Information Warfare and Deterrence

Written By

Gary F. Wheatley

Richard E. Hayes

NDU Press Book

December 1996

Table of Contents

Foreword

This report documents the sixth in a series of workshops and roundtables organized by the Institute for National Strategic Studies (INSS) Directorate of Advanced Concepts, Technologies, and Information Strategies (ACTIS). These meetings bring together operators, planners, researchers, and analysts to identify and examine those aspects of command and control and information warfare of contemporary interest. The results are used to increase the dialogue and understanding of the subjects and to develop Mission Capabilities Packages (MCP) that support U.S. Armed Forces in joint, combined, and coalition operations.

Earlier workshops identified "information warfare and deterrence" as a subject that has strong command and control implications that need to be examined in light of our nascent understanding of IW. The workshop was convened to examine this subject in some detail.

ACTIS combines the research and education resources of NDU by merging the Center for Advanced Concepts and Technology (ACT) with the School of Information Warfare and Strategy (SIWS) under a single Directorate. This Directorate serves to improve the state of the art and practice of command and control and information warfare by undertaking selected research and analysis initiatives and by serving as a bridge between the operational, technical, analytical, and educational communities. The Center focuses on emerging requirements and mission areas where new concepts are needed. IW is clearly one of those areas.

Individuals interested in participating in this initiative or other ACTIS-sponsored activities are invited to contact either myself; Mr. Larry Wentz (Director of ACT) at 202-685-2263; or Dr. John Alger (Dean of the School of Information Warfare and Strategy) at 202-685-2249.

Dr. David S. Alberts
Director, ACTIS

Acknowledgments

The authors wish to acknowledge the efforts of several colleagues who supported this work in a variety of ways. The Proceedings, Strategic Forums, and other publications from the ACT and ACTIS workshops and roundtables are the products of serious work by dozens of professionals representing not only all the military services and The Joint Staff, but also staff members at NDU, outside academics, civilian researchers, and representatives of the Department of State, the Department of Energy, the intelligence community, and other interested U.S. Government agencies. Captain William H. Round, U.S. Navy, the former Director of ACT, was, as always, the unifying force that brought the many elements of the effort together. The Evidence Based Research, Inc. (EBR) team of Kenneth E. Kaizer, Karen R. Nickens, and Astrid C. Pardo, led by Richard L. Layton (EBR's Director of Military Studies), handled the myriad of details involved in making the workshop a smooth running success and a most productive experience. Lt. General James R. Brickel USAF (Ret.) was particularly helpful throughout the effort, both in organizing the workshop and drafting the proceedings. Constructive criticism of earlier drafts by Martin C. Libicki, Vice Admiral Henry C. Mustin USN (Ret.), and General Brickel was very helpful to the authors and assisted us in making a more readable document. Finally, Rosemaria B. Bell and Lydia Candland took the report from draft to print, coordinating with the NDU Press.

Executive Summary

Background

Information Warfare (IW) and Deterrence was the focus of the sixth workshop in a series sponsored by the Directorate of Advanced Concepts, Technologies, and Information Strategies (ACTIS), of the National Defense University. The topic arose from both (1) issues that surfaced in earlier workshops on subjects as diverse as Coalition Command and Control (C2), Technologies and Operations Other Than War (OOTW), and Command Arrangements for Peace Operations; and (2) interests expressed by ACTIS sponsors in the Joint Staff (J-6) and the Office of the Secretary of Defense, Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASD/C3I).

The Workshop focused on three principal issues:

- What, in today's world, do the terms "Deterrence" and "Information Warfare" mean, and how are they related?
- How might IW attacks on the United States be deterred, if at all? This issue was broken, for practical analysis, into "cyber-attacks" and "media warfare" attacks.
- Can the United States use IW to deter attacks on itself, its allies, or its interests?

As with past ACTIS workshops, this one brought together senior analysts and technical experts, as well as active military leaders and action officers with operational responsibility in the affected areas, for a non-attribution discussion working toward consensus or clear articulation of alternatives and their consequences. This workshop was conducted at the Secret level, which inhibited discussion of some topics largely by preventing discussion of particular systems and examples. However, the participants were able to engage in a rich give-and-take and achieved a high degree of candor.

Key Concepts and Implications

On one level, deterrence and information warfare are well matched. Both belong to the world of robust ideas with broad implications. Both are highly relevant to the post-Cold War era in which conflict has been transformed from bipolar global structures to multi-sided, local and regional contests in which the military element is a crucial part of, but not the driving force for, competition and conflict. On the other hand, the two topics can be seen as orders of magnitude apart. IW is a huge domain, ranging from media wars to electronic combat and from economic competition to strategic conflict waged against civilian populations. Deterrence, while it has proven robust (i.e., applies across a range of situations), actually is a narrow concept that works only under a set of quite restrictive assumptions. Not surprisingly, therefore, the workshop participants found the relationship between the two concepts to be spotty -- highly relevant on some topics, marginally so on others, and not at all relevant in many areas.

Deterrence in the Information Age

The concept of deterrence is well understood. The workshop readily reached consensus on a basic definition of deterrence as *"prevention or discouragement, by fear or doubt, from acting."* Clearly, this definition implies an actor and a target. Moreover, the group also agreed on a simple set of conditions necessary for successful deterrence. These were seen as:

- A threat to something of value that exceeds the perceived gain of non-compliance.
- A clear statement of the behavior to be avoided or performed.
- Clear and unambiguous communication of the threat and the desired or proscribed behavior to the target.
- Credible threat, meaning that the target believes the actor has the will and capability to execute the threat.
- Situational constraints that make it impossible for the target to avoid punishment.
- Controllability of the threat and its implications by the actor.

On the other hand, workshop participants were well aware that "deterrence theory" was largely a product of the Cold War era. This suggests that those whose experience is from that era may bring extraneous concepts or baggage to the topic. Hence, they readily agreed that deterrence applications outside the nuclear war arena must be thought through carefully and should be exposed to domain experts from the appropriate arenas before they are considered mature.

The Domain of Information and Information Warfare

The read-ahead package for the workshop included a paper that stressed the size and complexity of the information warfare domain (see Appendix B). As illustrated in the paper, three relatively independent dimensions are required to capture and describe the information warfare arena: the degree of conflict/cooperation, substantive focus (political, military, social, economic, etc.), and the nature of the actors involved (individuals, private organizations, nation states, international organizations, the general public, media, etc.).

The workshop participants generally accepted the broad nature of the information warfare domain and the central role of information systems and processes in the world today. However, they inferred several very important implications from this broad characterization of the relevant domain.

- First, the term "information warfare" is used to mean many things, but is often focused on the military domain or the cyber-war domain dominated by computers. This narrow definition is inconsistent with the broad policy questions relevant to competition and conflict using information media.
- Because information warfare is really a broad and diverse arena, analysis of it must be focused on selected elements, which must be clearly defined in each

application. Overall, the field is so broad that virtually no meaningful generalizations can be drawn about it.

- Isolation, except in rare instances, of military, national, public, and private information systems is all but impossible today. Even very important military traffic is likely to be carried on national infrastructure systems. Public and private sectors are heavily interdependent, and this linkage will continue to grow.
- A whole raft of information systems make potential targets -- banking systems, control systems for railway operations, air control systems, control systems for pipelines, media systems, and others. Only a fraction of these are primarily military or under the direct protection of the Department of Defense (DoD).
- As has been stressed by ADM Owens as Vice Chairman of the Joint Chiefs of Staff, the civilian sector is no longer a sanctuary that can be protected by interposing military forces between adversaries and their targets. Traditional military forces can be flanked at the speed of light by information age attacks on the general population or key economic systems.
- More profoundly, there is no consensus on the appropriate boundary between the military and Department of Defense roles and missions, those of the law enforcement and intelligence systems, and those of the commercial sector.

Workshop participants were aware of a variety of policy initiatives to create interagency working groups and coordinating mechanisms as well as public-private dialogues and mechanisms for both exchanging information and developing plans for dealing with information age threats that cut across communities. Considerable progress has been made in generating better awareness of the threat and some effort has been made toward cooperation. However, the general consensus was that these helpful activities were only now developing momentum and were far from successful completion.

Information Warfare and Deterrence

At the abstract level, the interface between these two concepts is dependent on setting the context clearly. First, deterrence is always from an actor toward a target. The very nature of the actor and target, as well as the degree of asymmetry between them, is important.

Moreover, the nature of the relationship between the parties is important to the analysis. Hence, specification of the context (type of relationship, nature of the actors, substantive domain) is essential before any conclusion is possible about the potential or actual effectiveness of deterrence.

The most important insight arising from looking at the two concepts, however, is the fact that they are only relevant to one another in highly selective contexts. The analogy that emerged was that of a steamroller and a wrench. Both are tools and, depending on the situation, appropriate wrenches may be useful for, or even crucial to, the operation of the steamroller. However, most of the things the steamroller does are irrelevant to the wrench and most of the things the wrench can be used for do not involve a steamroller. In many cases, therefore, the workshop found itself venturing away from a pure consideration of the two concepts and into meaningful discussions in areas related to one or more of the central topics.

How Might IW Attacks on the United States Be Deterred?

Workshop participants divided discussion of this topic into two very different topics: deterring attacks directed through computers and their connectivity (cyber-war attacks) and those directed at the general public through public media such as television, radio, and print. Indeed, one of the most profound dimensions of disagreement among workshop participants was the degree to which the Department of Defense ought to consider media attacks at all. However, because media messages can influence, and arguably have (Beirut bombing, Mogadishu television pictures, etc.) influenced, both the tasking of military assets and mission accomplishment, both types were examined.

Cyber-War Attacks

Considerable discussion was required for the group to agree on the wide range of types of computer attacks that must be considered. Initially, some felt the discussion should focus only on protection of internal DoD systems, while others wanted to include broad strategic or operational attacks on the banking system or other commercial or quasi-governmental arenas. The workshop was aware, however, of an ACTIS analysis of Defensive Information Warfare (Appendix D) that differentiates attacks by their targets and implications into:

- **Day-to-day or routine attacks with limited or diffuse impact on U.S. interests.** These include ônormalö hacking for fun and profit, typical white collar crime, and other attacks with discrete impact.
- **Potentially strategic (catastrophic) attacks.** These are limited attacks with unpredictable consequences that could, under some circumstances or in some combinations, have catastrophic implications for U.S. interests. For example, an attack on a single bank, even if the losses are large (millions), is no threat to the U.S. banking system. However, an orchestrated and publicized series of successful attacks on individual banks could undermine confidence in the banking system and create a much more serious problem, even though the specific attacks were each quite limited.
- **Strategic (catastrophic) attacks** are those which, if successful, will in themselves do great harm to the United States. Destruction of the systems that control systems in key industries and leave them so they cannot be repaired promptly would fall in this category.

In addition, workshop participants stressed that not all information warfare attacks on computer systems need take the form of computer intrusion. Physical destruction of crucial telephone switching stations or other national information infrastructure assets would, themselves, be very damaging.

One significant finding was that the workshop participants consistently found themselves assuming that a visible set of defenses was the beginning point for deterring attacks on important computer systems. In essence, the argument was that information attacks are

instrumental acts and will not occur if the attacking party perceives little opportunity for success.

At the same time, the workshop also noted that "success" has very different meaning for different types of actors and that some individuals, particularly those with ôtypicalö hacker attitudes, would be likely to perceive a more robust defensive posture as a challenge, not as discouragement. This, of course, is a lesson in the need for specific contexts when discussing deterrence and IW. What works in some circumstances may be very wrong in others.

Regardless of whether good defenses necessarily deter attacks, there was consensus that the set of defenses now in place is inadequate for discouraging any but the least well prepared intruder. Not only are systems poorly protected, very few intrusions are detected (reportedly about 5%) and few of those (another 5%) are actually reported, even within the Department of Defense. If these figures are correct, the likelihood of knowing about an attack is .0025 (one-quarter of one percent) and the risk of being caught must be, by definition, even lower. Improved indications and warning (I&W), as well as improved reporting of detected attacks, are essential elements of improved defensive systems. In this context, the workshop also concluded that assessing the ability of DoD or others to deter attacks will require a sound understanding of the pattern of attacks being experienced. Better data collection as well as I&W was also a priority.

Finally, a variety of defensive measures were identified for computer systems. These are not unique to the deterrence arena, but rather reflect the workshop participants' assumption that some attacks will be deterred by effective defenses. The technical representatives in the workshop also stressed that for the foreseeable future the advantage in the cyber-war arena will lie with the offense. Hence, building defenses does not guarantee success. Creating redundancy as well as the capacity to contain, recover from, and reconstitute in spite of successful attacks are essential elements of a successful deterrence strategy. Vice Admiral Cebrowski, the JCS J-6, argued, in his luncheon presentation to the workshop, that decoupling information attacks from their purpose is an effective deterrent.

Media War

The workshop explored the potential for media attacks to deter effective military action in a Middle Eastern context. The scenario involved a campaign aimed initially at public attitudes in friendly and other regional countries whose cooperation is essential for major U.S. operations in and around the Persian Gulf, and later at public attitudes in the United States. The thrust of the argument was that prudent, even essential, military actions could well be called into question through media attacks with primarily political messages. Several conclusions emerged from these discussions.

- First, because of its democratic traditions and freedom of speech considerations, the U.S. is almost certainly going to be placed in a reactive mode if a media war campaign is launched.

- Second, foreign powers will find it difficult to intimidate U.S. leaders or to put forward obviously false information toward the U.S. public without effective U.S. media responses, but may be able to communicate quite inaccurate images to selected foreign publics who are predisposed to believe them.
- Third, the infrastructure to deliver television images into distant regions may not be readily available within DoD, particularly in a non-warfare situation where the sovereignty of foreign states must be respected.
- Fourth, wargames and seminars are needed involving not only DoD, but across the range of civilian agencies and industry representatives necessary for effective television imagery and counter-imagery in media wars.

Media warfare can put enormous time pressure on U.S. and allied decision making, particularly when the adversary is an authoritarian state with little or no necessity for either internal or international consultation.

Core Conclusion About Deterring Information Warfare Attacks on the United States

While recognizing that the variety of potential attackers, attack contexts, and arenas where information warfare attacks may take place is vast and too complex for simple solutions, the workshop participants were confident that the United States already has basic policies in place that serve as effective deterrents in many circumstances. *In essence, some information warfare attacks on the United States are deterred by the same policy that deters other types of attack. Acting under its rights as a sovereign state, the U.S. stands ready to respond to any attack on its interests with all appropriate means, including law enforcement as well as military capacity.*

Finally, the workshop recognized that considerable legal work needs to be completed in this arena. First, U.S. law (both state and federal) needs to be clear about the definition of crimes in the information arena. Second, international agreements and treaties are needed to ensure that foreign attackers can be prosecuted effectively and that acts of war are clearly identifiable.

Using Information Warfare to Deter Foreign Governments

In large measure because the discussion on defending against information operations was so rich, but also to a certain extent because of the relatively low level of classification for the meeting, this topic was addressed more quickly and in less detail than the others.

Some limits on U.S. offensive activities were noted. First, media manipulation that involves government personnel providing false information is neither politically wise nor consistent with U.S. policy and law. Second, information attacks are attacks and therefore subject to international law.

Those limits having been noted, the workshop participants also recognized that the technical capacity to render an adversary "ignorant," poor, uncertain of the capability to

control its own forces, unable to communicate with its population, or uncertain of the quality of its basic information, could have a profound effect on its willingness to undertake a military adventure and thus equate to a powerful deterrent.

Moreover, while barely unveiling the true potential of highly leveraged information and superior battlefield awareness, *Desert Storm* has provided the world with a demonstration of the potential advantage of information dominance. Finally, the workshop concluded that research and development into tools and techniques that can impact potential adversaries' knowledge of the battlefield, control of their own forces, resources necessary to support armed conflict and deliver services to their populations, or leverage uncertainty about their own information, should go forward.

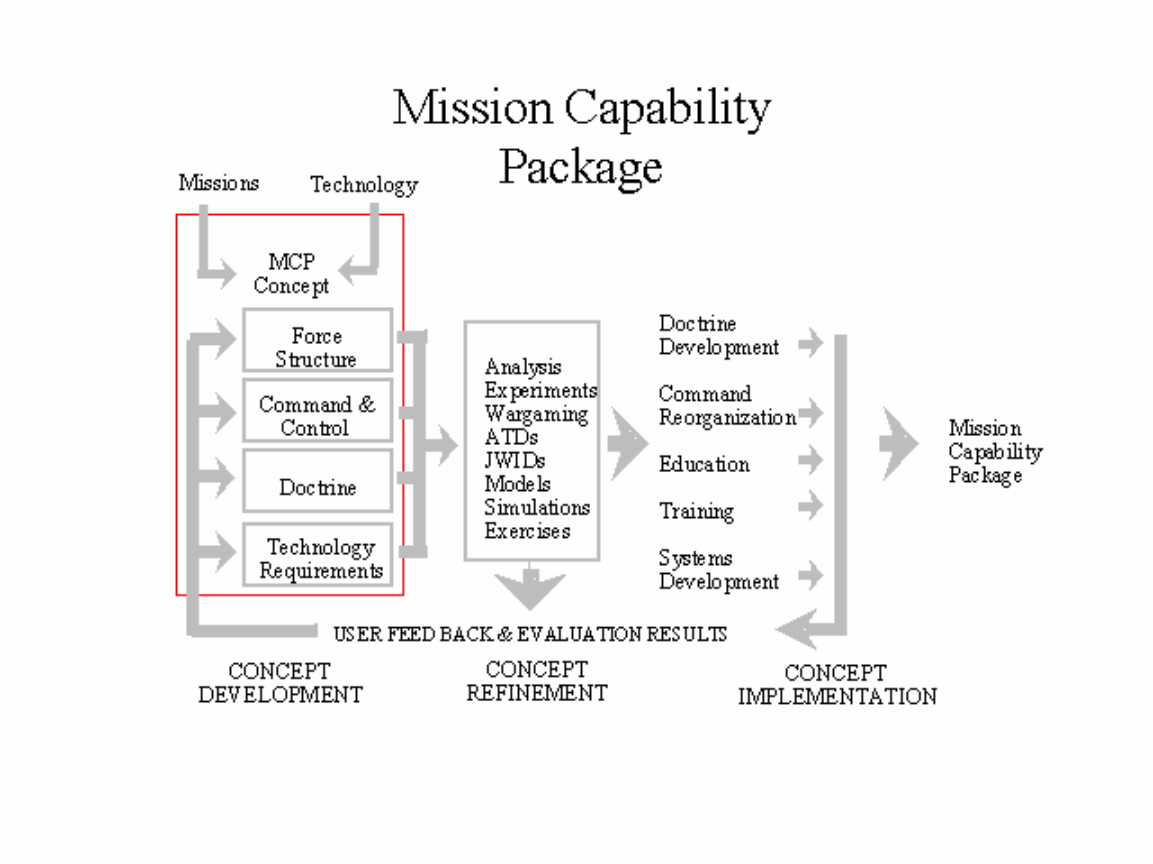
A series of more focused roundtables (smaller working groups with selected expertise) is planned to follow up on significant issues left unresolved or where more sensitive issues need to be considered.

