Toward a Functional Model of Information Warfare

L. Scott Johnson

> **“But the simple fact that almost every writer on IW feels compelled to define it tells us that a clear concept has not yet crystallized.”**

Information Warfare (IW) is one of the hottest topics in current discussions of battlefield and geopolitical conflict. It has been addressed in writings, conferences, doctrine and plans, and military reorganizations, and it has been proposed as a fundamental element of 21st-century conflict. In a way, the IW situation is reminiscent of the concept of logistics as a military discipline, circa 1940:

- Elements of the concept had been known and used for millennia.
- The value of integrating those elements into a coherent discipline was just beginning to be recognized.
- The discipline was to become a central element of modern warfare—it is now said that “amateur generals [that is, Saddam Hussein] talk strategy, professional generals talk logistics.”

This comparison has another point of similarity: the interest in IW far outstrips the users’ understanding of the concept. Early in World War II, a senior US Army general said, “I don’t know what this ‘logistics’ is, but I want some.” Today, many people worldwide are saying the same about IW.

Searching for a Definition

This lack of a consistent and specific definition of IW is apparent throughout the literature. Col. Owen Jensen, USAF, discussing the evolution and use of the IW concept, says, “Although the Tofflers [Alvin and Heidi] have expounded on the origins of this type of warfare, no guru has yet established its principles.”[1] VAdm A. Cebrowski, director of C4 for the US Joint Staff, has said, “The services and various Pentagon agencies that must prepare for IW do not yet agree on what the concept encompasses.”[2] Almost every writing on IW makes a similar comment. Certainly, many definitions have been put forth; at the top level they sound much alike. But the simple fact that almost every writer on IW feels compelled to define it tells us that a clear concept has not yet crystallized.

Military writers discuss IW in terms of “information dominance” over an enemy, which is described as maintaining and applying a superior understanding of the battlefield situation.[3]

Strategic writers discuss IW as the next “paradigm” of modern warfare, and they quote military thinkers from Sun Tzu to Clausewitz and examples from Xenophon’s “March of the 10,000” to the Gulf war. The concept of information dominance is again raised, in a related but different sense, as a means to identify the enemy’s “centers of gravity” against which force can be most productively applied, while preventing an enemy from knowing one’s own critical points.[4]

Finally, there have been many discussions of IW attack and defense as related to telecommunications and computer networks, often but not always at the national level. The focus of these discussions is the

L. Scott Johnson works for Tera Research, Inc., a contractor performing analysis on behalf of the Directorate of Intelligence.

vulnerability of such networks to penetration, exploitation, and degradation; the magnification of these actions owing to a modern country's dependence on such networks; and the potential application of these actions in warfare, crises, international competition, and criminal activities.

These different points of view incorporate common elements, but a rigorous definition of the concept of IW has not yet evolved. Before we can identify and assess capabilities for IW and related activities, we need a definition, or a model, that is sufficiently concrete and specific to serve as a working aid.

A Starting Point

One can begin to derive a definition by asking why one should even bother with the concept of IW—is there any difference between IW and previous concepts of information attack? One might conclude, after a cursory review of some of the literature on the topic, that the concept of IW is in fact a rehash of existing concepts and techniques and that it adds little or no value. That conclusion, although understandable, would be incomplete.

Traditional forms of information attack, such as radar countermeasures, C3 countermeasures, computer intrusion, and psychological operations, typically:

- Consist of techniques, or measures and countermeasures.
- Have limited and local goals, and limited scope and orchestration (that is, being restricted to a specific combat operation).
- Perform a supporting role in combat activities.

These forms of attack tend to be used at the tactical level, and they require knowledge of the target's technical characteristics and operational procedures. In noncombat activities, these forms of attack typically are independent and isolated.

> **"IW truly is a form of comprehensive warfare, not merely a set of techniques"**

In contrast, IW truly is a form of comprehensive warfare, not merely a set of techniques. IW is differentiated from individual measures in that IW (like any other form of warfare) is governed by a strategy, which is focused on an objective. The strategy is a comprehensive plan for the use of IW-related weapons and tactics to attain the desired objective. The weapons and tactics may be *any* combination of military and nonmilitary techniques; the objective may be military, political, economic, or some combination thereof.

A unified IW campaign thus can be conducted alongside multiple concurrent or consecutive combat operations, can extend beyond the immediate battlefield, and can cross the boundaries between peacetime, crisis, and combat. The term "information" in IW suggests that the objective of such a campaign involves generation of effects on the adversary's information that will prevent or prompt certain actions, thereby creating an advantage for the attacker. (The objective of defensive IW involves prevention or counteraction of those effects.)

