage the interagency policy coordination process; Monitor implementation of Presidential policy decisions; Crisis management; Support negotiations; Articulate President's policies; Liaison with Congress and foreign governments; Coordinate summit meetings and national security-related trips

[23] President, Executive Order "President's Council on Year 2000 Conversion," 13073 (4 February 1998).

[24] President, Amendment to EO 13073 (14 June 1999).

[25] President, Executive Order "National Science and Technology Council (NSTP)," 12881 (23 November 1993), and Executive Order "President's Committee of Advisors on Science and Technology (PCAST)," 12882 (23 November 1993).

[26] Ibid.

[27] President, Presidential Decision Directive "Security Policy Coordination" 29 (16 September 1994).

[28] Department of Defense, Undersecretary of Defense for Policy and Assistant Secretary of Defense for Command, Control, Communications and Intelligence, Joint Memorandum, *Direction to the Staff: Seamless Integration between USD(P) and ASD(C3I) regarding*

Information Operations, by Walter B. Slocombe and Arthur L. Money (Washington, D.C.: 1999).

[29] President, Executive Order " United States Intelligence Activities" 12333 (4 December 1981).

[30] President, National Security Telecommunications and Information Systems Security Committee Document (NSTISSCD) "Incident Response and Vulnerability Reporting for National security Systems" 503 (30 August 1993).

[31] President, National Security Decision "National Policy for the Security of National Security Telecommunications and Information Systems" 42 (5 July 1990).

[32] Department of Defense, The Joint Staff, "Information Assurance: Legal, Regulatory, Policy and Organizational Considerations" (August 1999), A-88.

[33] Ibid, 5-2.

[34] President, Interdepartmental Committee on Communications (26 October 1921), updated (21 August 1963) and by Executive Order " Assignment of National Security and Emergency Preparedness Telecommunications Functions" 12472 (3 April 1984).

[35] President, Executive Order "National Security Telecommunications Advisory Committee" 12382 (13 September 1982), continued by EO 12610 (30 September 1987).

[36] Information Assurance, A-79.

[37] To get more information on IATAC and which products are currently available, you can contact their Director Robert Lamb at (703) 289-5454 or iatac@dtic.mil.

[38] Department of Defense, Joint Publication "Joint Doctrine for Information Operations" 3-13 (9 October 1998).

[39] Department of Defense, Chairman, Joint Chiefs of Staff Instruction (CJCSI) "Joint Information Operations Policy (U)" S3210.01A (5 November 1998).

[40] Department of Defense, Joint Chiefs of Staff, "Unified Command Plan Changes 1999" (accessed on 2 March 2000); available at http://www.defenselink.mil/specials/unified/planchanges1.html.

[41] Ibid.

[42] Department of State, "Reform and Restructuring Act (30 December 1998).

[43] President, Presidential Decision Directive "International Public Information" 68 (30 April 1999).

[44] President, Presidential Decision Directive "Critical Infrastructure Protection" 63 (22 May 1998).

[45] President, President's Commission on Critical Infrastructure Protection (PCCIP), "Critical Foundation: Protecting America's Infrastructures" (13 October 1997).

[46] Ibid.

[47] Originally formed as the National Bureau of Standards in 1901, NIST was renamed and reorganized by the Omnibus Trade and Competitiveness Act of 1988, U.S. Code (P.L. 100-418, 102 Stat. 1107).

[48] Department of Commerce, National Institute of Standards and Technology Authorization Act (1989).

[49] Computer Security Act of 1987 (P.L. 100-235) and Information Technology Management Reform Act of 1996, National Defense Authorization Act of Fiscal Year 1996, 10 February 1996 (P.L. 104-106).

[50] Department of Defense, National Security Agency and Department of Commerce, Letter of Partnership "National Security Agency and National Institute of Standards and Technology" (22 August 1997).