Chapter 1: Terms of Reference

Background and Purpose

The Workshop on Information Warfare and Deterrence was held at the National Defense University as the sixth in a series sponsored by the Directorate of Advanced Concepts, Technologies, and Information Strategies (ACTIS). The topic arose both from (1) issues that surfaced in earlier workshops on subjects as diverse as Coalition Command and Control (C2), Technologies and Operations Other Than War (OOTW), and Command Arrangements for Peace Operations; and (2) interests expressed by ACTIS sponsors in the Joint Staff (J-6) and the Office of the Secretary of Defense, Assistant Secretary of Defense for Command, Control, Communications and Intelligence (ASD/C3I).

As with past ACTIS workshops, this one brought together senior analysts and technical experts, as well as active military leaders and action officers with operational responsibilities in the affected areas, for a non-attribution discussion working toward consensus or clear articulation of alternatives and their consequences. The list of attendees is included as Appendix A. The overall goal of the workshop series is to conceptualize and develop Mission Capability Packages (MCPs) that will support effective decision making and command and control in arenas where DoD has significant responsibilities. As Figure 1 illustrates, MCPs are coherent blends of doctrine, command organization, education, training, systems, and force structure that increase the likelihood of mission accomplishment across a range of anticipated situations and threats. Workshops are a beginning point for MCPs, suggesting novel concepts for later revision and analysis. As this process develops, the MCP is refined and its implications become better understood until an implementable concept emerges which can be passed from the research and development community to the practical world of implementation and action.



Workshop Objectives

When exploring new or relatively new concepts like the relationship between IW and deterrence, analysts can be fairly certain that outcomes will likely be different than expectations. With this in mind the workshop sought to bound the initial explorations to those that might logically be achieved in a two-day effort. The workshop focused on three principal issues:

- What, in today's world, do the terms "deterrence" and "information warfare" mean and how are they related?
- How might IW attacks on the United States be deterred, if at all? This issue was broken, for practical analysis, into "cyber-attacks" and "media warfare" attacks.
- Can the United States use IW to deter other kinds of attacks on itself, its allies, or its interests?

This workshop was conducted at the Secret level (except for one unclassified discussion of media war). Being restricted to classification levels no higher than Secret inhibited discussion of some topics largely by preventing discussion of particular systems and examples. However, the participants were still able to engage in a rich give-and-take and achieved a high degree of candor. A series of more focused roundtables (smaller working groups with selected expertise) is planned to follow up on significant issues left

unresolved or where more sensitive issues need to be considered. Evidence Based Research, Inc. served as workshop organizer and rapporteur for the discussions.

Key Concepts and Implications

On one level, deterrence and information warfare are well matched. Both belong to the world of robust ideas with broad implications. Both are highly relevant to the post-Cold War era in which conflict has been transformed from bipolar global structures to multi-sided, local and regional contests in which the military element is a crucial part of, but not the driving force for, competition and conflict. On the other hand, the two topics can be seen as orders of magnitude apart. IW is a huge domain, ranging from media wars to electronic combat and from economic competition to strategic conflict waged against civilian populations. Deterrence is actually a narrow topic that only applies when a set of quite restrictive assumptions apply. Not surprisingly, therefore, the workshop participants found the relationship between the two concepts to be spottyùhighly relevant on some topics, marginally so on others, and not at all relevant in many areas.

Deterrence as a Concept

Many of our common notions of deterrence arise from the recently concluded Cold War. Strategic deterrence was equated with deterring both a Soviet invasion of Western Europe or a first strike on the United States, by the assured ability to reply with a devastating nuclear attack on the Soviet UnionÆs homeland. The workshop participants were well aware that most ôdeterrence theoryö is largely a product of that Cold War era. This suggests that those whose experience is from that era may bring extraneous concepts or baggage to the topic. Hence, they also heavily agreed that deterrence applications outside the nuclear war arena must be thought through carefully and should be exposed to domain experts from the appropriate arenas before they are considered mature.

Throughout history the primary form of deterrence has been defenses. These defenses have been both passive and active. Passive defenses include fortifications, moats and natural features such as rivers, oceans and high ground, and serve to deter by making attacks more difficult and costly. Active defenses and their ability to deter can best be summed up by the quotation frequently attributed to President Theodore Roosevelt: "Speak softly and carry a big stick." In the aggregate, this involves military defense forces.

Military capability or force is obviously not the only way to deter. For example, economic self-interest may deter. Just as an employee is restrained from insulting his employer or a businessman from annoying his customer, nations may be restrained from some information adventures either by the direct cost of the adventure or by the harm to future trade and other economic activity that may result. Building economic interdependency can therefore be considered as a form of deterrence. Likewise, information actions and interdependency might also be a kind of deterrence.

In any sphere, the retaliatory capability need not be real; but it must be perceived as real. Conversely, capability to deter may be insufficient if the adverse party is unaware of the

capability or is not persuaded that the capability might be used. Military examples include the Strategic Defense Initiative as deterrence through perception management, and the reverse, when the perception of U.S. military might did not deter Iraq's 1990 invasion of Kuwait. Saddam Hussein either underestimated our power or our willingness to use that power.

Deterrence in the Information Age

The workshop readily reached consensus on a basic definition of deterrence as *"prevention or discouragement, by fear or doubt, from acting."* Clearly this definition implies an actor and a target. Moreover, the group also agreed on a simple set of conditions necessary for successful deterrence. These were seen as:

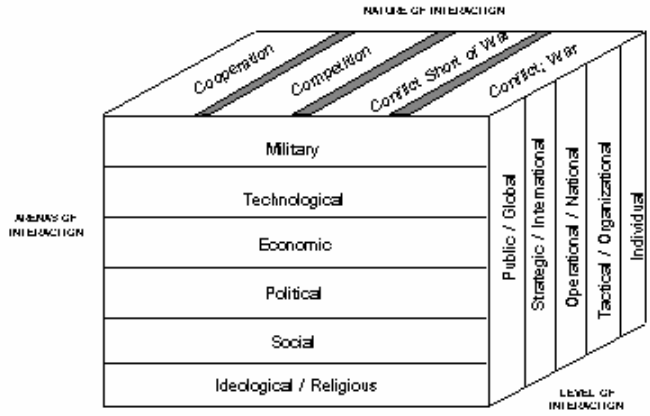
- A threat to something of value that exceeds the perceived gain of non-compliance.
- A clear statement of the behavior to be avoided or performed.
- Clear and unambiguous communication of the threat and the desired or proscribed behavior to the target.
- Credible threat, meaning that the actor is perceived by the target to have the will and capability to execute the threat.
- Situational constraints that make it impossible for the target to avoid punishment.
- Controllability of the threat and its implications by the actor.

The Domain of Information and Information Warfare

The simple, but crucial, step of defining what is encompassed by the term "information" is all too often ignored by those who write about its importance and its future. Appendix B is a study of the information dominance concept that was included as read-ahead material for workshop participants. It examines the hierarchy of information and the relationships of information interactions and the players who function in the arenas of interaction. It further suggests that what is commonly understood as "information warfare" might be too narrow a focus that ignores other significant information interactions across and through the full scope of human activity. Appendix C (also read-ahead material) addresses information warfare from perhaps the less theoretical and more practical viewpoint of a professional military practitioner. In spite of the contrasting approaches, both papers strongly assert that what we call information warfare today goes well beyond mere military interactions.

As Figure 2 illustrates, three relatively independent dimensions were required to capture and describe the information warfare arena: the degree of conflict/cooperation, substantive focus (political, military, social, economic, and so forth), and the nature of the actors involved (individuals, private organizations, nation states, international organizations, the general public, media, etc.).

FIGURE 2. INFORMATION SPACE



The workshop participants generally accepted the broad nature of the information warfare domain and the central role of information systems and processes in the world today. However, they inferred several very important implications from this broad characterization of the relevant domain.

- First, the term "information warfare" is used to mean many things, but is often focused on the military domain or the cyber-war domain dominated by computers. This narrow definition is inconsistent with the broad policy questions relevant to competition and conflict using information media.
- Because information warfare is really a broad and diverse arena, analysis of it must be focused on selected elements, which must be clearly defined in each application. Overall, the field is so broad that virtually no meaningful generalizations can be drawn about it.
- Isolation (except in rare instances), of military, national, public, and private information systems is all but impossible today. Even very important military traffic is likely to be carried on national infrastructure systems. Public and private information sectors are heavily interdependent, and this linkage will continue to grow.
- A whole raft of information systems make potential targets -- banking systems, control systems for railway operations, air control systems, control systems for pipelines, media systems, and others. Only a fraction of those are primarily military or under the direct protection of the Department of Defense.

- As has been stressed by ADM Owens, Vice Chairman of the Joint Chiefs of Staff, the civilian sector is no longer a sanctuary that can be protected by interposing military forces between adversaries and their targets. Traditional military forces can be flanked at the speed of light by information age attacks on the general population or key economic systems.
- More profoundly, there is no consensus on the appropriate boundary between the military and Department of Defense roles and missions, those of the law enforcement and intelligence systems, and those of the commercial sector.

Workshop participants were aware of a variety of policy initiatives to create interagency working groups and coordinating mechanisms as well as public-private dialogues and mechanisms for both exchanging information and developing plans for dealing with information age threats that cut across communities. Considerable progress has been made in generating better awareness of the threat and there is some effort toward cooperation. However, the general consensus was that these helpful activities were only now developing momentum and were far from successful completion.

Information Warfare and Deterrence

It is clear that the information age has spawned new relationships and greatly expanded the range of possible interactions. It is no longer possible to separate and isolate military, national, public, and private systems. Thus, concepts of national security, to include protecting information systems and deterring attacks, need to be expanded to consider the full range of likely interactions. This would help to determine where the boundary between DoD and the rest of the national information infrastructure should lie. It was in this context that the workshop primarily addressed the relationship between information warfare and deterrence.

At the abstract level, the interface between these two concepts is dependent on setting the context clearly. First, deterrence is always from an actor toward a target. The very nature of the actor and target, as well as the degree of asymmetry between them is important. A nation state has much greater power than an individual hacker and has broad powers of law enforcement that can be brought to bear if the individual is within its borders or the reach of accepted international laws. However, two nation states are, at least in legal terms, equal and must exercise the international system (diplomacy, warfare, etc.) to influence one another's behavior.

Moreover, the nature of the relationship between the parties is important to the analysis. The use of deterrence is unlikely in cooperative arrangements, more likely in competitive ones, and most likely in conflictual patterns. Finally, substantive context may also make a difference. For example, deterrence is most likely in military arenas where the credibility of threats is greatest and easiest to assess. Hence, specification of the context (type of relationship, nature of the actors, substantive domain) is essential before any conclusion is possible about the effectiveness of deterrence.

The Steamroller and the Wrench

The most important insight arising from looking at the two concepts however, is the fact that they are only relevant to one another in highly selective contexts. The analogy that emerged was that of a steamroller and a wrench. Both are tools and depending on the situation, appropriate wrenches may be useful for, or even crucial to, the operation of the steamroller. However, most of the things the steamroller does are irrelevant to the wrench and most of the things the wrench can be used for do not involve a steamroller. In many cases, therefore, the workshop found itself venturing away from a pure consideration of the two concepts and into meaningful discussions in areas related to one or the other of the two central topics. These discussions revolved around the concepts, but kept slipping tangentially to more familiar issues such as command and control warfare (C2W), or IW in some other context such as retaliation in kind for an IW attack. It eventually became apparent that the main reason for frustration was that the related concepts and issues are grossly mismatched. IW is just too big and encompasses so much (particularly in the context of information dominance), while deterrence is limited and almost always case specific.

In retrospect, the revelation should not have been surprising. While workshop participants noted that certain IW actions are as old as warfare (a bluff for example), the exploding vistas of information technology and cyberspace are only beginning to be understood. Several of the participants were comfortable discussing deterrence as it might be related to command and control warfare (C2W). In this application there are five clearly defined "Pillars" which include Operational Security (OPSEC), Electronic Warfare (EW), Psychological Operations (PSYOPS), Military Deception, and Physical Destruction. The pillars are arrayed both offensively as "Counter-Command and Control" and defensively as "Command and Control Protection." Both arrays are dependent on and supported by intelligence. Any one of the pillars can have a deterrent effect. For example, in EW the presence of anti-radiation missiles may deter the use of air defense radar. Likewise, the adroit use of psychological operations might disrupt the enemy decision making process to the point where they are deterred from action, or at least their C2 process is greatly slowed.

While we believe that we understand C2W, the workshop brought into clear focus the fact that C2W is only a very small subset of IW, and it is that larger context that needs further exploration and analysis. Likewise, one size IW deterrence does not fit all. Equally important to the action itself is the intended recipient. Without getting into the adversary's mind and understanding his social, cultural, and religious values, as well as his education and past history, IW deterrence actions may be like the tree that falls in the forest and goes unheard. They may even be misunderstood and, therefore, have unintended consequences. The earlier discussion of deterrence stressed that creditable deterrence requires that the message be communicated clearly. Knowing how the adversary receives and understands messages is essential.

It also became increasingly clear that IW deterrent actions must be part of an orchestrated and integrated effort. Seldom will an IW action in and of itself be a creditable deterrent.

However, skillfully combined as part of an overall information dominance concept, some combination of IW and other actions may produce the desired deterrence.

Chapter 2: How Might IW Attacks on the United States Be Deterred?

As information age technologies become more useful and valuable across all arenas and levels of interaction, vulnerabilities to disruption, deception, penetration, theft, and destruction increase as well. The vulnerabilities cluster around two basic areas: the computers that form the heart of most information systems and increasingly control operating systems, and the communication networks that tie them together. Workshop participants noted that recent studies indicate that all too often computer security is still given short shrift. Records that would be locked up if they were paper are often left unprotected in computers. When computers are networked, they become even more vulnerable because information can be accessed from remote locations. Both locally and remotely, data can be manipulated, viruses inserted, and records stolen or destroyed. When the data being manipulated or moved represents money or other things of value, the manipulation is theft. Presently, the banking system is reportedly losing millions of dollars each year to computer theft. At the Department of Defense, hackers have penetrated DoD networks and systems (mostly unclassified). Moreover, recent tests indicate that only about five percent of attacks are detected, and of those detected, only five percent reported. If these figures are correct, the likelihood of knowing about an attack is .0025 (one-quarter of a percent) and the risk of being caught must be, by definition, even lower. Other military systems are likewise vulnerable. In many cases that vulnerability cannot be reduced by isolation because military systems depend on the national information infrastructure for about ninety percent of their traffic. Over ninety-five percent of all U.S. Government telecommunications within the U.S. travel on commercial circuits.

From the banking system to air traffic control, from military logistics to the telephone networks, from the stock exchanges to computer controlled trains, the United States, its economy, and its security are inexorably bound up in information technology. Many of the key systems lack safeguards or redundancy. Some, including some defense systems, are extremely fragile and easily disrupted. Most are vulnerable in one way or another. The U.S. information infrastructure is easily the world's biggest IW target.

Given these vulnerabilities, what can be done to enhance security and improve the likelihood that the United States can deter IW attacks? What are the DoD's responsibilities, and where are the boundaries of those responsibilities? Since U.S. forces cannot fight effectively without being well connected to the national information infrastructure, the responsibility would appear to go well beyond the protection of military systems alone. The workshop noted that this is a broad national security issue that the military cannot ignore. Since IW defense and deterrence are essential to military effectiveness, a crucial issue is to determine what role the professional military should have in this mission.

Cyber-War Attacks

Beyond the attacks that one might envision in the context of classic IW and C2W, there are other vulnerabilities. For example:

- Attacks by creative individuals skilled and determined enough to exploit communications systems and computer networks for illegal gain or to disrupt society.
- Criminal organizations (terrorists, drug smugglers, illegal arms merchants, international poachers, and rogue banking groups) that sit across any one country's boundaries, move money or information from jurisdiction to jurisdiction, and all too often represent a poorly met challenge.
- Coalition warfare in which military cooperation and interoperability are essential, but political goals are not fully compatible and intelligence sources and methods must be protected.
- Psychological warfare waged against a general population in order to undermine confidence in leaders or the wisdom of their actions, often exploiting ethnic, social, or moral cleavages in the target society.