IW's Ultimate Target

Such an objective implies that the true target of an IW campaign is not the specific systems that are actually attacked, but rather the adversary's decision process. Thus, IW attack planning has to be based not only on the characteristics of those systems, but also on the desired higher order effects. This consequence can be illustrated by a simple example, a jamming attack on a sensor. As an individual electronic warfare (EW) operation, the attack is based largely on the sensor's technical and operational characteristics. As an element of an IW campaign, the planning and conduct of the attack has to be based on the way in which that sensor contributes to the adversary's situation picture and the information that the sensor provides on the attacker's forces and operations. An even higher level that has to be considered in the attack planning and implementation is the effect on the adversary's decisions of blocking, degrading, falsifying, or inserting the sensor information. The same requirement holds for attacks on communications systems, networks, links, and processing centers.

The overall concept of IW can thus be considered as having three parts: a set of IW elements (techniques and capabilities), a comprehensive strategy that applies and orchestrates them, and a target and objective. Only the elements are common to both IW and the earlier concepts of information attack.

A useful definition or model of IW therefore has to:

- Describe the ultimate target and objective.
- Identify and list the applicable elements of IW.
- Show how the elements can be combined in the strategy to attack the target.

Inasmuch as the target and objectives are the basis for designing an IW strategy, I will start with a "target model." Then I will describe the elements involved in IW. Finally, I will present a templating approach to organize the elements and their interrelations, so as to support analyses of IW strategy.

A Target Model

A generic model of the target of an IW operation is based on the abovementioned difference between IW and individual information attacks. Consider the previous example—a sensor is attacked in order to affect its contribution to the adversary's knowledge, thereby affecting the adversary's decision process. Thus, a three-layered target model is defined as:

- The **information systems** layer—the physical elements that generate, transfer, or store information. Attacks against information systems create **technical effects**.
- The **information-management** layer—the processes for handling and dissemination of information. At this layer, attacks create **functional effects**.
- The **decision-process** layer—the intellectual processes for interpreting and using information. At this layer, attacks create **operational effects**.

Effects at one level generate consequent effects at the higher levels. For example, a communications jamming attack on an information system creates blockage or corruption of the signal at a receiver (technical effect), which in turn reduces the information available from this channel (functional effect). One type of consequent operational effect would be decision delay.

One has to recognize, however, that this propagation of effects is not the only way to attack the decision layer, because attacks can be performed against *any* level. Although an attack ultimately comes down to a physical operation involving a physical information system, that system may be only a vehicle, not the target, of the attack. Thus, the attack may have little or no direct technical effect. In fact, an attack may have no functional effect either—it may create directly an operational effect on the decisionmaker. An example is a propaganda campaign wherein the information system being used is the local newspaper, the target is the decisionmaker, and the technical and functional effects are nil. Thus, attacks may have different immediate targets and effects, and not all effects propagate up from the basic information-system layer.

Some examples of different attack processes, and how they can be mapped against the model, are illustrated in Table 1 on the next page.

The point to remember is that the operational effects are the ultimate objective. Any attack has to create or contribute to the desired operational effect(s), either by itself or in combination with other attacks. Note that the propagation of effects may be complex and that not all IW attacks will create every type of effect. A given technical effect may generate widely different operational effects, depending on what is attacked and under what circumstances. Also, operational effects may depend on combinations of technical and functional effects. IW strategy has to account for these factors.

This model provides a framework for mapping and analyzing IW strategies and attacks. With the model, doctrine and capabilities for IW can be correlated. Intentions, doctrine, and plans usually start with the operational effects, whereas capabilities are usually described at the technical level. The layered model allows one to link the two and to find applicable capabilities that may be only indirectly related to IW. Directly related capabilities are usually apparent at the technical level. By looking at the functional level, additional capabilities that will have IW effects can be identified.

The Three Target Layers

Information systems layer. IW attacks, regardless of their ultimate objective, have to start with an information system, often but not always an electronic system. In many but not all cases, that system is the initial target of the attack, and technical effects are intended—receiver overload, data corruption, computer shutdown, data erasure, physical destruction, and so forth. This point is well recognized in the literature, and detailed discussions of IW capabilities often concentrate almost

Table 1
Use of the Target Model To Analyze Attack Processes
The initial effect, corresponding to the target layer, is highlighted.