[51] NTIA was created by Reorganization Plan Number 1 (1977) and implemented by Executive Order "Relating to the Transfer of Telecommunications Functions" 12046 (25 March 1978).

[52] PDD-63.

[53] Ibid.

[54] A NGO is a transnational organization of private citizens that maintains a consultative status with the Economic and Social Council of the United Nations. NGOs may be professional associations, foundations, multi-national businesses or simply groups with a common interest in humanitarian assistance activities (development or relief).

[55] Sun Tzu, *The Art of War*, 400-320 BC, quoted in JP 2.0, p. IV-14.

[56] JP 3-13, pp. vii-viii

[57] GL-5

[58] Graphically, the fundamental aspects of Intelligence (Relevant Info) and Command, Control, Communications, and Computers (Information Systems) in supporting Information Operations are shown in Figure 1-2, Information Operations Across Time, in JP 3-13, p. I-4.

[59] JP 3-13, p. I-5

[60] The problem with a smorgasbord approach to providing intelligence products is that it increases the likelihood of security breaches and affects a command's Operations Security (OPSEC) posture when "need to know" is thrown by the wayside.

[61] Carl Von Clausewitz, *On War*, 1832, quoted in JP 2.0 *Joint Doctrine for Intelligence Support to Operations*, 5 May 1995, p. IV-1.

[62] General Colin Powell, quoted in JP 2.0, p. IV-7.

[63] In most cases, intelligence officers will generate these on behalf of a commander and then seek approval after the fact, if they have not received specific guidance.

[64] JP 2.0, p. III-4.

[65] DRAFT Revision of JP 2.0, 2nd Final Coordination 13 July 1998, p. II-1.

[66] JP 2-0, Doctrine for Intelligence Support, 9 March 2000, p.II-3.

[67] Different commands have other names, ie EUCOM calls it the Joint Analysis Center (JAC) and JFCOM calls it the Joint Forces Intelligence Center (JFIC).

[68] For a complete description of each category, see DRAFT JP 2.0, Second Final Coordination Copy, 13 July 1998, pp. II-12 through II-13

[69] Robert V. Ackerman, "Military Intelligence Looks Within," *SIGNAL* Magazine, October 2000, p. 16.

[70] Compared to the one contained in the earlier version of JP 2.0, p. II-3.

[71] Most intelligence analysts and collectors understand the system and know how to work it to their advantage. For example, one analyst working scientific and technical intelligence always gave every HUMINT report that cited her CIR a rating "of major significance" simply because the priority of collection against her requirements was so low. Collectors, in turn, who were rated based on the number of evaluations they received "of major significance" learned then to cite her CIR often, knowing they would get top marks simply by asking their sources a few questions related to her intelligence production tasking.

[72] A case in point is the *Mayaguez* Incident in May 1975. When the Cambodians seized the U.S.-flagged merchant vessel, a presidential decision was made to effect a hostage rescue operation. At the time the operation was conducted, there were contradictory intelligence reports on the size of the opposition to be encountered, as well as the location of the captive crew. Furthermore, within the intelligence community, there were no established procedures to deconflict intelligence discrepancies. The Marines who conducted the assault on Kao Tang Island suffered large numbers of casualties due to the underestimated size of the opposition, while the crew of the *Mayaguez* had been released hours earlier from a different location. See Patrick W. Urey, *The* Mayaguez *Operation*, Center for Naval Analysis Document # CNS 1085, May 1991 and LTC Theodore H. Mueller, "Chaos Theory: the *Mayaguez* Crisis," U.S. Army War College, Carlisle, PA, March 1990

[73] *A Consumer's Guide to Intelligence*, Central Intelligence Agency, Document Number PAS 95-00010, July 1995, and p. 39.

[74] *CJCS Report on the Roles, Missions, and Functions of the Armed Forces of the United States*, February 1993, quoted in DRAFT JP 2.0, p. IV-1.

[75] DRAFT JP 2.0, p. IV-8.