This wide range of possibilities caused considerable discussion before the group could agree on the various types of computer attacks that must be considered. Initially, some felt the discussion should focus only on protection of internal DoD systems, while others wanted to include broad strategic or operational attacks on the banking system or other commercial or quasi-governmental arenas. The workshop was aware, however, of an ACTIS analysis of Defensive Information Warfare (Appendix D, the third and final part of the workshop read-ahead material) that differentiates attacks by their targets and implications into:

- Day-to-day or routine attacks with limited or diffuse impact on U.S. interests. These include "normal" hacking for fun and profit, typical white collar crime, and other attacks with discrete impact.
- Potentially strategic (catastrophic) attacks. These are limited attacks with unpredictable consequences that could, under some circumstances or in some combinations, have catastrophic implications for U.S. interests. For example, an attack on a single bank, even if the losses are large (millions), is no threat to the U.S. banking system. However, an orchestrated and publicized series of successful attacks on individual banks could undermine confidence in the banking system and create a much more serious problem, even though the specific attacks were each quite limited.
- Strategic (catastrophic) attacks are those which, if successful, will in themselves do great harm to the United States. Destruction of the systems that control systems in key industries and leave them so they cannot be repaired promptly would fall into this category.

In addition, workshop participants stressed that not all information warfare attacks on computer systems need take the form of computer intrusion. Physical destruction of

crucial telephone switching stations or other national information infrastructure assets would, in them-selves, be very damaging.

One significant finding was that the workshop participants consistently found themselves assuming that a visible set of defenses was the beginning point for deterring attacks on important computer systems. In essence, the argument was that attacks are instrumental acts and will not occur if the attacking party perceives little opportunity for success.

At the same time, the workshop also noted that "success" has very different meaning for different types of actors. Some individuals, particularly those with "typical" hacker attitudes, would be likely to perceive a more robust defensive posture as a challenge, not as discouragement. This, of course, is a lesson in the need for specific contexts when discussing deterrence and IW. What works in some circumstances may be very wrong for others.

Regardless of whether good defenses necessarily deter attacks, there was consensus that the set of defenses now in place is inadequate for discouraging any but the least well prepared intruder. As mentioned earlier, many systems are poorly protected, very few intrusions are detected, and very few of those detected are actually reported. Improved indications and warning, as well as improved reporting of detected attacks, are essential elements of improved defensive systems. In essence, the workshop concluded that assessing the ability of DoD or others to deter attacks will require much better documentation and understanding of the pattern of attacks being experienced.

Deterrence of cyber-attacks was also understood to depend on the nature of the attacker. On one level, deterrence requires identification of the values held by the potential attacker as well as the capacity to communicate with that attacker. Neither is possible without information about the nature of the person, group, or entity to be deterred. The variety of potential attackers is vast, which makes it impossible to create a "one size fits all" deterrence policy that will be effective. However, cyber-attacks and physical attacks on key computer systems can be prevented or discouraged by aggressive, visible, effective defensive systems. Analogies were drawn to terrorists, who also act from a variety of motives against a wide range of targets (including information domain targets), but who have been deterred in selected instances by explicit threats and retaliatory actions implying future threats unless the terrorists cease to attack some types of targets.

There is no single, simple solution. However, combinations of defensive measures are important initial building blocks. Further, defense against information attacks should be viewed as a continuing process rather than a "finishable" project. The process begins with awareness of the issues and problems and proceeds to indoctrination, education, training, and physical defensive measures. Awareness, education, and security training are being taught within the DoD but need to be improved across all levels. It would also appear that DoD should reach out further and address the issues to other government agencies and relevant non-governmental organizations through interagency seminars, vulnerability analysis, and training.

Systems vulnerability analysis is a critical first step. We should lay out our potential target sets and interconnecting networks and look for actual and potential vulnerabilities. Defensive nodal analysis (like that conducted in offensive command and control warfare) is particularly important. Once the weaknesses are identified, defensive measures should be put in place. Table 1 lists some of the common and accepted system defenses.

Table 1: Information Systems Defensive Measures

- Systems Vulnerability Analysis
- Systems Hardening
- Security Training
- Redundancy and Backup
- Aggressive Law Enforcement
- Tagging Hardware and Software with Electronic ID
- Embracing (Systems Interdependency with Potential Attackers)

Systems vulnerability analysis and improved design can yield three positive results. Besides the obvious result of reducing vulnerability, the systems can be made less attractive targets; that is, successful attacks would yield less damage and publicity. As stated by VADM Cebrowski (the JCS J-6, and workshop luncheon speaker), decoupling IW attacks from their objectives is an effective deterrent technique. Since IW attacks, like almost all types of attack, are assumed to be conducted for instrumental purposes, he argued that de-coupling the attack from its goal was an important way to ensure such attacks were unsuccessful and also to deter the attacks themselves because the attackers saw little opportunity for success. Good design can also raise the potential costs of attacking in terms of time and equipment needed to penetrate. This also has a deterrent effect. Hardening and protective measures should be designed into all systems. This is an enormous field that spans the spectrum from satellite antenna design to electrical protection of personal computers and workstations.

Security training is absolutely essential at all levels, and without it other defensive measures are less effective. Password protection, for example, can make information systems less accessible, but bad procedures can defeat its purpose. One of the workshop participants described security exercises where he was able to penetrate password-protected computer networks by manipulating the password protection system itself. Perhaps more important, almost every penetration and technique tried on that exercise and those in the experience of other workshop participants had been successful in the vast

majority of cases. Hence, the need for basic system security design, improved security procedures, and better training within DoD.

Other key steps include redundancy and backup. These methods reduce or limit the harmful effects of an attack or system penetration. Frequent backup can minimize the damage caused by lost, stolen, or disrupted data, and information can be rapidly restored or reconstituted. Redundant baseline data can also be used to check against unwanted changes or clandestine data manipulation.

Aggressive domestic and international law enforcement can certainly have a deterrent effect on potential adversaries. Since cyberspace recognizes no borders, international agreements and laws are necessary. This is particularly important because many information systems are not only national, but also worldwide. Telecommunications and international banking systems are prime examples. Further, hackers appear motivated by the challenge of defeating defenses. Defenses alone apparently just make hacking more enjoyable. To deter hackers, there must be a realistic threat of capture and punishment.

Tagging information systems hardware and software with electronic IDs can also deter would-be penetrators and attackers. The analogy is similar to caller ID, where those who penetrate systems are identified, and a record of the penetration is made.

"Embracing" is a concept that engages potential attackers by including them as stakeholders in the information system. By embracing and educating these possible adversaries, they may be less likely to consider attacks that could potentially cause self-harm. The concept is already in effect since many systems are worldwide, and an attack by one nation on another could have cascading effects beyond those intended. An attack on the banking system in one nation, for example, could have unintended consequences and cause disruptions around the world. Embracing would appear to have deterrent effect only on rational nation-states. There are two weaknesses to the concept. First, it is doubtful that cyber-terrorists would be deterred in such a scenario; rather, cascading consequences might actually make the attack more attractive. Second, what may be viewed as embracing by one party may instead be an opportunity for infiltration by the other. Again no "one size fits all" deterrence policy is available because of the range of motives that may be encountered.

Finally, we must develop an effective system of IW attack indications and warnings (I&W). The adage of "forewarned is forearmed" is particularly relevant here. Indications of attack can come from traditional intelligence sources, monitoring of events and activity, and perhaps other cyber-tags that we have yet to discover. Penetration warning systems should be designed and built into critical information networks, nodes and stations. Cyber I&W is an area that needs much more careful study, analysis, and debate.

Many of the defensive measures discussed are not unique to the deterrence arena, but rather reflect the workshop participants' assumption that some attacks will be deterred by effective defenses. The technical representatives in the workshop also stressed that for the foreseeable future the advantage will lie with the offense in the cyber-war arena. Hence, building defenses does not guarantee success, and creating redundancy as well as the

capacity to contain, recover from, and reconstitute in spite of successful attacks are essential elements of a successful strategy.

Media War

An interactive exercise scenario introduced the topic of "SOFTWAR," which is a trade name for one concept of media war. This concept involves the use of television images to change or modify the political will of an opponent. SOFTWAR was defined as "the hostile utilization of instantaneous global television to shape another nation's will by changing its view of reality." The main technique of SOFTWAR is to unglue the adversary government's hold on the unifying national mass communications system, the most powerful medium of which is television, and distribute alternate video productions (or some other form of video manipulation) in its place. The speaker asserted that the controlled projection of video information has joined economic, political, and military power as a pillar of national security and that it will become a co-equal power by the year 2020.

The exercise scenario involved a campaign aimed initially at public attitudes in friendly and other regional countries whose cooperation is essential to major U.S. operations in and around the Persian Gulf, and later at public attitudes in the United States. In the demonstration scenario, the U.S. was the victim of a carefully orchestrated television campaign aimed at both the U.S. TV audience and at a selected Middle East and North Africa audience within the footprint of a direct broadcast satellite. The thrust of the argument was that prudent, even essential, military actions could well be called into question through media attacks with primarily political messages.

Some workshop participants were skeptical about the impact such a campaign might have on U.S. resolve and action. There are, however, past examples of how TV has affected U.S. political action going back to the Vietnamese War when rather primitive TV reporting (by today's standards) brought bloody battlefield images into U.S. homes for the first time. There is little doubt that television coverage of Vietnam changed or eroded the will of the U.S. population to sustain the conflict. Likewise, TV images of the bombing of the U.S. Marine Barracks in Lebanon tested our resolve and hastened our departure.

More recent examples include the Somalian relief mission where graphic, quite gruesome TV images of relatively light U.S. casualties soured the support for continued presence and led to an early U.S. pullout. In Haiti, TV images of U.S. soldiers standing by while Haitian police beat innocent people celebrating the arrival of U.S. forces caused an overnight change in policy as to how Rules of Engagement (ROE) were interpreted. The workshop agreed that indeed, television is an extremely effective, and potentially dangerous, medium for propaganda. Given the ability of modern technology to manipulate images, it becomes an even more powerful IW weapon. Several other conclusions emerged from the media war discussions:

- First, because of its democratic traditions and freedom of speech considerations, the United States will almost certainly be placed in a reactive mode if a hostile media war campaign is launched.
- Second, foreign powers will find it difficult to intimidate U.S. leaders or to put forward obviously false information toward the U.S. public without effective U.S. media responses, but may be able to communicate quite inaccurate images to selected foreign publics who are predisposed toward them.
- Third, the infrastructure to deliver television images into distant regions may not be readily available within DoD, particularly in a non-warfare situation where the sovereignty of foreign states must be respected. Review of the hardware requirements for flexible responses that give the National Command Authority a rich set of options appears to be wise. Equally important, the workshop concluded that the creation of reserve units or other mechanisms to ensure the availability of the human capital needed for commercial quality television production on a sustained basis, also appears wise.
- Fourth, wargames and seminars involving not only DoD, but also the range of civilian agencies and industry representatives necessary for effective television imagery in media wars, appear to be needed. Incorporation of meaningful media attacks into appropriate military exercises is an important first step, but would be inadequate in itself over the long run.
- Fifth, media warfare can put enormous time pressure on U.S. and allied decision making, particularly when the adversary is an authoritarian state with little or no necessity for either internal or international consultation. With proper preparation and effective technical support, however, this time pressure can be managed.

Policy Issues

Many of the workshop discussions naturally evolved into policy explorations. Two of the most prominent were: one, "Should the United States have a declarative policy about its response to IW attacks?" and two, "Should information be viewed as a separate element of national power?" Opinion was divided on both issues. Table 2 highlights the arguments for and against a declared policy on U.S. response to IW attacks.

Table 2. **Summary of Opinion**

Should the United States Have A Declaratory Policy About IW Attacks?

YES	NO
◆ Declared policy necessary basis for deterrence	◆ Premature (we still don't know what an IW attack is)
◆ No policy equals no direction (to government agencies, industry, etc.	◆ Ambiguity is useful in terms of deterrence
◆ Sets the standard for the rest of the world	◆ There are non-trivial international complications
◆ Policy defines areas of broader cooperative agreements (laws, treaties)	◆ Don't separate IW from other kinds of attacks
◆ Policy should be very broad	
◆ Policy should deal with attack effects, not method of attack	

The workshop participants were strongly in favor of a declared policy, with 70 percent voting for such a policy, 17 percent against, and 13 percent ambivalent. A declared policy was considered essential if there was to be any deterrent effect. Further, without a policy, there is no direction for the government, and many agencies are going their own ways and establishing their own policies. If we are to have cooperative international agreements and treaties, a declared policy is an essential starting point. The policy should be coordinated with industry and public debate encouraged to secure support and resources required to protect our interests. The overall workshop consensus was that there should be a broad, publicly stated, general policy phrased in terms of effects rather than method or type of attack (e.g., economic, military, social, political). One recommended statement was: "Attacks on the U.S., its infrastructure, or other interests (by whatever means) will receive an appropriate response using the fullest range of U.S. capabilities."

Those who were ambivalent or opposed to a declared policy were generally concerned that such a policy was premature, that we lacked sufficient understanding of IW attacks and their effects and consequences. By not stating a specific policy, we create ambiguity, which some felt was useful in terms of deterrence. There is much to think through before declaring an IW policy particularly in terms of the international implications and complications. Finally, and somewhat in agreement with those who advocated a formal policy, one reason not to have a policy is simply that there is no need to separate IW from other kinds of attacks.

On the second issue, whether information should be viewed as a separate element of national power, opinion was also divided; however, most participants viewed information as a separate element of national power. Table 3 summarizes the comments.

***Table 3.* Summary of Opinion**

Should Information Be Viewed As A Separate Element of National Power?

YES	NO
◆ Information is power.	◆ Information is ubiquitous and pervasive; it is a subsumed aspect of each element of national power.
◆ Information supports all other elements of national power and is emerging as important in its own right.	◆ It would simply spawn another government agency.
◆ Information is key to international competitioin and conflict.	◆ Information is simply correlated data; it can be pertinent or trivial.
◆ Need to identify specific information categories as components of national power.	◆ Information attacks and crimes are already covered by existing laws.

All participants agreed that information was an essential element of power. The debate ranged around whether that should be stated explicitly or not. Those in favor (80 percent) cited the growing importance of information and information age technologies, and how information is creating a cultural revolution and changes in the behavior processes between nation-states. For those who voted "no" (20 percent), the major consideration was that they viewed information as ubiquitous and pervasive in each element of power, and not an independent element. One participant made the analogy that information was like "electricity." It is subsumed in other elements and systems.

There were numerous other questions with policy implications and these included:

- What is (what constitutes) an information attack?
- When is an information attack an act of war?
- How do we verify an attack?
- How do we determine or confirm the attacker?
- Does penetration into an information system equate to an attack?
- Can one develop a concept of hostile intent for IW?
- Are there reasonable or potential tripwires?
- How do we respond, and who should respond?

Since at present no one has the charter for IW (in the larger context -- beyond C2W) responses will be ad hoc at best. The boundary between DoD and the rest of the national infrastructure is blurred and undefined. The workshop reached no consensus as to where that line should be or what DoD's role should be within the larger context.

IW policy issues emerged as the area that needed much further study. Without policy definition, concepts like IW and deterrence can't be fully explored. Policy is essential and the workshop participants recommended a follow-on roundtable to explore policy issues. Basic policy statements have begun emerging, but final work appears necessary.

The Role of DoD

Given the low rate of reporting system penetrations and other security problems, the U.S. presently lacks the data needed to know just how serious the unauthorized penetration problem might be. Are we hemorrhaging or simply suffering "duck bites"? Better reporting is essential.

The starting point for DoD should be to raise the level of awareness, not only within the Department, but also throughout the national information infrastructure upon which it is so vulnerably dependent. Developing and implementing cyber I&W should also take high priority. One note of concern voiced was that the DoD procurement cycles and information technology growth cycles are greatly mismatched. That is, several technology cycles occur within one DoD procurement cycle. This can result in DoD developing yesterday's solutions for tomorrow's problems.

DoD's next priority should be a comprehensive vulnerability analysis, first of DoD systems and later expanded to the national infrastructure upon which they depend. At present, vulnerability is usually assessed for only a particular system or subsystem. Future vulnerability analyses should expand the studies to examine interrelated systems, and systems of systems. In due course, the analyses should be expanded to include all U.S. systems. We should implement defensive and deterrent actions as soon as vulnerabilities are uncovered.

Beyond DoD, there is a need for a national level, strategic debate to formulate a coherent IW policy and a determination of DoD's boundaries and responsibilities. Neither DoD nor the Federal Government can do this alone; all relevant public and private sectors should be included. But until there is policy about IW defense and deterrence, DoD still has the responsibility to protect its strategic, operational and tactical systems. The strategic systems appear reasonably well protected and redundant through hardening, elaborate security procedures, and multiple backups. Operational and tactical systems appear far less protected and need additional emphasis.

Core Conclusion About Deterring Information Warfare Attacks on the United States

While recognizing that the variety of potential attackers, attack contexts, and arenas where information warfare attacks can occur is vast and too complex for simple solutions,

the workshop participants were confident that the U.S. already has basic policies in place that serve as effective deterrents in many circumstances. *In essence, information warfare attacks on the United States are deterred by the same policy that deters other types of attack. Acting under its rights as a sovereign state, the U.S. stands ready to respond to any attack on its interests with all appropriate means, including law enforcement as well as military capacity.* As discussed in the workshop:

- Individual hackers and white collar criminals are liable when they break the law and can be prosecuted within a legal system that takes into account both their motives and the degree of harm that they cause.
- International criminal enterprises, such as drug cartels, terrorist groups, or interest groups willing to engage in illegal information attacks or manipulation, are liable under the legal system and also pursued under international law and treaties that govern their behavior and specify both the jurisdictions and processes for determining their punishment if caught.
- Nation states are restricted by the rights of others and liable for a range of political, economic, diplomatic, or military sanctions if they undertake information operations that harm U.S. interests. As in other arenas, the U.S. reserves the right to undertake actions it perceives to be both appropriate and proportional.

There was also consensus that information attacks may well pose some unusual challenges that may make them more difficult to deter. For example, information warfare attackers will likely seek to be anonymous, thereby making it impossible for the U.S. to punish them. Cyber-attackers, in particular, have a variety of mechanisms by which they can hide their identity. Since certainty of punishment is a prerequisite for deterrence, anonymity is an effective counter-strategy.