Type of Attack	Target Layer	Technical Effect	Functional Effect	Operational Effect (examples)
Communications jamming	**Information system**	**Signal blockage**	Information loss	Delayed or wrong decision
Communications intrusion—short control message*	**Information management**	None—link continues to exist	**Information misrouting, self-generated overload (diagnostic, correction, repeat messages)**	Delay, confusion
Communications intrusion—short information message	**Decision process**	None—link continues to exist	Negligible—short message does not affect routing/handling/storage	**Delay, confusion, wrong decision**
Computer virus	**Information system**	**System paralysis**	Loss of data, loss of function at node	Delayed or wrong decision
Network worm	**Information management**	None—network links continue to exist and operate	**Delay or overload amounting to loss of function**	Delayed decisions; deliberate shutdown of unaffected nodes
PSYOPS/propaganda messages	**Decision process**	None	None	**Decision influence**
Military operation as PSYOPS maneuver	**Decision process**	None	None	**Perception manipulation**

* Many modern communications systems/protocols use machine control messages to establish links and route traffic. The control network may be separate from the information-carrying network. Examples are Signaling System 7 and computer-controlled adaptive HF systems.

exclusively on the technical attack methods and targets. What is not always recognized is the need for those effects to propagate through the target and create the desired operational effects, and those only. It is quite possible to conduct a technical attack that degrades or negates other elements of an IW operation.

Information management layer. Information management means information transfer, dissemination, storage, fusion, and conversion. These functions are performed by information systems, and they represent a logical layer overlaid on the physical information-systems layer. Examples of functional effects are a change in information transfer capacity, performance delays, and misrouting of traffic.

Information management is becoming increasingly important and vulnerable, because modern information systems are barely keeping pace with evolving formation-generation capabilities and information technologies. For example, data overload has come to be a serious problem in US military sensor and C3 nets. The US Navy encountered this problem in the Gulf war. Aegis systems and E-2/E-3 surveillance aircraft provided so much data that the flagship command center displays were overloading and locking up. As a result, it was necessary to reduce the original surveillance area (Red Sea-Iran-Turkey) to a region covering only southern Iraq, the Persian

Gulf, and part of Iran.[5] An enemy who takes note of this problem could develop measures to increase overload and exploit the lack of reserve capacity in US military information-management systems.

Civil systems are also becoming more vulnerable to this problem. The Internet "worm" of 1988 was an example of an overload attack. The worm was intrinsically harmless to the information systems—it did not destroy files or operating systems. Rather, it occupied the memory and resources of computers and virtually monopolized the network links among computers. The result was that many systems nationwide came to a grinding halt, and countless hours of effort were expended in diagnosis and recovery measures.[6]

Another increasingly serious military problem is information incompatibility. This problem represents another network vulnerability. It is caused by evolving requirements for joint operations, coupled with a huge increase in the number of communications and data systems that have stringent compatibility requirements. Traditional VHF voice radios working on standard channels could be used by anybody; Link 11 can be used only if the recipient has compatible equipment. Many articles have discussed this problem, often in connection with Desert Storm and the joint operations in the Mediterranean and Adriatic. As just one example, an attempt to pass imagery between the US Air Force and the Navy revealed 12 incompatible systems. The Navy ultimately solved compatibility problems in Desert Storm by providing equipment to selected other units. Other compatibility problems were solved by developing conversion

“The desired effects of IW attacks may be indirect—not just blinding or confusing the enemy, but shaping his perceptions, decisions, opinion, or behavior.”

systems and deploying them on selected platforms.[7]

An enemy could exploit this problem by identifying and targeting the critical nodes where data conversion is performed, or by taking advantage of the confusion via deception, confusion, or intrusion attacks. If information managers are accustomed to seeing unreadable data, they might not recognize the fact that some data have been garbled or corrupted, attributing the problems to the known inadequacies of their system. Thus, the IW planner has to understand an adversary's information-management processes and problems.

Decision process layer. The ultimate target of IW is the way in which information is used—that is, the decision process. The desired effects of IW attacks may be indirect—not just blinding or confusing the enemy, but shaping his perceptions, decisions, opinions, or behavior. The IW planner's understanding of the target has to extend to this layer, and knowledge of the adversary has to include his decision criteria, decision processes and time scales, and vulnerabilities. Many or most of the successful commanders and leaders throughout history had an intuitive understanding of their adversaries at this level; they often applied it in "IW-like" tactics, maneuvers, and psychological operations that confused, delayed, manipulated, or paralyzed the enemy.

