NATIONAL DEFENSE UNIVERSITY
STRATEGIC FORUM
INSTITUTE FOR NATIONAL STRATEGIC STUDIES

Number 87, October 1996

Information Warfare and Deterrence

by Richard E. Hayes and Gary Wheatley

Summary

- On one level, Information Warfare (IW) and deterrence are well matched, but on other levels the two topics can be seen as orders of magnitude apart. IW covers a huge domain while deterrence is a narrow topic. Their relationship is spotty-highly relevant on some topics, marginally so on others, and not at all relevant in many areas.

- The term "information warfare" typically focuses on the military or cyber-war domains dominated by computers. This narrow definition is inconsistent with the broad policy questions relevant to IW, its impact from cooperation to competition and conflict, and the key role of information media.

- Deterrence is part of IW only when the attacker is known (or can be discovered), the defender has a credible capability to threaten important interests of the attacker, and the attacker cannot defend those interests.

- Participants argued that a visible set of defenses is the beginning point for deterring attacks on important computer systems. Attacks are essentially instrumental acts that will not occur if the attacking party perceives little opportunity for success.

- Media warfare (i.e., countering an adversary's propaganda) can put enormous time pressure on decisionmakers, particularly when an authoritarian state adversary, with little or no necessity for consultation, targets unsuspecting, easily manipulated publics.

- Information warfare attacks on the United States are presently deterred by the same policy that deters other types of attack. Acting under its rights as a sovereign state, the United States stands ready to respond to any attack on its interests with all appropriate means, including law enforcement as well as military capacity.

Background

At a recent Information Warfare (IW) and Deterrence workshop, participants focused on three principal issues:

- What do the terms "Information Warfare" and "Deterrence" mean and how are they related?

- How might IW attacks on the United States be deterred, if at all? For practical analysis, this issue was broken into "cyber-war attacks" on computers and infrastructure, and "media warfare" attacks.

- Can the United States use IW to deter attacks on itself, its allies, or its interests? Can U.S. actions be deterred by IW?

Key Concepts and Implications

On one level, information warfare (IW) and deterrence are well matched. Both belong to the world of robust ideas and have broad implications. Both are highly relevant to the post-Cold War era, in which conflict has been transformed from bipolar global competition 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 other levels, 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 actually is a narrow topic that only applies when a set of quite restrictive assumptions are met. (Deterrence was defined as "prevention or discouragement, by fear or doubt, from acting.") The relationship between the two concepts is spotty-highly relevant on some topics, marginally so on others, and not at all relevant in many areas.

The Domain of Information and Information Warfare

The term "information warfare" is used to mean many things, but is often focused on the military or cyber-war domains dominated by computers and communications infrastructure. 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, its analysis must be focused on selected elements, which must be clearly defined in each application. The field is so broad that virtually no meaningful generalizations can be drawn about it.

- Except in rare instances, isolation of military, national, public, and private information systems is all but impossible today. Very important military traffic is 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 could be potential targetsCbanking 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.

- The U.S. civilian sector is no longer a sanctuary that can be protected by interposing military forces between threats or adversaries and their targets. Traditional military forces can be bypassed at the speed of light by Information Age attacks on the general population or key economic systems.

- 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 organizations, and those of the commercial sector.

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 directed 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, nation-states are, at least in legal terms, equals and must act within the international system (diplomacy, warfare, etc.) to influence 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 most important insight arising from examination of the two concepts is the fact that they are only relevant to one another in highly selective contexts. The analogy that emerged at the workshop 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.

How Might IW Attacks on the United States Be Deterred?

Two aspects of this topic were analyzed: deterring attacks directed through computers and their connectivity (cyber-war attacks), and those directed at the general public through media such as television, radio, and print (media war).

Cyber-War Attacks.

Earlier ACTIS analysis of defen-sive information warfare differentiates attacks by their targets and implications and categorizes them as:

- Day-to-day or routine attacks with limited or diffuse impact on U.S. interests. These include electronic vandalism, hacking for profit, typical white collar crime, and other attacks with discrete impact.

- Potentially catastrophic attacks 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 not a threat to the U.S. banking system. However, an orchestrated and publicized series of successful attacks could undermine confidence in the banking system and create a much more serious problem, even though the individual attacks were each quite limited.

- Catastrophic attacks are those which, if successful, would in themselves do great harm to the United States. Long-term damage or destruction of critical control systems in key industries would

fall in this category.

Not all information warfare attacks on computer systems take the form of computer intrusion. Physical destruction of crucial telephone switching stations or other national information infrastructure assets would, themselves, be very damaging.

Workshop participants argued that a visible set of defenses is the beginning point for deterring attacks on important computer systems. Attacks are instrumental acts and will not occur if the attacking party perceives little opportunity for success.