[76] JP 2-01.3 *Joint Tactics, Technique and Procedures for Joint Intelligence Preparation of the Battlespace*, 24 May 2000.

[77] Ibid.

[78] Items known as OCOKA: observation, cover and concealment, obstacles, key terrain, and avenues of approach.

[79] In 1995, when NATO bombed Serbia to pressure Milosevic to back off supporting Bosnian Serbs, he did capitulate after a couple days of intense air strikes. During the Kosovo conflict, intelligence analysts failed to calculate the psychological, historical, and cultural ties of Serbs to Kosovo that was much stronger than those to Bosnia-Herzegovina. In addition, Milosevic was willing to risk his country's survival (and his political survival) over Kosovo.

[80] JP 3-13 p. II-11 through II-13

[81] JP 3-13, p. I-10

[82] Ibid, p. III-1

[83] Former Secretary of Defense, Dick Cheney, quoted in *Concept for Future Joint Operations: Expanding Joint Vision 2010*, The Joint Staff, May 1997, p. 14.

[84] JP 3-13, p. GL-5

[85] A precedent-setting case occurred on September 9, 1998, where the Pentagon, having advanced notice of a cyber-attack, actively shut down the Internet browsers of those logging in to participate in the attack. See George Seffers, "Thwarted Hackers Call Pentagon Actions 'Offensive'," *Army Times*, October 12, 1999.

[86] Joint Publication 3-13, I-9.

[87] The Insider Threat to U.S. Government Information Systems, NSTISSAM INFOSEC/1-99 July 1999, National Security Telecommunications and Information Systems Security Committee

[88] Richard Clarke, Director NSC, CBS 60 Minutes, 9 April 2000.

[89] http://www.defenselink.mil/news/Jan2000/t01052000_t104myer.html

[90] CJCS MEMO CM-510-00, 10 March 1999

[91] Information Assurance Defense In Depth, JCS 2000

[92] Deputy Secretary of Defense, Implementation of the Recommendations of the Information Assurance and Information Technology Integrated Process Team on Training, Certification and Personnel Management in the Department of Defense, 14 July 2000

[93] Office of the Assistant Secretary of Defense Command,Control,Communications,and Intelligence, DOD CIO Annual Information Assurance Report, April 2000.

[94] For more information on these different organizations and their efforts, see the following web site: http://www.biometrics.org/.

[95] General Henry H. Shelton, Chairman, Joint Chiefs of Staff, The Transatlantic Commitment at *"NATO at 50"* conference, London, 08 March 1999.

[96] Bruce Hoffman, *Inside Terrorism*, New York: Columbia University Press, 1998, Pg. 13.

[97] Walter Laqueur, *Terrorism*, Boston: Little, Brown and Co., 1977, pg. 7.

[98] U.S. Department of Justice. *Terrorism in the United States 1997*, (Washington, D.C.: Federal Bureau of Investigation, 1998), Pg. ii. In their book *Political Terrorism*, Schmid and Jongman cited 109 different definitions of terrorism, which they obtained in a survey from leading terrorism scholars. From these definitions, the authors isolated the following recurring elements, in order of their statistical appearance in the definitions: violence, force 83.5% of the definitions; political 65%; fear, emphasis on terror 51%; threats 47%; psychological effects and anticipated reactions 41.5%; discrepancy between the targets and the victims 37.5%; intentional, planned, systematic, organized action 32%; methods of combat, strategy, tactics 30.5%.[98]

[99] U.S. Department of Justice. *Terrorism in the United States 1997*, (Washington, D.C.: Federal Bureau of Investigation, 1998), Pg. ii. (Includes the following definitions)

[100] Cited in Richard W. Leeman, *The Rhetoric of Terrorism and Counterterrorism*, New York: Greenwood Press, 1991, pg. 11.

[101] Walter Laqueur, *The Age of Terrorism*, (Boston: Little, Brown, 1987), pg. 306.

[102] Ibid.