Moreover, information attacks can be hidden or made to look like natural events. In media war, this may be a half-truth fed to an aggressive reporter. In cyber-war it can be a destructive attack made to look like a system error or design flaw. Disguised attacks are also effective countermeasures for deterrence, regardless of the capability and will of the actor. Hence, while significant, overall U.S. capability and will do not guarantee deterrence of information attacks.

Finally, the workshop recognized that considerable legal work needs to be completed in this arena. First, U.S. law (both state and federal) needs to be clear about the definition of crimes in the information arena. Second, international agreements and treaties are needed to ensure that information criminals can be prosecuted effectively. Cases in which lack of appropriate law limited or prevented prosecution were easy for participants to recall. The Departments of Justice and State are generally aware of these needs and interagency working groups have been making some progress on them, but this area will require continued effort for some time to come.

Chapter 3: Using Information Warfare to Deter Foreign Governments

In large measure because the discussion on defending against information operations was so rich, but also to a certain extent because of the relatively low level of classification for the meeting, this topic was addressed more quickly and in less detail than the others.

Previous Efforts and Analyses

A workshop presentation reviewed the results of a U.S. Navy-sponsored war game on "Strategic Deterrence and Information Warfare," held at the Center for Naval Analyses in December 1993. The game explored deterrence and examined IW as it relates to deterrence.

Using a Middle East scenario, the game explored IW actions and their effects from several perspectives including world opinion, the adversary (Red), the U.S. National Command Authority (NCA), and the U.S. military Commander-in-Chief (CINC). The game progressed from peace to crisis to hostilities, and in each phase, the players examined possible IW actions and results.

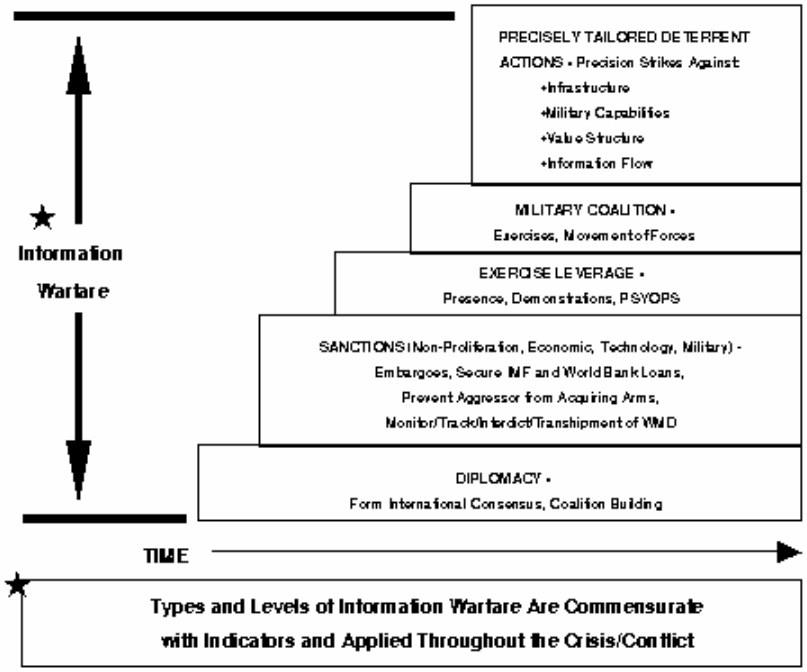
The game produced several relevant conclusions. First, deterrence in any form is an integrated political, economic and military effort, and the military part is Joint. That is, no single service or agency is or should be designated as responsible for IW actions in isolation from others. At the national level, IW strategy is needed and it must have full interagency involvement. Possible unintended con-sequences need examination and resolution for each proposed course of action. In pre-hostilities, many desirable information actions may be cast as "acts of war," so there are additional requirements for high level coordination with allies and coalition partners. There is also a long lead time required for most IW applications. As a crisis moves closer to the brink of hostilities, more direct IW actions become more acceptable. Again, these must be shared with allies on a case by case basis.

One of the most significant game findings was that while IW can provide high leverage options, these options seldom can "stand alone." They work best with other deterrent measures such as presence, force movements (e.g., movement into theater; call up of reserves), and other direct deterrent actions that serve as a demonstration of will. There is a critical need to start IW actions early (in some scenarios this can be years), but this must be balanced by judicious restraint. That is, premature "bridge blowing" may limit future action or demonstrate a capability that can later be defended against by the adversary. Another similar dilemma is the need to balance an early preparation of the IW battlefield with the concern that such action could "poison the well" of a future ally. Given the nature of alliances and coalitions in the post Cold War era, a potential adversary could well become an ally.

As a result of the game play, the players developed a time-phased approach to deterrence which is illustrated in Figure 3. The information warfare actions shown illustrate the

kinds and levels of actions that would progress from peace time through hostilities. As both time and the interactions progress towards hostilities, so does the type and intensity of information warfare. In the context of this Middle East "Desert Shield/Storm" type scenario, the IW actions and intensity levels were an integral part of the plan, commensurate with indicators and applied throughout the crisis and conflict. The presentation served as a starting point for the discussions of offensive IW actions. As noted earlier, these discussions were somewhat constrained by the workshop classification level.

Figure 3. **Time Phased Approach**



Limits on U.S. Actions

The workshop also noted some significant limits on U.S. offensive activities. First, media manipulation that involves government personnel providing false information is neither politically wise nor consistent with U.S. policy and law. Second, information attacks are attacks and, therefore, are subject to international law. Violations of sovereignty and acts of war are no less real because they use the information domain than if they involved violations of air space. Like other sovereign governments, the United States is free to defend itself and may choose to engage in acts of war for sufficient cause, but should not believe that this arena is an exception to normal rules of behavior. Indeed, U.S. disregard for international law in this crucial arena could set precedents that are very dangerous, in part because the United States is the world's largest potential IW target.

Potential of Offensive IW to Deterrence

The limits having been noted, the workshop participants also recognized that the technical capacity to render an adversary "ignorant," poor, uncertain of the capability to control its own forces, unable to communicate with its population, or uncertain of the quality of its basic information could have a profound effect on its willingness to undertake a military adventure and thus potentially equate to a powerful deterrent.

Moreover, while barely unveiling the true potential of highly leveraged information and superior battlefield awareness, *Desert Storm* has provided the world with a demonstration of the potential advantage of differential information capacities. Finally, the workshop concluded that research and development into tools and techniques that can impact potential adversaries' knowledge of the battlefield, control of their own forces, resources necessary to support armed conflict and deliver services to their populations, or leverage uncertainty about their own information, should go forward. This will help to ensure that the U.S. advantage in commercial information systems is translated into the capacity to influence and deter potential aggressors. And should deterrence fail, it is needed to minimize casualties in future conflicts.

Chapter 4: Workshop Insights and Conclusions

Scope of the Problem

The most significant insight about IW and deterrence is that the two concepts are only relevant to one another in highly selective contexts. IW is just too big and encompasses so much (particularly in the context of information dominance), while deterrence is limited and almost always case specific. But once that insight occurs, the problem can be analyzed in deliberate and methodical ways.

First, the term "information warfare" is used to mean many things, but often focuses on the military or the cyber-war domains dominated by computers. Actually the field is so broad that virtually no meaningful generalizations can be made about it. But by focusing on defensive cyber-war and media war, and a range of offensive IW actions, it is possible to bound the problems into workable segments. That is, analysis must be focused on selected elements which must be clearly defined in each application.

The U.S. national information infrastructure is interlinked and interwoven. It is not possible, except in rare instances, to separate the military, national, and private information systems. Public and private sectors are heavily interdependent and this linkage will continue to grow. Further, U.S. information systems and the U.S. information infrastructure appear extremely vulnerable, and a whole raft of information systems could be potential targets. The U.S. civilian sector is no longer a sanctuary that can be protected by interposing military forces between threat or adversaries and their targets. Traditional military forces can be flanked at the speed of light by information attacks on the general population or key economic systems. Accordingly, our concept of national security needs to be expanded to consider the full range of interactions and to determine the proper boundary between DoD and the rest of the national information infrastructure.

Deterring Attacks on the United States

While the workshop recognized that potential IW attacks can occur in ways and means too complex for simple solutions, it reached the core conclusion that the U.S. already has basic policies in place that serve as effective deterrents in many circumstances. *In essence, information warfare attacks on the United States are deterred by the same policy that deters other types of attack. Acting under its rights as a sovereign state, the U.S. stands ready to respond to any attack on its interests with all appropriate means, including law enforcement as well as military capacity.* Beyond this, some workshop participants strongly believed that the United States should have an explicit, publicly stated, declaratory policy about its response to IW attacks.

Cyber-War Attacks

Workshop participants consistently found themselves assuming that a visible set of defenses was the beginning point for deterring attacks on important computer systems.

However, there was little consensus about the scope of the problem and how serious a threat cyber-war (digital) attacks might be. But with less than one-quarter of one percent of unauthorized DoD system penetrations detected and reported, current defense effectiveness must be very low and cannot be measured precisely. Workshop participants felt that DoD should establish department-wide requirements to report system penetrations, viruses, attacks, and suspected attacks as well as similar systems for collecting information about attacks on other types of systems in the United States. While new organizations and procedures have emerged in recent years to improve DoD's defenses and responses, the necessary level of awareness and cooperation has not yet been developed. Further, DoD needs to develop appropriate I&W metrics integral (i.e., included in the design) with other defensive measures.

Media War

The workshop's consensus was that the United States is vulnerable to media attacks. At the least, because of its democratic traditions and freedom of speech, the U.S. is almost certainly going to be placed in a reactive mode to media campaigns. While foreign powers will find it difficult to directly intimidate U.S. leaders or to put forward obviously false information toward the U.S. public without effective U.S. media responses, they may be able to communicate quite inaccurate images to selected foreign publics. This can put enormous time pressure on U.S. and allied decision making, particularly when the adversary is an authoritarian state with little or no necessity for consultation.

DoD appears to lack the infrastructure, hardware, and human capital necessary to deliver television images into distant regions, especially in a non-warfare situation where the sovereignty of foreign states must be respected. Review of the requirements for flexible responses that give the National Command Authority a rich set of options appears to be wise.

Finally, wargames and seminars involving not only DoD, but also the range of civilian agencies and industry representatives necessary for effective television imagery in media wars are needed.

Using Information Warfare to Deter Foreign Governments

The workshop noted some significant limits on U.S. offensive IW activities. First, media manipulation that involves government personnel providing false information is neither politically wise nor consistent with U.S. policy and law. Second, information attacks are attacks and, therefore, are subject to international law. The workshop also recognized that considerable legal work needs to be completed in the IW and deterrence arena. This includes not only state and federal laws defining criminal information acts but also international treaties to protect the United States from attacks launched from foreign territory.

It appears that IW techniques and technologies have great potential for supplementing and enhancing other methods of deterrence. But seldom will an IW action in and of itself be a creditable deterrent. That is, while IW can provide high leverage options, these

options seldom can "stand alone." Analysis of the optimum linkages between IW deterrence and other deterrent measures is needed. The workshop concluded that when skillfully combined as part of an overall information dominance concept, some combination of IW and other actions can produce the desired deterrent results. Research and development of IW tools and techniques should go forward.

The workshop discussions also made it clear that we need to continue the IW and deterrence exploration and analysis process. Additional studies through a series of roundtable discussions are planned to include:

- IW and deterrence policy issues such as definitions of IW deterrence options and solution spaces.
- The role of the Joint Staff and military services in supporting national information infrastructure security.
- The political and military utilization of IW.
- The role of technology versus policy.
- How IW techniques can influence decisions.
- Technical and training methods to improve IW defenses.
- Media war.

These additional roundtables and other forums will also examine classified and compartmented capabilities. Readers of these proceedings are invited to comment and join the forums at their appropriate security level and field of interest.

Appendix A. Workshop Participants

Dr. David S. Alberts
Director
Directorate of Advanced Concepts, Technologies, and Information Strategies
National Defense University

Dr. John Alger
Dean
School of Information Warfare & Strategy
National Defense University

COL Kenneth Allard USA
Directorate of Advanced Concepts, Technologies, and Information Strategies
National Defense University

Mr. Christopher M. Arey
Advisory Staff Member
Computer Sciences Corporation

Dr. Lyntis Beard
Center for Naval Analyses

Lt.Gen. James R. Brickel USAF (Ret.)
Director of Operations
Evidence Based Research, Inc.

Mr. Mike Brown
Science Applications International Corporation (SAIC)

VAdm Arthur Cebrowski USN
Director for Command, Control, Communications & Computer Systems
The Joint Staff (J-6)

RAdm James D. Cossey USN (Ret.)
Assistant Vice President
Science Applications International Corporation (SAIC)

Mr. Charles de Caro
President
AEROBUREAU Corporation

Mr. Steve Doyle
National Defense University

Maj. Link Ermis, USMC
Combat Development Command (C42)

Dr. Gary Federici
Center for Naval Analyses

Ms. Mary C. FitzGerald
Research Fellow, National Security Studies
Hudson Institute

Professor Fred Giessler, Ph.D.
School of Information Warfare & Strategy
National Defense University

Capt William Gravell USN
Chief, IW Division (J6K)
Joint Chiefs of Staff

Mr. Gus Guissanie
Infrastructure Policy
Office of the Secretary
Department of Defense

Mr. Tom Handel
Executive Director
Naval IW Activity

Dr. Richard E. Hayes
President
Evidence Based Research, Inc.

COL Thomas Hill USA
Chief, IW Division
US SOCOM/J3-IW
MacDill AFB, Florida

Col. Doug Hotard
Director, IW
Office of the Secretary, C3I
Department of Defense

Dr. Daniel T. Kuehl
School of Information Warfare & Strategy
National Defense University

Dr. Martin C. Libicki
Directorate of Advanced Concepts, Technologies, and Information Strategies
National Defense University

Lt.Col. Douglas Martin USAF
Joint Warfighting Center
Fort Monroe, Virginia

Mr. Terry Mayfield
Assistant Director
Computer & Software Engineering Division
Institute for Defense Analyses/ARPA Information Survivability Program

Mr. Ed McGrady
Center for Naval Analyses

VAdm Henry C. Mustin USN (Ret.)
Senior Analyst
Evidence Based Research, Inc.

Capt James R. Neff USN
IW/C2W Advisor
Naval Doctrine Command

Capt Richard O'Neill USN
Deputy Director for Strategy and Policy
Office of the Secretary, C3I
Department of Defense

Mr. Mark S. Pellechi
Office of National Security Policy
Department of Energy

Capt William H. Round USN
Director
Center for Advanced Concepts and Technology
National Defense University

Capt. James A. Rousseau USAF
USSTRATCOM

Mr. Matthew Russell
Office of the Under Secretary (Strategy & Resources)
Department of Defense

Dr. J. Kenneth Schafer
Director
Office of National Security Policy
Department of Energy

Maj. Chuck Schoonover USAF
Chief, IW Branch
US SOCOM J3-IW

Mr. Stuart J.D. Schwartzstein
Visiting Senior Fellow
Center for Strategic and International Studies

Dr. Stuart Starr
Vice President
MITRE Corporation

GEN Donn A. Starry USA (Ret.)
Chairman of the Board
Maxwell Laboratories, Inc.

Dr. Irvin D. Sugg, Jr.
Investigative Training Unit
Federal Bureau of Investigation Academy

Ms. Glenda Turner
Office of the Secretary (Infrastructure Policy)
Department of Defense

RAdm Gary F. Wheatley USN (Ret.)
Senior Analyst
Evidence Based Research, Inc.

Maj. Bob Wiedower USMC
Action Officer
USMC Headquarters

Mr. Fred Wieners
National Defense University

Mr. Owen Wormser
President & CEO
C3I

Mr. David Wynn

Lt.Col. Ernie Zernial USAF
HQ USAF SCTW

Appendix B. The Realm of Information Dominance: Beyond Information War

by

Dr. Richard E. Hayes

President, Evidence Based Research, Inc.

Dr. David S. Alberts

Director, Directorate of Advanced Concepts, Technologies, and Information Strategies

October 1995

Background and Purpose

"Information warfare" has become the buzzword for those looking to the future of U.S. national security as we approach the 21st century. Consensus has emerged that those capable of acquiring, leveraging, and protecting information and information processing systems will dominate the first decades of that era. However, little systematic thought has been given to the overall size and shape of the realm within which these contests will occur, the range of actors who will play significant roles, the instruments that will be brought to bear, or the opportunities and vulnerabilities inherent in the process.

This paper provides an initial exploration of the arena and attempts to (a) identify the key dimensions of the problem, (b) locate the most important areas of the global information systems, and (c) generate insights about the processes of important information interactions.

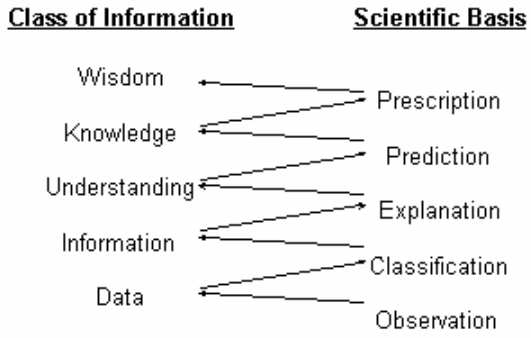
Typology of Information

The simple, but crucial, step of defining what is encompassed by the term "information" is all too often ignored by those who write about its importance and its future. Most typically in the fields of communication and computer systems "information" derives its technical meaning only when it is contrasted with the lesser category of "data." In this formulation, unsorted, inchoate data and reports (for example, raw sensor information or a set of unanalyzed news reports) are seen as data. Once sorted, classified, or interpreted into useful form (air tracks, an assessment of enemy military readiness, etc.) this same material becomes information. Thus, the key distinction is between data as raw material, and information as a product with added value for its users because of the processes by which it has been selected, organized, and presented.