Media War. Media War has the potential to influence public attitudes and support for U.S. military (and other) involvement. The thrust of the argument is that prudent, even essential, military actions can be called into question through an adversary's propaganda. Media warfare can put enormous time pressure on U.S. and allied decisionmaking, particularly when the adversary is an authoritarian state with little or no necessity for consultation.

- First, because of its democratic traditions and freedom of speech considerations, the United States is almost certainly going to be placed in a reactive mode if a sophisticated media 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.

- 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. The hardware requirements that give the National Command Authority a rich set of options for flexible responses should be reviewed and prioritized.

- 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. Incorporation of meaningful media attacks into appropriate military exercises is an important first step, but would be inadequate in itself over the long run.

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 is vast and too complex for simple solutions, the United States 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 United States stands ready to respond to any attack on its interests with all appropriate means, including law enforcement as well as military capacity.

Policy Issues

Notwithstanding the core conclusion, the workshop participants were strongly in favor of a specific, declared policy about United States response to IW attacks. This was considered essential if there was to be an effective deterrent effect. Further, policy was deemed necessary to provide guidance and direction to U.S. government agencies and to develop international cooperative agreements.

The workshop further agreed that information should be viewed as a separate element of national power because information and information age technologies are creating a cultural revolution and spawning changes in the behavior processes between nation-states and other entities such as international business. 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. While some basic policy statements have recently emerged, much more work is necessary.

Policy issues that need exploration and definition include:

- What is (what constitutes) an information attack?
- When is an information attack an act of war?
- How is an information attack verified?
- How is the attacker identified and confirmed?
- Does system penetration equate to an attack?
- Can one define an IW version of hostile intent?
- Are there potential tripwires?
- How should the United States respond?
- Who should respond for the United States?

Using Information Warfare to Deter Foreign Governments

The United States has the ability to conduct offensive IW within certain self-imposed limits. 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. Violations of sovereignty and acts of war are no less real because they use the information domain than if they involved more traditional violations. 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 the IW arena offers an exception to normal rules of behavior.

These limits having been noted, IW 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 deterrent effect.

Moreover, while barely unveiling the true potential of highly leveraged information and superior battlefield awareness, Operation Desert Storm has provided the world with a demonstration of the potential advantage of differential information capacities. Development of tools and techniques that can impact potential adversaries' knowledge of the battlefield, control of their own forces, resources necessary to support armed conflict, ability to deliver services to their populations, or level uncertainty about their own information, should continue.

About the Workshop

The workshop on Information Warfare and Deterrence was held at National Defense University as the sixth in a series exploring advanced command relationships and technologies. The topic arose from (1) issues that surfaced in earlier workshops; and (2) interests expressed by the Advanced Concepts, Technologies and Information Strategies (ACTIS) Directorate sponsors in the Joint Staff (J-6) and the Office of the Assistant Secretary of Defense for Command, Control, Communications and Intelligence (ASD/C3I). The workshop brought together senior analysts and technical experts, as well as active military leaders and action officers with operational responsibility in the affected areas. For additional information regarding the workshop, please contact the workshop chairman, Rear Admiral Gary Wheatley USN (Ret.), at (703) 893-6800 EXT. 24. Dr. Richard E. Hayes is President of Evidence Based Research, Inc. Trained as a political scientist, social psychologist, and a methodologist, he specializes in multi-disciplinary analyses of intelligence and national security issues. RADM Gary Wheatley USN (Ret.) is a former carrier aviator and Commanding Officer who presently specializes in advanced technologies and command and control.

|Return to Top | Return to Strategic Forum Index |Return to Research and Publications|

The Strategic Forum provides summaries of work by members and guests of the Institute for National Strategic Studies and the National Defense University faculty. These include reports of original research, synopses of seminars and conferences,the results of unclassified war games, and digests of remarks by distinguished speakers.

Editor in Chief - Hans Binnendijk

Editor - Jonathan W. Pierce

INTERNET DOCUMENT INFORMATION FORM

A . Report Title: Information Warfare and Deterrence

B. DATE Report Downloaded From the Internet: 09/27/01

C. Report's Point of Contact: (Name, Organization, Address, Office Symbol, & Ph #): **National Defense University Press**
Institute for National Strategic Studies
Washington, DC 20001

D. Currently Applicable Classification Level: Unclassified

E. Distribution Statement A: Approved for Public Release

F. The foregoing information was compiled and provided by:
DTIC-OCA, Initials: __VM__ **Preparation Date 09/27/01**

The foregoing information should exactly correspond to the Title, Report Number, and the Date on the accompanying report document. If there are mismatches, or other questions, contact the above OCA Representative for resolution.