[103] Cited in Richard W. Leeman, *The Rhetoric of Terrorism and Counterterrorism*, (New York: Greenwood Press, 1991), pg. 19.

[104] Secretary of State Madeleine K. Albright, American Legion Convention, September 9, 1998.

[105] For a more in-depth discussion of the classification of these seven types of terrorist groups please see *Counter-terrorism Information Operations Case Study* by The Rendon Group, August 1999.

[106] Eds. Carnes Lord and Frank Barnett, *Political Warfare and Psychological Operations: Rethinking the US Approach*, Washington, D.C.: National Defense University Press, 1988, 160.

[107] The Clinton Administration announced Presidential Decision Directive 39 on June 21, 1995, which stood as the United States counterterrorism policy and that left a great deal of implemental discretion to federal agencies. It is a very simplified, broad approach to combating terrorism.

[108] WMD means chemical, biological, or nuclear weapons employed by terrorists.

[109] OMB Annual Report

[110] Office of the Press Secretary, Fact Sheet: Countering Terrorism PDD 62, Washington: White House, May 22, 1998.

[111] http://www.nipc.gov/history.htm

[112] Many of the functions of this new office are very similar to those of the National Domestic Preparedness Office. Both aim to improve coordination efforts among federal counterterrorism agencies as well as review existing federal programs. However, this new office would not have the authority to affect the daily operations of such agencies as the FBI, DOJ, or the Department of State. This is the same problem the National Coordinator for Security, Infrastructure Protection, and Counterterrorism within the National Security Council faces: the lack of authority to affect actual counterterrorism operations and expenditures.

[113] GAO/NSIAD-99-135 Combating Terrorism Pg. 10

[114] U.S. Department of Justice, FEMA, TOPOFF and NCR-2000 Fact Sheet, http://www.ojp.usdoj.gov/osldps/230ag2.htm The Office for State and Local Domestic Preparedness Support (OSLDPS) within the DOJ arranged this planning conference in Chantilly, Virginia. The sites for the training exercise were Portsmouth, New Hampshire and Aurora, Colorado. The conference selected these sites since those that attended the conference believed the OSLDPS should choose one city that has had Nunn-Lugar-Domenici Domestic Preparedness Training under the DOD, and one city that has not had the training.

[115] James Notter and John McDonald. *Building Regional Security: NGOs and Governments in Partnership*, (Washington, D.C.: Institute for Multi-Track Diplomacy, July 1998), Pg. 1.

[116] Ibid., Pg. 1.

[117] http://www.fas.org/irp/crs/95-112.htm

[118] Ibid.

[119] U.S. Department of State Annual Report on Global Terrorism 1996-1999.

[120] The White House, *Remarks by the President to the Opening Session of the 53rd United Nations General Assembly*, (New York, New York: Department of State, 1998), Pg. 1.

[121] Federation of American Scientists. *U.S.-EU Counterterrorism Summit*, May 18, 1998.

[122] Lieutenant General S. Bogdanov, Former Chief of the General Staff Center for Operational and Strategic Studies, October 1991, quoted in JP-3-13, p. II-15.

[123] JP 3-13, p. GL-9

[124] JP 3-13, p. viii

[125] Interestingly, within Australian IO doctrine this is referred to as “decision superiority.”

[126] This observation was made by Brigadier General John Goodman, Chief of Staff, U.S. Southern Command during an office call in Miami, FL, September 1998.

[127] Office of the Press Secretary, The White House, *Remarks by the President on Keeping America Secure for the 21st Century*, National Academy of Sciences, Washington, D.C., January 22, 1999.

[128] Department of Defense, The Joint Staff, "Joint Publication 3-13" (9 October 1998), GL-5.