In fact, however, information dominance and information warfare include much more than simple data and its value-added transformation into information useful for decision making. As Figure 1 indicates, the hierarchy of "information" can be related to the

scientific process of exploring a new field, developing theories about a knowledge domain, and applying it to achieve specific purposes. In this paper "information" has been italicized when it refers to the full range of meanings -- from data through wisdom.

FIGURE 1. TYPOLOGY OF INFORMATION AND SCIENCE



At the lowest level, scientists approach a new field by observation, which involves the assembly of large amounts of raw data. New tools emerge for better observation and large enough sets exist to allow comparison. Types of objects may then be identified that can be reliably classified by characteristics that have validity (are substantive meaningful differences). With these classifications, scientists can begin to exchange information and identify patterns - learning what is associated with what, what is common or rare, and so forth.

Understanding about a set of objects emerges when explanations can be offered that link the classifications together by means of causal statements. Simple correlations do not provide causal information since they can result from unseen factors or random chance. However, once the causal mechanisms for differences and changes over time have been found, the field approaches a new level of maturity, with the corresponding transformation from having information to developing knowledge.

Prediction requires more than simple understanding. It implies that the cause and effect relationships are so well known that the implications of changes in the environment on the causal processes can be established before the fact. For example, knowing that supply and demand interact to produce price in an efficient market is insufficient to predict the

impact of a change in supply unless the nature of the market (monopoly, oligopoly, competitive, etc.) and the elasticity of demand for the goods in question are also known. Hence, "knowledge" requires both an understanding of the causal relationships at work and the boundaries or limiting conditions where and at which those causal relationships are transformed.

Finally, "prescription" deals with the wise use of knowledge. The human condition and modern society are so complex that unintended consequences abound. Hence, the moral science of prescription -- deciding what to control and what degree of control to exercise -- requires not only knowledge, but also informed judgment.

Understanding that the term "information" is used to encompass all these forms provides a crucial insight into the breadth of "information dominance." First, one immediately grasps that attacks on an adversary may be directed at all these different levels of information. Defenses of information must, therefore, be built to protect all these levels as well. By the same token, successfully leveraging information requires coherence and validity at all five levels -- proper measurement and classification in order to support analysis of the correct relationships to reach conclusions that are valid over time and can be acted upon effectively. Hence, those who concern themselves only with the narrow concepts of protecting or attacking at the levels of data or information content will both miss major opportunities and fail to recognize those types of information with greatest leverage.

Describing The Realm of Information Dominance Contests

The realm where information dominance is sought can only be fully described by specifying three key aspects of these contests:

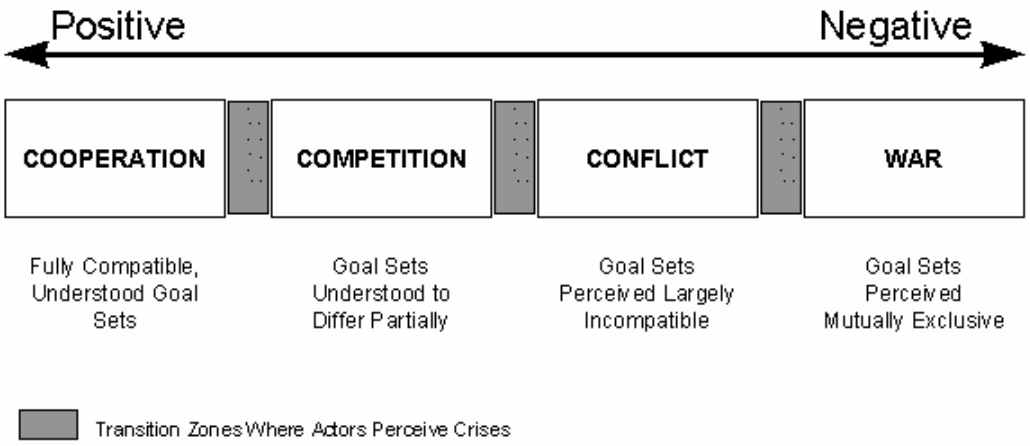
- the nature or quality of the interactions;
- the arenas of interaction; and
- the types of entities that interact (actors).

Each of these three aspects of the information dominance realm is large and complex, but none of them are genuinely independent. That is, the type of actor, type of interaction, and arena of interaction must all be known to reach an intelligent understanding of what has occurred, is occurring, or may occur. In reality, there are multiple "contests" occurring simultaneously.

Types of Interaction

Because the ideas of information war and dominance are usually portrayed in a negative environment, they are often imperfectly perceived. In fact, as Figure 2 illustrates, the quality of significant information interactions depends upon the goal compatibility of the entities involved in the interaction. These range from pure positive or cooperative models to purely negative (or combative) ones.

Figure 2. **Nature of Interactions**



The information warfare literature begins with the assumption that two entities (e.g., nation states or groups of countries) have decided that their goals in important arenas are mutually exclusive, which requires one actor to seek to impose its will on another through force of arms. The traditional view has been that the imposition of will is accomplished largely through means of kinetic weapons or weapons of mass destruction. The information warfare prophets of the "Revolution in Military Affairs" (RMA) foresee employing information based systems and weapons through "soft kills" and sowing confusion on the other side, to either defeat military forces (for example, by persuading the general population or political elite to abandon a struggle) or have a decisive impact by creating dominant battlefield awareness for one side. This includes a variety of subsets of information warfare that have been commonly identified, including command and control warfare (C2W), electronic warfare (EW), and information based warfare (IBW).

The narrow nature of this interpretation becomes apparent when coalition warfare (expected to be a common mode of operation in the 21st century) is considered. Effective information dominance in this context involves both a set of conflictual interactions (the information warfare with an adversary) and a set of cooperative interactions (coalition planning and appropriate sharing of information), potentially involving competition based on complementary, but not fully compatible, goals such as conducting effective warfare without compromising intelligence sources and methods. Thus, the concept of information dominance goes far beyond what is typically considered the information warfare of the 21st century.

Another weakness of considering information dominance only in the context of information warfare emerges in debates about the proper boundaries between war, conflict by other means (economic, ideological, etc.), and "legitimate" international competition. Economic competition in the global marketplace is seen as "good" by

economists, who see intervention by governments to gain advantage in that competition (import substitution policies, tariffs and other barriers to protect domestic industries, etc.) as "bad." However, governments routinely gather information about the strengths, weaknesses, strategies, and vulnerabilities of foreign companies and seek to provide support (political, informational, economic, etc.) of their own corporations in order to generate employment and collect more in taxes. Recent trends appear to reinforce the nation state in acting to support the domestic economic system.

Indeed, there are a number of areas where cooperative economic and other interactions among international actors are highly beneficial or absolutely essential. OPEC represents an economic effort at cooperation by some governments. Free trade zones and trading blocks are strategies employed by countries perceiving compatible goal sets. Global environment issues are increasingly arenas where cooperative information exchanges are perceived as essential.

Continuing to think about information warfare rather than information dominance will lead to myopic views regarding the possibilities for harnessing and protecting information to achieve national ends. This is not a question of offensive or defensive uses of information, nor the use of information to make the instruments of power more effective. Rather, this is the use of overall information dominance in arenas other than direct warfare or conflict to advance national ends. **Failure to understand that information dominance can only be obtained through the correct mix of positive and negative interactions could make the task of crafting an effective strategy for information dominance all but impossible.** The full range of positive through negative interactions, often some of these with mixed strategy across arenas and actors, will be essential to success. Some types of cooperation will be essential to effective competition. Cooperation in some arenas will prove essential to managing conflicts and conducting successful warfare in others.

Arenas of Interaction Containing the Instruments of Power and Influence

The broad areas where societies interact have been organized in Figure 3 from the most concrete to the most abstract, using traditional mid-20th century concepts. The military arena here represents concrete forces -- kinetic weapons and weapons of mass destruction, military formations organized and equipped to fight in areas as sophisticated as tank battles and as primitive and guerrilla fighting in the jungle. The quality of information about the battlefield (completeness, accuracy, currency, precision, and consistency across the military force) has long been accepted as an important determinant of fighting capability and military mission success.

FIGURE 3. ARENAS OF INTERACTION

(Instruments of Power)

ARENA	SUBSTANTIVE CONTENT
Military	Organized Armed Forces
Technological	Application of Knowledge to Accomplish Work
Economic	Creation and Distribution of Goods and Services
Political	Authoritative Allocation of Goods, Services, and Intangible Rewards
Social	Interactions Between and Within Groups
Ideological/Religious	Moral Sciences and Prescriptive Knowledge

Only slightly less concrete is the technological area in which knowledge is applied to accomplish work (physical or mental). Military systems typically represent some of the most advanced and most reliable forms of technical application, both in engines of destruction and in supporting activities such as transportation or information technology. Societies compete fiercely in some technology areas and cooperate in others (for example, safety equipment and anti-pollution devices), though mixed motives are quite common. Protecting technologies, gathering information about the technologies of potential rivals, and leveraging technology are major arenas for interaction.

The economic system, which creates and distributes goods and services, is one of the key dimensions of interaction. Efforts to collect, protect or leverage data, information, models or explanations, predictions and prescriptions (including plans) in the economic arena are a classic application of information systems.

Political systems by which power is brokered and goods, services and other rewards are allocated authoritatively are less concrete than economic systems, but very important nonetheless. Social structures, which organize the interactions between and within groups, also contain and depend heavily upon information. Understanding the cleavages and bonds that undergird a society or define the relationships between two actors can be very important.

Finally, and in many ways quite important, interactions take place in an ideological or religious dimension that represents the moral science or prescriptive knowledge of a

society. Without insight into this type of interaction, prediction is all but impossible because the goal structure of potential allies, neutrals or adversaries is almost impossible to understand. With such knowledge, however, highly leveraged courses of action are possible.

Two other points need to be made with respect to the arenas of interaction. The first is that depicting these dimensions as a continuum is an artificial way to decompose reality for purposes of analysis -- significant interactions and activities often cut across these boundaries, though they typically have a dominant arena. For example, warfare clearly has military, technological, economic, political, social, and moral components. The more connected a process or entity across these levels, the more important the interactions in which it participates. Those that are richly connected across arenas usually offer greater opportunities for mixing positive and negative interactions, thereby avoiding overt conflict. At the same time, however, those that are richly connected also offer multiple avenues of approach to any adversary seeking to operate conflictually. Thus, the existence of rich connectivity creates vulnerabilities and "encourages" the spread of conflict or war into traditionally non-military realms.

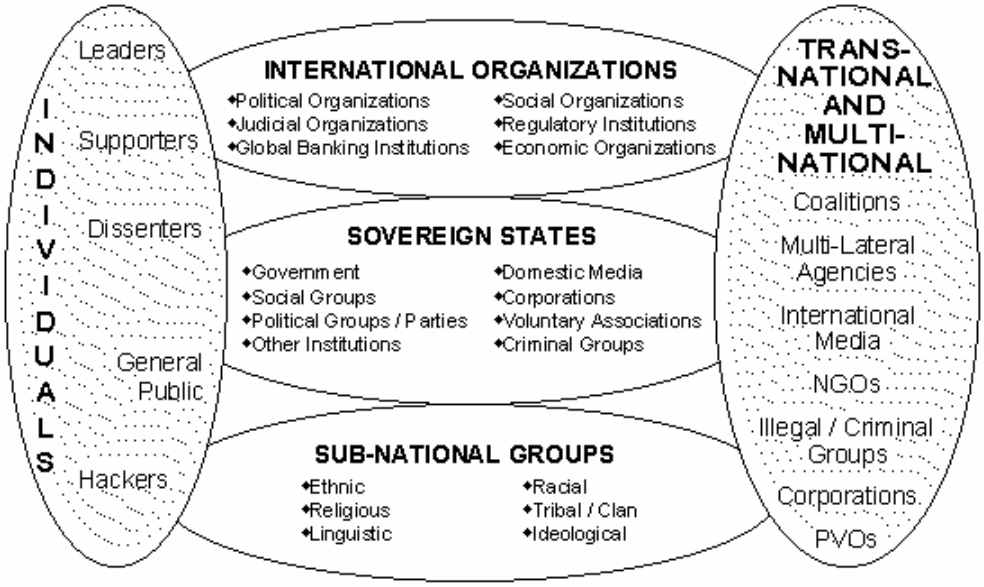
The other key point is that these arenas are both the context of interaction and the classes of instruments of power that can be applied. Attacks that cross arenas can be particularly effective. The classic idea of winning political victories that force a military adversary to retire from a conflict is one of the more obvious forms of asymmetric battles. Economic sanctions, use of computer disruption of financial systems in foreign countries, attacks exploiting social differences in a society, and the use of military forces to gain access to raw materials or valuable land represent other asymmetries that exploit the holistic nature of the conflict arena.

At the current point in history, the potential for asymmetric information exploitation (including patterns of cooperation that gain technological or other advantages as well as negative interactions) is extremely significant for information dominance and makes focus on information warfare particularly dangerous. Focusing attention and defensive measures only on a single level of society, but particularly concentration on the military sector, will leave major vulnerabilities and will lead to important missed opportunities. The military sector in most societies is subject to political, social, economic, technological, and moral attack. Understanding that true national security involves effective control of all these arenas is essential for successful creation of information dominance.

Types of Entities

An enormous variety of actors is relevant to the actors information dominance. Figure 4 shows one way to think about this variety -- organizing them by levels of analysis. As it shows, thinking through global information interactions requires more than dealing with the sovereign states that compose the international system. A wide variety of other entities must be considered.

Figure 4. **Types of Entities**



On one level, the legal status of groups can be used as an organizing principle. Sovereign states have created a variety of international organizations to perform global functions. These include a range of functional entities that most sovereign states find useful. These seek to provide both forums for working out successful patterns of international interaction (political and judicial organizations), or ways of implementing significant programs (banking, social, regulatory and economic organizations). At the same time, there are subnational groups, formed around a wide range of issues, that may cut across or fall within sovereign states, but lack the attributes of sovereignty (territory, legitimacy or recognition, and monopoly of coercive force). Increasingly, however, there is a third type of actor that tends to exist outside of or cut across state boundaries -- transnational and multinational groups and organizations. These vary widely in legitimacy, purpose, and visibility, sharing only the unique capability to defy sovereign governments by moving their activities across national borders.

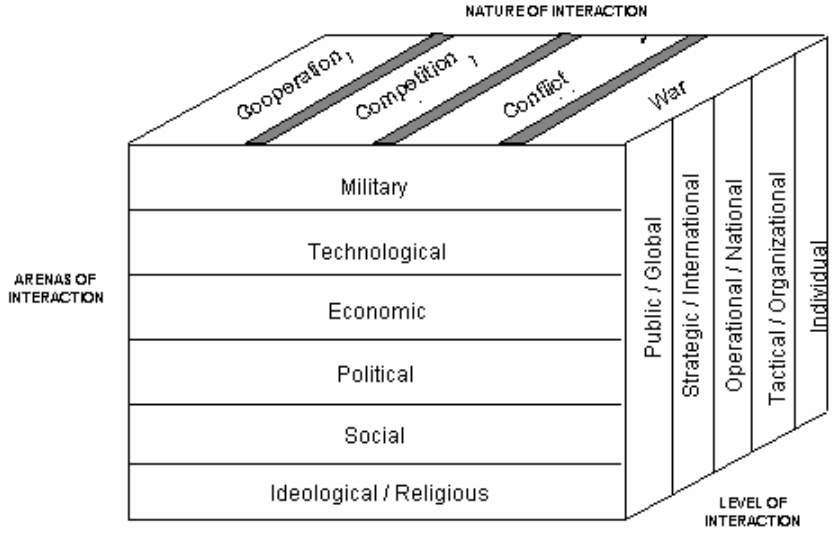
Finally, but very important, information interactions also involve specific individuals. These include leaders of governments, groups, institutions, and other entities as well as their supporters and dissenters. The "general public" also plays a major role in many interactions (notably the social, economic, and political) and, therefore, makes a significant potential target. Even isolated individuals, such as computer hackers, must be considered when the arena is defined because they have the potential for highly disruptive or dangerous actions.

This mass of actors and potential actors greatly complicates the problems of information dominance. On one level, it makes the target environment immensely rich. On another level, the threat matrix is also huge. Deciding how to deal with the vast array of potential information arena entities remains a central challenge.

The Integrated Information Dominance Realm

The three most important dimensions of the information dominance realm are brought together in Figure 5. For simplicity, the levels of interaction dimension has been integrated into a continuum ranging from the individual level through interactions between discrete organizations (tactical operations for the military) to the national (operational) level and the international (strategic) to the global (public) level. Other distinctions between actors, such as their legal status, were judged less important than the level of complexity and range of issues they address.

Figure 5. **Information Space**



The key insight that emerges when these three dimensions are brought together is the very large overall space within which information dominance must be sought. On the one hand, **specific arenas, such as counter-command and control warfare (C2W) or the broader information warfare concept actually occupy only a small portion of the relevant space.** While they may be very important, these are but part of the overall problem.

Perhaps more important is the fact that narrowly defined information warfare ideas are doomed to failure. On one hand, they are doomed because they can be readily flanked. Massive military capability can be rendered impotent by sophisticated media attacks. Economic power can be attacked based on concepts of social differences and "fair" competition, resulting in boycotts, legal barriers, or other asymmetric strategies. Building powerful information infrastructures that depend on the global information industry for maintenance may well build in vulnerabilities or even systematic structures that permit electronic espionage.