[129] “Satellite Spying Cited by Johnson.” The New York Times. March 17, 1967. Internet source: (http://webster.hibo.no/asf/Cold_War/report1/williame.html)

[130] White House Press Release, May 1, 2000, “Improving the Civilian Global Positioning System (GPS)”

[131] The use of the media as a tool of an information campaign has been given a new term in the last decade, namely Soft Power. First coined in his book *Bound to Lead*, Joseph Nye

defined soft power as the capability that you get when someone wants to be like you. He went on in later Foreign Affairs articles to explain that soft power is the ability to achieve goals through attraction rather than coercion. It works by convincing others to follow or getting them to agree to norms and institutions that produce the desired behavior.

[132] PDD-56

[133] International military information are overt/public activities to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning and ultimately the behavior of foreign governments, organizations, groups and individuals.

[134] Pilecki, 6 June

[135] Summe, 6 June

[136] A great number of excellent resources exist which can provide an authoritative and exhaustive discussion of the issues I will identify in more detail. At the least these include the following, from which much of the text of this paper is developed:

a) An Assessment of International Legal Issues in Information Operations, a paper written by the Department of defense Office of General Counsel and released in May 1999.
b) Michael N. Schmitt; *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 Colum. J. Transnat'l L. 885 (1999)
c) Michael A. Sussmann; *The Critical Challenges from International High-Tech and Computer-Related Crime at the Millenium*, 9 Duke J. Comp. & Int'l L. 451 (Spring, 1999)

[137] U.N. Charter, Art 1.

[138] For an outstanding discussion of this balance and its basis in international jurisprudence, see Col. James P. Terry, USMC (Ret.), *responding to Attacks on Critical Computer Infrastructure: What Targets? What Rules of Engagement?* 46 Naval L. Rev. 170 (1999).

[139] U.N. Charter, Art. 24.

[140] Compare the text in Articles 41 and 42 to the language in Article 2(4) and Article 51.

[141] U.N. Charter, Art 48-49.

[142] See, for example, Article 86 of the Law of the Sea Convention and Article 35 of the International Telecommunicatons Convention

[143] Article 38, International Telecommunicatons Convention

[144] On this aspect, see the discussion at page 4 of the DOD General Counsel Memorandum, cited note 1, *supra.*

[145] The law of Armed Conflict recognized the likelihood of applying the protections in the face of technological change. For example, the preamble to the Hague Convention IV eclares that, in cases not specifically addressed, civilians and combatants "remain under the protection and the rule of the principles of the laws of nations, as they result from the usages established among civilized peoples, from the laws of humanity, and from the dictates of the public conscience."

[146] See DOD General Counsel Memorandum, *supra* Note 1, at pp. 6-7

[147] See NWP 1-14M *Commander's Handbook on the Law of Naval Operations*, Section 8.1.1

[148] Additional Protocol I to the Geneva Conventions, Art 52(2).

[149] *Supra,* Note 12.

[150] Hague Convention IV, Art. 24

[151] Unclassified Brief *Information Operations: Legal and ROE Issues* provided by Phillip A. Johnson, Consultant to ASD (C3I) to the Law of Military Operations classes at the Naval Justice School, Newport, RI.

[152] These include, at the federal level, the following statutes:

18 USC 1029: Access Device Fraud

18 USC 1030: Computer Fraud Act

18 USC 2500 and 2511: Wiretaps and other Interception and Disclosure of Wire, Oral, or Electronic Communication

18 USC 2701: Stored Wire and Communication Access

18 USC 1343: Wire Fraud

18 USC 1363: Malicious Mischief

18 USC 1367: Interference with Satellites

18 USC 2701: Stored Electronic Communications

[153] Michael A. Sussmann; *The Critical Challenges from International High-Tech and Computer-Related Crime at the Millenium*, 9 Duke J. Comp. & Int'l L. 451 (Spring, 1999) at 458.

[154] *Id.* At 471.

[155] Jen Jui-Wen, "Latest Trends in China's Military Revolution," translation from FBIS-CHI-96-047, pp. 1-4.

[156] Russian National Security Concept, Nezvisimoye Voyennoye Obozreniye, 26 November 1999, as translated and downloaded from the FBIS Web page on 29 November 1999.

[157] E. A. Belaev, "Informatsionnaya bezopasnost' kak global'naya problems" [Information Security as a Global Problem], a chapter in, *Global'nye problemy kak istochnik chrezvychaynykh situatsiy* [Global Problems as a Source of Emergency Situations] (location: URSS, 1998), edited by Iu. L. Vorob'ev, p. 125.

[158] Joseph Nye, "Redefining the National Interest," *Foreign Affairs*, Vol. 78, No. 4, p. 26.

[159] Ibid., p. 24.

[160] Ibid.

[161] A. A. Kokoshin, "Voenno-politicheskie i ekonomicheskie aspekty reformy vooruzhennykh sil Rossii (Military-political and economic aspects of reform of the Russian armed forces), Voyennaya Mysl (Military Thought) No 6, 1996, p. 9.

[162] V.I.Tsymbal, "Kontseptsiya 'informatsionnoy voyny'"(Concept of Information Warfare), talk given at a conference in Moscow in September 1995, p 7.

[163] S. P. Rastorguev, *Informatsionnaya voina* [Information War], (Moscow: Radio and Communication, 1998).

[164] V. D. Tsigankov and V. N. Lopatin, *Psikhotronnoe oruzhie i bezopasnost' rossii* [Psychotronic Weapons and the Security of Russia], (Moscow: Sinteg, 1999).

[165] Even the military has written about the subject of psychotronic weapons in its publications. For example, see I. Chernishev, "Polychat li poveliteli 'zombi' blast' nad mirom," [Can a ruler make 'Zombies' out of the world]", *Orientir* [Orienteer], February 1997, pp. 58-62.

[166] Marshal Igor Sergeyev, comments in *Kraznaiya Zvesda* [*Red Star*], 9 December 1999 (no page given), as translated and downloaded from the FBIS web page on 9 December 1999. All of Sergeyev's comments in the next 8 paragraphs are from this document.

[167] Based on a discussion with modelers at the General Staff Academy in December, 1991.

[168] Author's discussion with General-Major (retired) V. D. Riabchuk, Fort Leavenworth, September 1996.

[169] Ibid.

[170] Lt Gen Huai Guomo, "On Meeting the Challenge of the New Military Revolution," translation from FBIS-CHI-96-130, pp. 1-7

[171] Su Enze, "Logical Concept of Information Warfare,"translation from FBIS-CHI-96-135, pp. 1-5.

[172] Lei Zhoumin, "Information Warfare and Training of Skilled Commanders," translation from FBIS-CHI-96-036, pp. 1-5.

[173] Renzhao, op. cit., pp. 4-5.

[174] Ibid., p. 4.

[175] Xu Chuangjie, "Military Revolution Gives Impetus to Evolution in Command," translation from FBIS-CHI-96-030, p. 1.

[176] Xu Chuangjie, "Military Revolution Gives Impetus to Evolution in Command," translation from FBIS-CHI-96-030, p. 1.

[177] Ibid., pp. 1-2.

[178] Wei Jincheng, op. cit., p. 3.

[179] Zhou Li and Bai Lihong, "Information Warfare Poses Problems," translation from FBIS-CHI-96-014, pp. 1-2.

[180] Zhou Li and Bai Lihong, "Information Warfare Poses Problems," translation from FBIS-CHI-96-014, pp. 1-2.

[181] Chou Hsi, "Exploration and Analysis of Military Computer Security and Virus Protection," translation from FBIS-CHI-96-116, pp. 1-6.

[182] Interview between Martin Libicki and Dr. Ahari. The Chinese have proven themselves remarkable in indigenizing Marxism to suit their cultural requirements. They are likely to develop information-based warfare techniques to suit their special needs before too long. The United States must remain specially sensitive to this profound historical reality about the PRC.