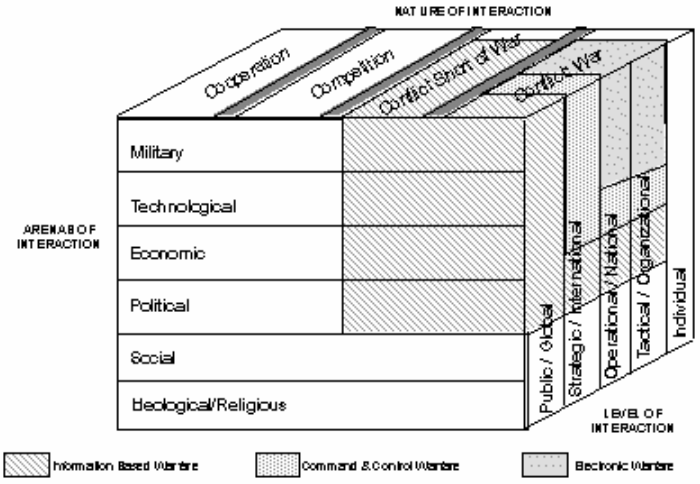
Asymmetries of different types may also create vulnerabilities. Groups or organizations with different agendas undertake attacks in forms that cannot be predicted from threat analyses that focus on national targets. Individual hackers have shown remarkable flexibility and resilience when attacking large systems. Differing perceptions of goals compatibility can also lead to inappropriate cooperation, virtually giving away key information. Indeed, "false flag" operations will undoubtedly be an important tool for gathering information where social cleavages or other differences can be exploited.

Finally, the integration of systems across arenas and the access implied for a wide range of actors and the mix of motives they will have combine to ensure massive vulnerabilities. As information sciences tie the world together more closely, three types of key vulnerabilities are magnified. First, the ability of any given actor to acquire information (legally or illegally, openly or covertly) rises because of the increased connectivity of systems. At the same time, the ability to spread false information or "selected truths" rapidly and (at least in theory) anonymously increases apace. Finally, the "insider threat" will continue to rise in all systems because the knowledge of how to use the systems will spread along with the variety of actors participating in the global information network.

Locating Efforts in The Information Dominance Realm

With the information dominance realm described, as in Figure 5, the narrowness of the current thinking about information warfare is thrown into bold relief (Figure 6). Electronic warfare, for example, covers only a narrow band of military and technological fields and is practiced only in time of war, largely against targets ranging between tactical and operational levels. Counter command and control warfare (C2W) is somewhat broader, often aimed at the strategic level as well as the tactical and operational, but is still limited to warfare scenarios and those crises likely to become wars and stays in the military and technological arenas. Even the much-touted "information based warfare" concepts, which do take into consideration the general public and arenas such as the economic and political, focus only on conflictual arenas, thereby missing the massive opportunities inherent in competitive (mixed motive) and cooperative information instruments. Hence, **the need to focus on the entire information dominance realm and to integrate efforts across that broad realm comes into focus when the larger picture is considered.**

Figure 6. Locating Common Information War Elements



However, only at the most general level of policy and planning can the entire information dominance realm be considered. Useful plans and programs, for offense, defense, and better leveraging existing information will have to focus on particular elements of the problem. Several arenas where U.S. policy makers have experienced difficulty are obvious examples of interactions that are either not military enough or not technological enough to be handled by those who have been thinking about information warfare. For example:

- the vulnerability of democracies to false, misleading, or carefully crafted attacks orchestrated through the news media;
- attacks by creative individuals skilled and determined enough to exploit communications systems and computer networks for illegal gain or to disrupt society;
- criminal organizations (terrorists, drug smugglers, illegal arms merchants, international poachers, and rogue banking groups) that sit across any one country's boundaries represent a poorly-met challenge;
- coalition warfare in which military cooperation and interoperability are essential, but political goals are not fully compatible and intelligence sources and methods must be protected; and
- psychological warfare waged against a general population in order to undermine confidence in leaders or the wisdom of their actions, often exploiting ethnic, social or moral cleavages in the target society.

Perhaps more important, there are entire fields where virtually no systematic thinking has been done. One important example is the topic of international technological cooperation in order to acquire information about foreign competition or foreign technologies and to

protect technological capabilities. Another is pursuit of selected cooperative development programs by which access to foreign markets and technology is achieved through joint ventures or other arrangements. This field has largely been left to the major international corporations, who are transnational and have no incentive to protect U.S. national interests.

On a different level, very little effort has gone into developing knowledge about how information is processed and decisions are made in foreign societies. Better knowledge of these processes and an ability to understand their dynamics are essential for achieving information dominance. The leverage available from manipulating the way situations and processes are understood, the predictions made by foreign leaders, and the criteria by which they select courses of action is much greater than that inherent in simply manipulating raw data and information. Until this gap is addressed, U.S. policy makers will be working in an unnecessarily simple arena. In the rich realm of information dominance, they will be playing checkers when they could be playing chess.

Linkage across the information dominance realm is absolutely essential to prevent uncoordinated, piecemeal strategies and tactics and "open flanks" that can be readily exploited. In the Cold War, for example, U.S. moral, political, economic, social, technological and military policies were drawn from a common perspective and coordinated against common goals. In the absence of a single, massive threat, much of this coherence has been lost. The information dominance realm offers a meaningful opportunity to improve this situation.

Appendix C. Fundamentals of Information Warfare: An Airman's View

by General Ronald R. Fogleman

Chief of Staff

Presented to the National Security Industry Association-National Defense University Foundation Conference on The Global Information Explosion

Washington, D.C., May 16, 1995

The information technology explosion that's out there sweeping the world is an important matter, not just for the military services, but also for industry, the government, and our whole way of life. I have been looking forward to this opportunity to share with you what the Air Force is doing to capture the potential of new information realities. I see information warfare as having both an ascending and a transcending role in military operations. To understand why I say this, I will draw a little bit upon my academic background.

The history of the Second World War offers great examples of the military and civilian leadership manipulating information, even in a very crude fashion, to achieve rather spectacular results. In those days, as we thought about dominating the information spectrum, we turned to the cryptographers who were on the leading edge of these efforts, the so-called "code breakers." These specialized folks focused intently upon breaking the Japanese and German codes. In Europe, the ULTRA project -- "ULTRA" for the "ULTRA secret" -- produced spectacular results. Our code breakers literally worked miracles.

After the Normandy invasion, the German 7th Army attempted a counterattack to drive the Allied forces from the rather tenuous beachhead that they held. But with the help of ULTRA's ability to read the German mail and message traffic, we knew precisely what they were doing as they began to gather their forces to make this attack. We were able to put the British Second Tactical Air Force and the United States Ninth Tactical Air Force immediately upon these armor formations just as they massed. ULTRA gave us the critical information that allowed us to defeat the German forces before they ever came in contact with our ground forces.

By comparison, if you think to December of 1944 and the Battle of the Bulge, we see an example of where the Germans were able to catch us by surprise. They used an alternative communications network, and the Allies did not realize that the Germans had made this switch. It was our lack of information that really fueled the initial German success in the Battle of the Bulge. We had come to rely on ULTRA and had developed a little bit of self-delusion -- and the Germans took advantage of it very effectively.

Our ability to monitor the enemy's communications and use that information as an integral part of our operations is really nothing new. There is another example we should

not forget. That's how we control the information that we allow the enemy to receive. Again, I am going back to the Second World War and talking about disinformation, particularly the disinformation campaign that centered on General Patton before and during the D-Day landings.

At that time, the Allies understood the other guy's ability to intercept our open signals, so we devised a rather elaborate plan that played to this emerging capability on the part of the Germans. The Allies set up a fake Army headquarters and generated false communications transmissions in England. As a result, the Nazis ended up with a significant number of troops placed in the wrong positions. Even as they started to pick up indications that there was this great Allied armada that was going to invade Normandy, the Germans refused to believe that there could actually be an Allied invasion of Europe led by anyone but Patton. We played on that expectation in a way that kept Patton associated with his fake headquarters. Even as the Germans began to get higher and higher fidelity intelligence that indicated a real attack at Normandy, their leaders were frozen in indecision and, as a result, tied down considerable forces in France across from the shortest invasion route from England.

I think from time to time we tend to forget about these early successes. I am sure you understand fully the significance of such efforts during the Second World War. And, you can begin to extrapolate and see the potential for similar operations in today's environment where we have become more and more reliant on information and the infosphere environment.

As I reflect on these activities, I begin to realize the tremendous advances that have come about with microchips, fiber-optics, space, and information storage over the past five decades. I am convinced that a tremendous potential exists in this area for a major breakthrough in the conduct of war. In fact, as I stand back and look at the weapon systems we have today, and I try to project forward the evolution of weapons and technology into the next five to 15 years, I cannot see where there will be tremendous advances in the types of weapon systems we are fielding today.

For instance, the aircraft we will fly over this time frame are fundamentally the same kinds of aircraft we are flying today. Some will have more advanced avionics, more advanced stealth characteristics or other features; but in the main, aircraft will remain fundamentally aircraft as we know them today. Ships will remain fundamentally ships as we know them today. The same holds true for tanks and armored personnel carriers.

There are two closely coupled areas where I do see tremendous potential for breakthrough: the ability to exploit and exchange information, and the ability to detect, fix, and target objectives on a battlefield. Because fundamentally, it will be information and the capability to move it around that will change the internal characteristics of ships, aircraft, battle tanks, and armored personnel carriers we operate on and over the battlefield. It is upon this foundation that the services, and the Air Force in particular, approach this emerging area of information warfare.

I think that a useful place to start is to define what I mean by information warfare, particularly since I think there is a risk in perceiving all warfare in the information age as "information warfare." In my view, I can tell you that's not the case. I would like to offer a definition that focuses on the military fundamentals of information warfare, or what I've called the fifth dimension of warfare.

There are three key parts to this definition. First, information warfare (IW) includes those actions we take to gain and to exploit information on the enemy. Second, IW includes what we do to deny, to corrupt, or to destroy our adversary's information databases. Third, how we protect our systems must also be included as part of IW. No matter how you define information warfare, we must think of it in terms of how it enhances joint warfighting. If it doesn't do so, then I am not much interested in it, and neither are the other service chiefs. I believe that this is an important point.

Information warfare is not the exclusive domain of the Air Force, or any other service. I think information warfare has different meanings to a soldier, sailor, Marine, or airman. For instance, the soldier's focus may be on what happens at the corps level and below. The sailor's and Marine's focus is on the maritime and littoral regions. At the same time, an airman's focus is theater-wide, from the front lines to the adversary's capital. You begin to see how IW covers the entire battlefield. But, because of these divergent views and unique needs, I think it's critical that all services come to grips with and develop capabilities for their respective mediums of operations -- that is land, sea, and air. Then, it falls to the joint force commander, or the regional commander-in-chief, to integrate these capabilities to accomplish the mission.

The Air Force has put considerable effort into developing our concepts. In fact, over the past four months, we have had a team travel to every commander-in-chief (CINC) of a U.S. unified command and brief them on our efforts to incorporate IW into our doctrine and to integrate these concepts into our force employment. Most importantly, we want to be sure that what we are doing and how we approach the subject as an institution will be consistent with the way the CINCs intend to fight. And we want to make sure that what we are doing will meet their needs.

As a practitioner of the profession of arms, I view information technology advances with a single-minded interest. I am motivated by the fact that throughout history, soldiers, sailors, Marines, and airmen have learned one extremely valuable lesson relative to engagement with an opposing force. That is, if you can analyze, act, and assess faster than your opponent, you will win.

The information explosion discussed here today is going to make dramatic changes in how this nation fights wars in the future. Such technology will allow a commander's vision and view of the battlefield to be shared at the lowest level -- to the flight for the airman, to the company on the ground, and to the ship's bridge. Simultaneously, soldiers, Marines, sailors, and airmen on the front lines will be able to see and exploit opportunities as they occur.

What this means is our joint forces may enjoy what some are calling "dominant battlefield awareness." We have some of this kind of capability today. We've made significant enhancements to our ability to leverage our forces with faster command and control and intelligence networks. Among other capabilities, these networks are dramatically reducing the time required to detect and destroy a target.

This process starts with how we gather data. Our intelligence, surveillance, and reconnaissance efforts have been significantly and dramatically improved since Desert Storm. If you are familiar with our TALON programs, you will appreciate what we are doing to reduce the sensor-to-shooter loop -- that is injecting what is detected by our space-based assets directly into the cockpit or a flight deck. We are making similar advances with the systems that operate within the earth's atmosphere. For example, our AWACS early warning aircraft have been greatly improved. Their current radar upgrade allows us to detect cruise missiles at twice the range that we could previously. The AWACS is being fitted with the Joint Tactical Information Distribution Systems, or JTIDS. We will start the initial JTIDS operational test this August. l expect that we will reach full operational capability before the end of the decade.

JTIDS alone will give us some pretty significant capabilities. It is not restricted just to AWACS. It also gives our warfighters a secure and jam-resistant data link between Air Force, Navy, Army, and Marine units and future coalition partners -- on land, at sea, and in the air. What that really means is all the players will have a real-time picture and awareness of both what is happening on the ground and what is going on in the air above those forces. JTIDS will give us a tremendous capability to know, at a much higher fidelity, the location of both the enemy and our own forces.

We are also making similar improvements in how we plan and control air operations. Today, we are fielding CTAPS -- the Contingency Theater Automated Planning System. CTAPS will connect our command and control from the joint forces air component commander (JFACC) to the air wings and the base-level planning cells. It will allow us to generate, disseminate, and monitor the progress of the daily air tasking order much faster than we ever have been able to do before. CTAPS also will tie in with the Combat Intelligence System which will provide us the enemy's order of battle through imagery and integrated threat data.

What does this really mean to us? During *Desert Storm,* it took us about 48 hours to plan and disseminate the ATO. That doesn't mean that it took 48 hours to execute a request from the field. But, it means that the deliberative process that planners went through to service targets was a 36- to 48-hour process. And you had to have someone manually intervene with an immediate air request to get inside those planning cycles. What the CTAPS system will do for us is take this 48-hour cycle and compress it to 12 hours. This really isn't some pie-in-the-sky system that we're dreaming about or visualizing. This is something that is in full use in exercises today and will be operational across the force next year. We have a similar planning tool that has been operational with our global air mobility forces for about three years.

These are a couple of examples of the kinds of tools we are putting in place. They are going to do more than replace the grease pencil and butcher block paper that (retired Air Force General) Chuck Horner and his staff had to use to run the air war during *Desert Storm*. These systems are going to help us dominate the information spectrum. I am convinced that this capability will be critical the next time our forces are employed in combat.

If you recall, I described information warfare in terms of how we deny, corrupt, or destroy our adversary's information base while we protect our own. Much of this activity has a very offensive element to it. I think we have been doing this for some time, but perhaps we didn't use that term. For example, during *Desert Storm,* we targeted many of the Iraqi communications nodes and physically destroyed Saddam Hussein's ability to talk to his troops through normal channels. We forced him into sub-optimum modes of communicating.

In the future, we will approach this objective by viewing our adversary's information activities as a system, and we will engage that system in a variety of ways. In fact, rather than put a precision guided munition into the central telephone exchange in Baghdad and destroy it next time, we may elect to leave it standing so we can better exploit it through our advances in information warfare. So, there will be trade-offs between lethal and non-lethal dimensions in the IW arena.

In the same manner, we have been doing some things along the way that we could properly classify as offensive information operations. There are ways that we corrupt information available to the enemy to deceive him. They include using psychological operations and our electronic warfare assets, like the Compass Call aircraft. I think that these kinds of measures that are designed to corrupt information the enemy has are really critical tools that we provide to the CINCs today. They open the envelope for the potential of further operations tomorrow. Again, if you think back to what we did on D-Day with disinformation, and you consider the tremendous advances in technology since 1944, you begin to appreciate the tremendous potential that exists in this area.

If we recognize an adversary's information network as a lucrative target, an adversary will view our data banks and weapon systems the same way. Information security -- the classic OPSEC, COMSEC, and the more recently stressed computer security -- takes on a whole new level of urgency. As a result, the Air Force is taking some rather significant measures to safeguard our assets. This year, we are spending more than $80 million on defensive measures alone, including establishing a base network control center to protect access to computers and communications. This same center will permit us to see if someone has tried to gain access to our system and, hopefully, will allow us to track down who tried to intrude on the system. These initiatives are important because we run a tremendous risk if we look at information warfare as something that is unique to America. It is not, and by the same token, the U.S. military is not alone in this vulnerability.

Our commercial sector, other elements of the government, and our industrial sectors rely on information systems just as much, if not more, than the military. If you've read Tom

Clancy's recent thriller, Debt of Honor, you're familiar with what may be plausible. In this fictional tale, Clancy describes the problems caused when someone infects the stock exchange's computers with a virus, literally bringing the stock market to a standstill. To me, Clancy's work reinforces how the information threat is more than just a unique military concern.

As I look at information warfare and how it relates to the services, I'm reminded of a story about a football team. It seems that during one of the games, the local team had to put in a back-up quarterback late in the fourth quarter. They were ahead, and they were just trying to hang on. So, they put this relatively untested young man into the game, and all he had to do was avoid making a mistake and the team would win. So, the coach grabbed the guy as he was about to go on the field and said, "OK, here's what I want you to do. Run the ball three times, and then punt." So, the kid understood that and goes out onto the field.

His first run gains 20 yards -- great. On the second play, he gains 30 yards. Now, this is going a lot better than he ever expected. On the third play, he gains 30 more yards. Now they are down on the 10-yard line, the fans are going crazy, and it appears they're going to wrap this thing up. All he has to do is score, and he'll seal the victory for sure. So, the center snaps the ball to him and he punts. Everyone is stunned by this. His coach pulls him over to the sidelines and asks him what he was thinking. And the quarterback replied, "I was thinking that since you didn't change that play, I must have the dumbest coach around."

It is not enough to make a game plan and go with it. You must act and react to what is happening around you. What we're doing today with information warfare is a little bit like that football game -- IW gives us the ability to plan faster with better information so that we can call the optimum play. It may allow us to know what defensive stunt the other team is going to use. It may allow us to give our opponent false information on what play we're about to use. And, most importantly, it may allow us to call an audible and adjust to a fluid situation.

But unlike the game that I just described, when America sends her military forces into action, we don't want a close, exciting game, and we don't want an inexperienced quarterback. This nation has come to expect in our military operations nothing but blow-outs -- 100 to nothing is a good score. And, I believe that exploiting this new and emerging information technology is going to be the key to making this happen.

As we approach tomorrow, we need to do more as a service and with the other services. Let me touch just briefly on what we are doing in terms of changing the way we organize, train, and equip our forces.

First, in terms of organizing, in September 1993, the United States Air Force stood up the Air Force Information Warfare Center in San Antonio. This center has more than 1,000 men and women chartered to support IW planning, intelligence gathering, weapon system analysis, and related activities. This group will be a source of IW support teams to go out and assist the CINCs and JFACCs during crises or exercises. They will help build

information warfare into the air campaign planning and execution. The Air Force is not alone in this. The Army has an Information Warfare Center at Fort Belvoir, Virginia, and the Navy has created a center at Fort Meade, Maryland.

Additionally, the Air Force is adjusting our training and education programs to include IW concepts. We have had a course for our major air command and numbered air force staffs to give them basic understanding of the issues. We are incorporating IW into our doctrine, so that airmen everywhere will share a common foundation and a common terminology. We're adjusting our mid- and senior-level professional military education schools at Maxwell Air Force Base, Alabama. You see part of this effort here today. We have four Air Force officers attending the inaugural class of the National Defense University's School for Information Warfare.

Finally, and most significantly, we are beginning to procure weapon systems with a mindset that places high priority on maximizing their performance as an information warfare platform. One example of that is the United States' new air superiority fighter, the F-22. This aircraft is the first platform to be built around information technologies. This was an established objective when we started the program, not something added after the fact. A lot of people have heard about the F-22's stealth. You've heard about its supercruise capability -- that is the ability to cruise faster than the speed of sound in military power. And possibly you've heard about the fact that it has tremendous agility in the air-to-air arena.

But, you cannot begin to appreciate its potential until you sit in the concept demonstrator and see how the F-22's integrated avionics work. The quality of the composite picture that's compiled from a variety of sources will literally water your eyes, particularly if you're an old-time fighter pilot. For the first time, you'll be able to sit with those flat glass displays and have tremendous situational awareness readily available to you. That is something we've needed for years, and we're finally in the process of getting it. It will allow our pilots to act and assess faster even when outnumbered. And I tell you it isn't just a concept -- it's being put into production today!

The F-22 is just one of many Air Force programs that we're continuing to push forward. You see the same thought processes in the space-based infrared system, in our Joint STARS, and in our precision munitions program. As we move forward, we are establishing an additional requirement for our weapon systems -- that is security against the information threat -- that's being written into the requirements documents.

This new mindset is found throughout our acquisition strategy. We are changing how we view our modernization needs. We're taking another look at IW capabilities, like those associated with command and control, and we're treating them more like force structure than support structure. It's part of how we must change the way we do business to incorporate the fundamentals of information warfare.

This broad approach means that we must get the lawyers involved. When I first heard about bringing in the lawyers, I thought we had really slipped off the deep end one more time. I apologize if I offend any lawyers out there -- I always have held lawyers in fairly

high esteem. The more I thought about bringing the lawyers into the equation, the more I realized we need their expertise. Because exploiting the information spectrum will readily cross international borders, we must be cognizant of what the law allows and will not allow.

When do you begin information warfare in the spin up to a conflict? When do you begin to go out there and intrude in somebody's banking system? When do you begin to get into somebody's telecommunications system? These are all very difficult questions. Clearly, information warfare is not something that is focused solely on the confines of a constrained battle area. While we will fight in a theater, information warfare will force us to be engaged worldwide. Thus, we must have some good advice as we pursue this capability.

I appreciate this opportunity to share with you what the Air Force is doing to try and keep up with the information technology explosion. The American way of war has very strong roots in understanding the value of exploiting information to deny information to our adversary, to corrupt what data he has, and to exploit what we know.

World War II was filled with many examples of information warfare. Perhaps Winston Churchill offered the best summary of its importance. At the Tehran conference, when discussing the Allied plans to manipulate information before D-Day, many of these same ethical questions came up. When do we do it? How do we do it? Who are the innocent victims of this thing? And Churchill, addressing the other Allied leaders said, "In wartime, truth is so precious that she should always be attended by a bodyguard of lies" (Anthony Cave Brown, *Bodyguard of Lies* (New York: Harper and Row, 1975), p. 10). Something to think about. Later, there was a book written with that title by Anthony Brown. If you read his thick volume, it is rather chilling to see what was possible in that era, and then think about how much more is possible today with the technology that's available.

Today and in the future, information warfare is, in fact, going to be this nation's bodyguard. It is essential for the success of our joint forces. To succeed, we are going to need help from a lot of people, including all the very interested people in this room. You understand the far-reaching implications of systems like LANDSAT or SATCOM which are readily available and widely employed at relatively low cost. You appreciate the potential for information technology to allow an adversary to build small, capable, autonomous, operating systems that can threaten U.S. forces on land, sea, or in the air. Such devices might operate relatively unseen and unobserved until they unleash their destructive power.

Appendix D. Defensive Information War: Problem Formation and Solution Approach

by

Dr. David S. Alberts

Director, Directorate of Advanced Concepts, Technologies, and Information Strategies

National Defense University

Introduction

This briefing was prepared, at the request of the Deputy Secretary of Defense (DepSecDef), for participants in a series of interagency meetings about Defensive Information Warfare (IW-D). In addition to providing some background about the nature of "information" attacks and their potential consequences, this presentation also proposes a strategy for dealing with the defensive challenge of protecting against such attacks.

It is hoped that the IW-D strategy suggested here serves to stimulate and focus discussion about the ways in which each of the represented organizations can work together, on a continuing basis, to come to grips with the daunting task of preparing our Nation to deal with what may become one of the most vexing problems of the Information Age.

Information Warfare (IW) has grown to become a "catch-all" term that encompasses many activities long associated with competition, conflict, and warfare, such as propaganda (including Media War), Deception, Command and Control Warfare (C2W), Electronic Warfare (EW), and Psychological Operations (Psyops). This briefing does not attempt to address all of these aspects of IW, but rather focuses its attention upon the subset of IW that involves attacks against information and systems, including what has become known as "Hacker War" and a more serious form dubbed "Digital War."

Analogies and Realities

Defending against "Information Attacks" appears to have a number of characteristics in common with societal efforts to combat disease, drugs, and crime. Noting these similarities helps to put this problem into perspective, provides some potential useful lessons learned, and serves as a relative benchmark.

Before reviewing the specific similarities between combating Information Warfare (IW) and these long-standing problems, it should be noted that, while "eradicating" IW may not be a realistic expectation, significant progress can be made in defensive IW (IW-D) -- enough so that the risks can be kept at acceptable levels.

The problem of IW is similar to the "wars" on disease, drugs, and crime on a number of dimensions. First, the solution to any of these problems requires the efforts of a number

of organizations, both public and private. Second, it is unlikely, given the competition for resources, that any of these problems will be "fully funded." Therefore, we can expect that there will never be what those of us who have IW-D responsibilities think are a sufficient level of funding for IW-D programs. Third, these are not static problems. Drug cartels and criminals certainly learn from their mistakes. Even viruses "learn." Thus, defense forces will be continuously locked in a battle to keep up with attackers. Fourth, awareness and concern will reach peaks, often accompanied with frenzied efforts to solve the problem. These relatively short periods of interest will be followed by longer periods when the urgency of the problem will give way to apathy. Maintaining funding and progress during these periods of waning public interest will be one of the key challenges of leadership in this area. Fifth, organizations and individuals will learn to make adjustments in their behavior to deal with IW attacks and their consequences, many of which will not be predicted. These adjustments will be made so that those organizations and individuals can accommodate some level of pain -- a dynamic equilibrium of sorts -- as the cost of doing business in the Information Age. Finally, solutions will, of necessity, be compromises. This is due to the natural tensions that exist among the various stake holders. Tensions between the law enforcement and civil liberties are a classic example that has already arisen in the information domain.

Current Situation

Attacks on information systems are already a fact of life in the Information Age. Although a small portion of these attacks result in significant loss or damage, the vast majority of them result in little or no damage -- the crime equivalents of trespass, public nuisance, minor vandalism, and petty theft. It has been estimated that over 90 percent of these attacks are perpetrated using available tools and techniques (based upon incidents reported to CERT), that only one successful attack in 20 is noticed by the victim, and that only one in 20 gets reported (these last two statistics were a result of a DISA study and similar rates have been reported by others).

Of more concern is the presence of a technically feasible "Strategic" threat. That is, the means exist to cause significant damage and disruption to U.S. public and private information assets, processes, and systems and to compromise the integrity of vital information. Analysts also have no difficulty identifying groups with the motivations and opportunities to launch such attacks. Given our present vulnerabilities as a Nation, a well planned, coordinated IW attack could have "Strategic" consequences. Such an attack or the threat of such an attack, could thwart our foreign policy objectives, degrade military performance, result in significant economic loss, and perhaps even undermine the confidence of our citizens in the Government's ability to protect its citizens and interests.

While no "smoking keyboard" has been found to validate such a threat, the very existence of the means to carry out such an attack, when coupled with the myriad of motives and the opportunities that exist, results in our present state of vulnerability. These circumstances have created a situation that calls for prudent defensive actions to be taken in the public interest. We need to be proactive rather than be forced to react after an Information Age "Pearl Harbor." Moreover, a successful strategic attack would point the

way and encourage others to plan similar attacks. Hence, we need to go on the offense with a vigorous defense.

"Digital War"

Each age has seen war transformed by "modern" means and concepts. The Information Age promises to be no different. Some have called the Gulf War the first "Information War" -- others have called it the last "Industrial Age" war. The power of information was clearly demonstrated in the context of "traditional" conflict. Information was leveraged to significantly improve the effectiveness of all aspects of warfare from Command and Control, Communications, Intelligence, Surveillance, Reconnaissance (C4ISR) to logistics.

The effectiveness of the United States and its allies in the Gulf War has surely somewhat deterred potential adversaries from taking on our forces in the rather symmetrical manner that Iraq attempted, and has stimulated thinking about other strategies for countering conventional forces. "Digital War," enabled by advances in technology and its wide-spread adoption as well as the globalization of economics and commerce, is surely a strategy that potential adversaries are thinking about to achieve some of the objectives that have previously been sought by means of traditional warfare.

Digital War, a subset of what we call Information War, may be defined as "non-physical" attacks on information, information processes, and information infrastructure that compromise, alter, damage, disrupt, or destroy information and/or delay, confuse, deceive, and disrupt information processing and decision making.

Digital War intrinsically possesses the ultimate form in some of the same characteristics that traditional military planners are striving for -- low cost precision guided munitions, standoff, and stealth. Digital War threatens the ability of a Nation State's military to interpose itself between its population and "enemies of the state," thereby causing a loss of sanctuary. The importance of sanctuary can be inferred by our willingness to spend significant resources on air, sea, and missile defenses.

How does one respond to a serious set of information attacks? Responding with traditional military forces may be politically unacceptable or in fact, may be ineffectual. Currently there is no consensus, even among those in the defense establishment that think about these issues, regarding how to deal with such an attack.

Another characteristic of information attacks stems from the loss of sanctuary. Attacks of this sort, particularly when they consist of more than an isolated incident, create a perception of vulnerability, loss of control, and loss of confidence in the ability of the State to provide protection. Thus, the impact can far exceed the actual damage that has occurred. This non-linear relationship between actual damage and "societal damage" makes the problem of Digital War a particularly challenging one because it creates a mismatch between "rational" defense responses and their effectiveness.

Given the potential effectiveness of Digital War, particularly as an instrument of power for niche competitors and non-State actors, we need, as a society, to take this Information Age form of war very seriously. If we do not, and if we rely solely on traditional weapons and concepts of war, we may be building our own 21st Century Maginot line that can literally be flanked with the speed of light.

Formulating the Problem

The first step in tackling any problem involves developing an understanding of the possible environments that may be faced (or the "states of nature"), one's options, and the objective that is being sought (Figure 1). This requires an identification of the variables that are relevant, that is, those that can significantly influence the outcome as well as the subset of these relevant variables that are controllable, which form the basis for designing options.

[Image not available]

In a problem as complex as defensive information war, working to formally formulate the problem accomplishes three things. First, it provides a useful framework for discussion. Second, it serves to keep the focus on those specific areas that are either unknown or in dispute. Third, it serves as a benchmark for measuring progress.

In this case, the states of nature correspond to the nature of the threat that will be faced vis-a-vis the vulnerabilities of our information infrastructure while our options correspond to the strategies we adopt and the actions we take to defend ourselves. The objective being sought corresponds to a level of infrastructure performance, its definition and measure being a major challenge in and of itself.

A good place to start is to try to develop an understanding of the nature of the threat, or more accurately, the spectrum of relevant threats. This involves the identification of potential threats and the estimation of their likelihood. Normally one would construct a set of states of natures that are mutually exclusive and collectively exhaustive so that a probability density function could be used. For the purposes of this discussion, the states of nature referred to correspond to potential threats grouped in some logical fashion to facilitate analysis of how well each defense strategy does in dealing with each of these threats.

Having an initial concept of the nature and range of potential threats, one can develop alternate defensive strategies and corresponding sets of action to counter one or more of these threats. A great deal depends upon what variables we believe we can and should control.

Each defensive strategy, with its corresponding set of actions, then needs to be analyzed with respect to each of the threats. The results of these analyses will be a characterization of the results or outcomes from pursuing each of the defensive strategies with respect to each of the threats. These outcomes, which are basically descriptions of results (e.g., number of penetrations and their consequences), then need to be translated into "value"

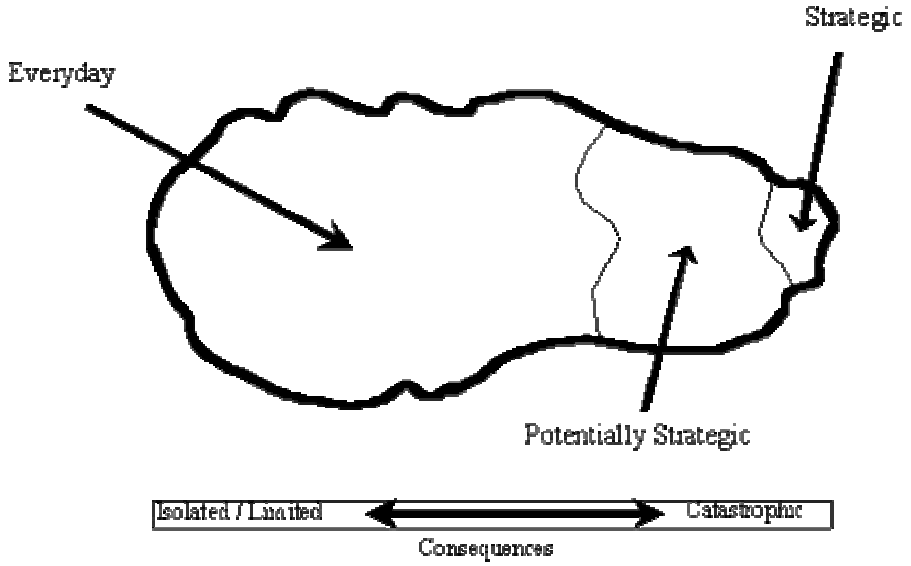
measures that represent their impact. These costs and benefits provide a rational basis for determining an appropriate defensive strategy. Much will depend upon how we measure success.

Given the central role that the threat topology plays in problem formulation, we will now turn our attention to examining this topology.

Threat Topology

The irregular shape of the graph in Figure 2 is intended to show that boundaries are not well defined. The consequences associated with a failure to counter a specific attack range, on the one hand, from isolated and limited consequences to, on the other hand, consequences of catastrophic proportions.

Figure 2. **Threat Topology**



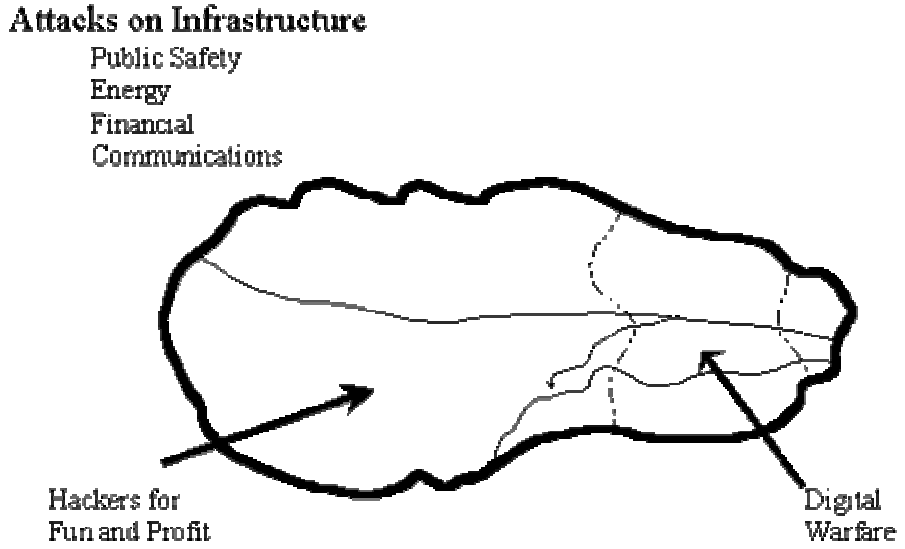
The threat space can be divided into three areas. On the left side of the space we can group the vast majority of the threats that occur everyday. These Everyday threats, while exacting a certain price, do not pose a threat to our national security. On the right hand side of the threat spectrum is a small area that represents those Strategic threats having national security implications. The third area contains threats that may have national security implications. These Potential Strategic threats represent a particularly difficult challenge.

For example, beyond those sets of threats that clearly fall into either the Everyday or Strategic categories, there are classes of threats that span the threat spectrum.

Attacks on our national, or for that matter international, infrastructure do not fall neatly into one area of the threat topology but in fact populate all three classes of threat (Figure

3). These attacks on our public safety, energy, financial and communications systems and services have different implications and consequences depending on the specific nature of the attacks and the circumstances surrounding the attack.

Figure 3. **Threat Topology**



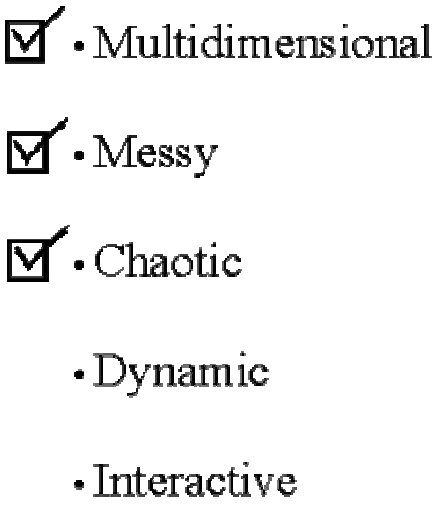
The vast majority of attacks on infrastructure are by hackers whose motives run the full gamut from having some fun to more serious forms of antisocial behavior. Some of these attacks are motivated by profit. While some of these attacks may have serious consequences in the form of significant loses of data, interrupted services, or stolen assets or services, only a small number of these lone perpetrator attacks is likely to have potential strategic consequences. This is not to say that it is impossible that some set of circumstances would result in the snowballing of one of these "hacker" attacks into a National Security concern, but rather that this outcome is unlikely.

However, infrastructure attacks can be quite serious if they are well planned and coordinated. Arguably this would require an adversary with seriousness of purpose and with some sophistication and organization. This kind of attack would be better named Digital Warfare rather than be included as part of the group referred to as Hacker attacks. Depending upon the level of sophistication of a Digital Warfare operation, its consequences could range from a "high- end" Hacker attack to an attack with Strategic consequences.

Threat Characteristics

So far we have seen the threat topology we face is multidimensional, somewhat messy and, with respect to the consequences of information attacks, can behave in a chaotic manner (Figure 4). The dynamic and interactive nature of the threat makes defending against them all the more demanding.

Figure 4. Threat Characteristics



Threat Dynamics

Attackers and defenders are locked in an ongoing battle of wits and resources (Figure 5). Unfortunately, the attackers possess some inherent advantages. For example, clearly the attacker can pick the time, place, medium, and method of the attack. The technology edge also goes to the attacker, for it is very difficult to develop defenses for unknown methods of attacks -- thus offensive technology usually is one step ahead of defensive technology. Those who choose to orchestrate coordinated attacks on infrastructure also have the advantage that comes from being able to control their attack more easily than can a number of loosely coupled defenders.

[Image not available]

In any event this is a learning environment for both attackers and defenders -- a dynamic one at that. In this organic environment, attacker learn from undetected attacks, whether successful or not, while both sides learn from detected attacks, whether successful or not. Both attackers and defenders make adjustments and the "game" continues.

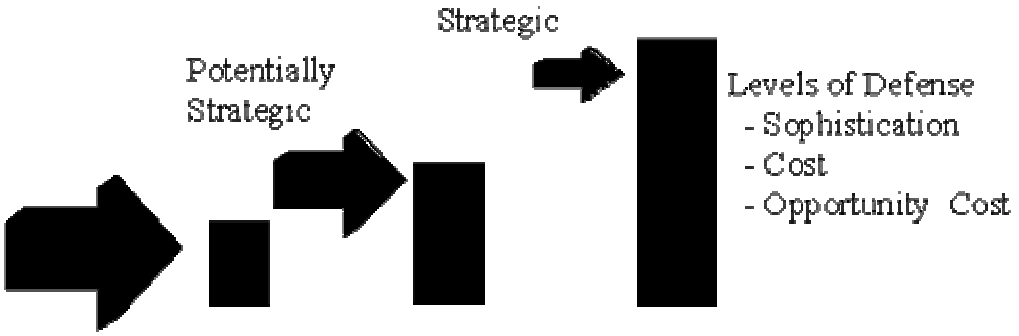
This aspect of the threat means that defense is not a one-time thing -- it must be a continuous activity. It also means that collection and analysis of information about attacks are vital to maintaining parity with attackers. Finally, it means that defenders must be proactive and undertake efforts designed to anticipate methods of attack so that timely defenses can be developed.

IW-D Strategy

The proposed "defense in depth" strategy consists conceptually of three lines of defense (Figure 6). Each line of defense is designed specifically to counter the threats associated with a particular region of the threat topology.

Figure 6. IW-D Strategy

- Defense in Depth Approach
- Majority of Attacks Can Be Handled With Basic Defenses
- Higher Hurdles Handle More Sophisticated But Fewer Attacks From Fewer Potential Sources
- Mix of "Information First" and "Security First" Philosophies



The first line of defense is to defend against Everyday attack, which constituted most of the threat topology. Based upon the information available, the vast majority of these attacks can be handled with basic defenses.

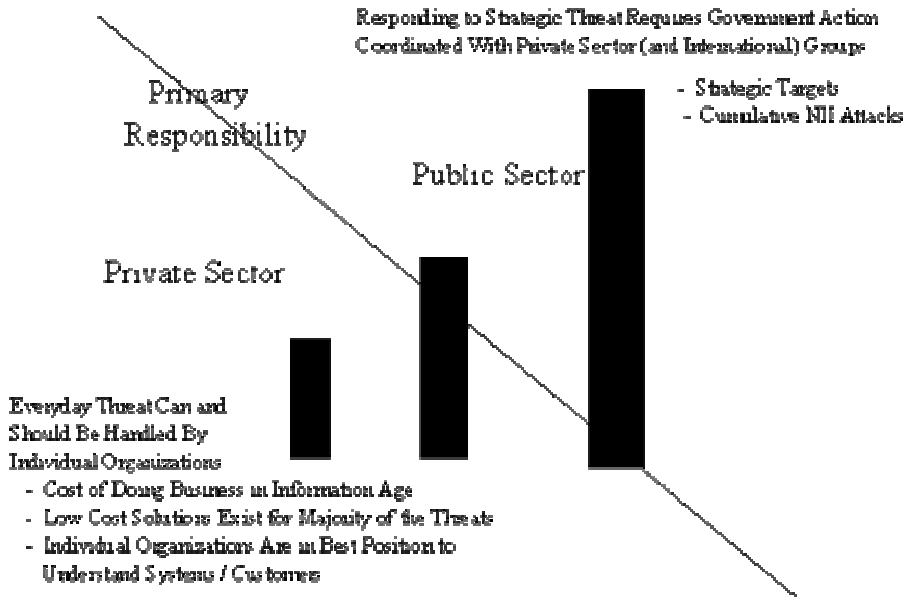
The higher hurdles associated with the Potentially Strategic and Strategic attacks are then responsible for handling more sophisticated but far fewer attacks from fewer potential sources. For example, attacks with strategic implications would need to get through the first two lines of defense that should filter out all but the most skilled, resourced, and persistent adversaries. This means we can concentrate our intelligence and monitoring efforts on a smaller population which in turn increases the chances of successful defense.

This defensive strategy also means that we can take different philosophical approaches with each line of defense depending upon the nature of the threat. The two endpoints of the philosophical spectrum can be thought of as the "information first" and "security first" approaches. In the Everyday region of the threat topology our approach has been to emphasize access to information. In the Strategic region, we put security first by restricting access and connectivity to the point of degrading performance and efficiency.

Division of Responsibility

Figure 7 graphically depicts a suggested division of primary responsibility for IW-D between the Public and Private sectors as a function of the threat topology. The modifier "primary" is used to make the point that, despite the assignment of responsibility in a particular area to either the Public or Private Sector, both Public and Private organizations have responsibilities in each area.

Figure 7. Division of Responsibility



The topological regions associated with either Everyday or Strategic threats are the most straightforward. Primary responsibility for the everyday threat should be the responsibility of the Private Sector. Handling such threats is simply the cost of doing business in the Information Age. With the availability of relatively low cost defenses against these threats, the burden placed on the Private Sector is affordable. Furthermore, organizations are clearly in the best position to understand their own systems and the needs and concerns of their customers.

Responding to Strategic threats is clearly the job of the Public Sector, although an adequate defense will involve some coordination with Private Sector and International organizations, particularly when it comes to the region of the threat topology that contains threats associated with attacks on the National Information Infrastructure or other institutions providing vital services.

Framework for Progress

While we have come a considerable distance in our journey to better understand the nature of this problem, many of us have been frustrated by the lack of a "supportive" environment for progress. Although we can continue to make progress, even on the rocky path we are currently forced to travel, progress in the six areas identified in the graphic will greatly smooth out our path and accelerate our progress.

First, one of the key prerequisites for progress is to create awareness of the problem and its complexities, as well as to foster a climate that will facilitate discussion and cooperation among the many groups and organizations that need to be a part of this effort. Given recent events surrounding some aspects of information security, we need to

start by rebuilding bridges between some Public and Private Sector groups and organizations.

Second, it is important that we work towards a well defined vision that clearly lays out what we are trying to achieve and the appropriate role of Government.

Third, the "rules of the game" need to be developed and promulgated. Many of our current laws and regulations have not caught up with the realities of the information age. A set of "rules" needs to address the establishment of information security standards, or a minimum level of defense to be associated with different kinds of data and information services. These would be similar to the recent development of privacy standards.

Fourth, self-interest, even enlightened self-interest and the desire of individuals and organizations to be a good citizens are not enough to ensure that appropriate actions and defenses will be developed and employed. Resources need to be provided for Government organizations to help implement this framework for progress and to develop and implement the needed defenses. We also need to provide incentives that encourage Public Sector organizations to do what is collectively needed. In some specific cases, the Government will need to actually provide funds to Private Sector organizations to implement enhanced security.

Fifth, the solution to this problem depends on a great deal of cooperation among disparate groups and organizations. Mechanisms to facilitate and enhance cooperation including the establishment of panels, groups, and clearinghouses need to be developed.

Sixth, we need to fix responsibility for the many tasks involved in IW-D. We need to decide questions of jurisdiction. We need to make liabilities known and well defined. Finally, we need to clearly establish the responsibility of each organization. The nature of organizational responsibilities is discussed in more detail below.

None of these six aspects of the framework for progress is likely to be accomplished anytime soon. One only need review the legislative process and experiences with the translation of privacy concerns into a set of rules of the game to realize that it will be quite a while before each of these foundational pillars is in place.

However, we must begin now to foster discussion of these issues and try to keep attention focused on this subject.

Responsibilities: Everyday Threats

The primary responsibility for the Everyday region of the threat topology falls upon the Private Sector (Figure 8). First and foremost, Private Sector organizations must assume responsibility for the protection of their own systems. When "security" laws and regulations are legislated and formulated, these organizations will, of course, also be responsible for adhering to these rules of the game.

Figure 8. Responsibilities

Given the time it may take to develop and put in place a legal and regulatory framework to deal with the myriad of information security issues, it is proposed, that on a voluntary basis, Private Sector organizations assume the responsibility for reporting incidents. It is hard to overstate the importance of the collection of information related to information attacks and its analysis. Without the development of a body of knowledge concerning these attacks, efforts at building defenses will be severely hampered.

The Government (includes Federal, state, and local levels) must assume certain responsibility for this region of the threat topology as well. Clearly, the Government bears the responsibility for protecting its own systems and for the enforcement of appropriate laws and regulations. Given the importance of gaining international cooperation on this problem which knows no state boundaries, the Government must take on the negotiation of the necessary treaties and agreements.

Clearly, the collection of incident data with respect to its own systems is also a Government responsibility. But given the importance of pooling information to gain a more accurate situation assessment, Government must also put in place appropriate mechanisms for data sharing and analysis and for its dissemination. Issues related to classification and security of this data and its analysis products will need to be addressed. A way must be found to get this needed information to individuals and organizations.

IW-D Challenges

For those of us who thrive on challenges, this is a great line of work. The five key challenges we face have been identified as:

- Increase awareness and understanding of the threat/vulnerabilities;

- Develop a strategy for IW deterrence;
- Implement defense in depth strategy;
- Improve I&W capabilities; and
- Develop responses to IW attacks.

Success requires that everyone be on board. Therefore, it is important that we continue to work to increase awareness of this problem and to develop a better understanding of both the nature of the threat and our vulnerabilities.

The first line of defense is deterrence. Not enough effort is being devoted to developing and gaming possible strategies. In mid-February ACTIS is sponsoring a workshop on this subject and we hope to gain a better idea where the latest thinking is on this subject, stimulate more thinking about the subject, and bring some key issues into sharper focus.

Given the trifurcated threat topology and the very different nature of each of the three threat regions, implementing the proposed "defense in depth" strategy will be a considerable undertaking. This challenge, as well as the first two challenges just mentioned will be discussed in great detail below.

The fourth challenge is to improve our ability to see an attack coming, or provide "indications and warning" (I&W) of attacks in a timely fashion. Given that currently, in many cases, an attack in progress is not even recognized, this will be a tall order.

The remaining "top five" IW-D challenge is to develop responses to IW attacks. Responses to attacks include identification, interdiction, apprehension, and punishment (possibly including retaliation).

IW Awareness/Understanding

We have much to learn and many to educate. When many of the individuals who need to become more aware of the threat and its potential consequences are exposed to the subject only by reading novels or going to the movies, we cannot really expect to develop the degree of understanding required. When the only exposure to the subject is through fiction, it is no wonder that the threat may be dismissed as fictional. There are still many individuals in key positions in both the Public and Private Sector who need to have a better appreciation for this problem and to be more motivated to work the issues.

On the other hand, admittedly we are not in possession of a great abundance of factual information. While we have clear indications that some potentially serious attacks, even crippling attacks, are technically feasible, as has been pointed out, there is no "smoking keyboard" to show. Yet it should be pointed out that the time it took to create a working atomic bomb from the time its theoretical feasibility was recognized surprised many, even the most knowledgeable scientists.

Our ignorance about the nature of potential attacks is mirrored by a lack of knowledge about the effectiveness of current and developing defensive techniques and strategies.

When our systems are not being adequately monitored and incidents are not being adequately recorded and investigated, it is hard to see how we can develop the vastly improved understanding of both the threat and the effectiveness of defenses we require. Increased collection and analysis is clearly needed to provide the empirical foundation required to a) increase awareness, b) increase our understanding, c) support planning, and d) develop effective defenses.

IW Deterrence Issues

With the dawn of the atomic age came the recognition that developing strategies for deterrence and counter proliferation needed to be pursued with a sense of the utmost urgency. IW differs from atomic warfare in a number of significant ways and therefore lessons learned from our experience in developing a workable strategy for deterrence may not apply directly to the problem of deterrence of IW attacks, but certainly may provide a starting point or checklist for consideration.

The chart above lists some of the compelling issues related to the development of a deterrent to IW attacks.

While raising the defensive threshold, thereby making attacks more difficult and costly as well as limiting the damage they can do, is widely recognized as an important component of any deterrence strategy, an issue that needs to be addressed relates to the "height" of the threshold. What is more defense? When does more defense become counterproductive?

Another critical issue is whether or not having and indicating a willingness to employ a potent offensive IW capability would be an effective deterrent, and if so, in which particular set(s) of circumstances.

Given the low cost and small footprint required, non-state and even individual actors may gain the wherewithal to pose a strategic threat. How can one gain the leverage on these kind of adversaries to deter them from launching such attacks?

Other key issues include the nature of preemptive actions that could be employed and the relationship between punishment (or retaliation) and deterrence.

Critical Technologies

Building defenses into systems presumes we have the means to do so. Many of the defensive capabilities we currently have are not adequate for certain known levels or types of attacks, not to mention technically feasible but undocumented attacks. The following are some areas in which we could use some advances in technology.

Real-time intrusion detection is clearly a key element in any set of defenses. Our ability to detect, in real time, intrusions into our systems and the identity of the intruder is currently very limited.

It does not take very long to carry out an information attack. Damage can occur in an instant. Clearly an automated capability to respond to an intrusion that can prevent or limit the damage would be highly desirable.

Given our increasing reliance on COTS, we need ways to cost-effectively make sure that the software we buy does what we want it to and only what we want it to. Any Information Age organization buys millions of lines of code each year whose exact origins are not known with any degree of confidence. Automated tools to perform quality assurance (QA) and to verify and validate (V&V) the code would be an immense help.

Knowing for sure that data was not altered or compromised and that the source of a piece of data or a message was verified would go a long way in the effort to combat certain types of IW attacks. More work needs to be done to provide cost-effective data and source authentication.

Summary

The problem is real. Our citizens and the organizations that provide them with the vital services they need can find no sanctuary from these attacks. The low cost of mounting these attacks has enlarged the field of potential adversaries and complicated efforts to collect intelligence and array our defenses. The consequences of a well planned and coordinated attack by a relatively sophisticated foe could be serious. Even the threat of such an attack or "digital" blackmail is a distinct possibility. How the public will respond to the threat of IW infrastructure attacks or to actual attacks is unclear, but their reactions will be a major determinate of future policy and actions.

This situation is getting worse with the rapid proliferation of information technology and know-how. We are becoming increasingly dependent upon automation in every aspect of our lives. As information technology becomes an essential part of the way organizations and individuals create products and provide services, the need for interconnectivity and interoperability increase -- and with these increased need for exchanges of information (and product) vulnerabilities increase. Finally, the increased reliance on COTS makes it more and more difficult for an organization and individual to control their own security environment.

Given this situation we need to focus upon two things. First, we need to find a way to protect ourselves against catastrophic events. Second, we need to build a firm foundation upon which we can make steady progress by continually raising the cost of mounting an attack and mitigating the expected damage.