The Elements of IW

The elements of IW extend beyond the techniques and capabilities for traditional forms of information attack. Taking a literal view of the term "warfare," the elements needed to perform IW are:

- Primary: Attack and defense capabilities and techniques.
- Supporting: Intelligence collection for targeting information—locations (which, for IW, may be physical or logical), strengths and vulnerabilities, and defenses.
- Supporting: Intelligence collection for battle damage assessment (BDA). Note that this concept is separate from the idea of conventional BDA information as a *target* of IW.
- Supporting: Intelligence collection for attack indications and warning (I&W).

The attack/defense capabilities and techniques are the primary functions of IW. As mentioned above, these capabilities currently exist under different guises—EW, computer intrusion and viruses, psychological operations, concealment and deception, firewalls and antivirus programs, encryption and spread-spectrum COMSEC techniques, and so forth.

Like traditional warfare, IW requires support from external sources. One is target intelligence collection, incorporating both prewar preparation ("strategic reconnaissance") and

operational targeting during IW activity ("tactical reconnaissance"). At the simplest level, this concept is obvious. An attacker needs to know the RFs of target communications links; the locations of sensors, communications nodes, and decision nodes; addresses, access protocols, and passwords for computer systems and networks; and so forth. The IW target model shows, however, that an attacker also has to know or discover how a candidate target system contributes to the adversary's situation picture and what information it provides on the attacker's forces and operations. Similar requirements exist at the decision-process level, relating to the decision criteria used by the adversary and to the effect on those decisions of blocking, degrading, falsifying, or inserting certain information.

IW therefore has to be supported by sensors for electronic intercept and monitoring, tools and access points for computer network probing and analysis, and reconnaissance to detect and locate C3 nodes. Again, these are pre-existing types of capabilities that may be applied in an IW strategy.

IW is like any other form of warfare in another respect—it has to be supported by a damage assessment function to be effective. The ability to measure IW effectiveness, however, is complicated. For example, even the effect of a direct attack on a communications node can be difficult to assess unless the attacker can tap a node or link elsewhere, or can exploit other elements of the communications net to assess the success of the attack (such as by monitoring requests for retransmission or traffic volume on return links). In this example, the attacker would be observing functional effects to diagnose technical effects. Higher level effects are even harder to assess, and some may be impossible to diagnose until the conflict is over and the adversary's records or memoirs can be examined.

Nevertheless, an IW strategy has to provide for intelligence collection and damage assessment, using typically the same elements that provide targeting data.

An IW capability also has to be supported by defensive intelligence elements, equivalent to I&W capabilities in traditional warfare. To use most defensive IW measures successfully, one has to detect, localize, and diagnose attacks on one's own information systems. The elements involved typically are detection/diagnostic tools embedded in or applied to one's potential target systems. Often, a detector may be merely a trained operator or analyst who can tell when jamming is occurring or when the pattern of incoming data is inconsistent or otherwise suspect. Technical measures include network analyzers, activity monitors, and signal analyzers. (One might also envision artificial-intelligence pattern recognition systems for data analysis and similar concepts.)

Two other key elements, which are related, cross over all these categories. These elements are expertise and understanding. Technical expertise and operational skills in the use of IW systems are necessary but not sufficient. An understanding of the target, whether a technical system, a network structure, an operational procedure, or a decisionmaker, and an understanding of how the target layers interact for the specific adversary and scenario of interest are necessary for the development of an effective IW strategy.

IW Orchestration

The orchestration of multiple IW elements is, again, one of the defining characteristics of IW. A combination of attacks is assembled and applied toward a specific objective. Military operations may involve IW campaigns designed to limit and control the enemy's knowledge of the situation and, ultimately, his ability to operate effectively. Nonmilitary IW also often involves orchestrated campaigns of multiple attacks—a political IW effort can involve PSYOPS, data denial, data insertion, cover and deception, and attacks on communications and computer systems. (A multipronged approach does not *always* apply, especially in technical attacks on computers and networks. In fact, these cases can be almost exactly opposite—a single attack generates multiple effects on multiple targets.)

To identify how the various IW elements can be combined and orchestrated, one can fall back on the target model. After dividing the target into layers, each layer can be broken down into its components. The next step is to list the attack actions that are possible against each component. Knowing the actions and the target characteristics, the capabilities needed to perform each attack against each component can be identified.

By combining the target model and the list of elements that resulted from consideration of IW as warfare, one arrives at a detailed list of required or relevant capabilities that can be used to guide data searches and analyses. This process justifies

Table 2
Template of Target Elements and Attack/Supporting Actions

Target Elements						Attack/Support Actions	
Logical				Physical			
Intelligence		Information		Nodes	Links		
Physical	Operation	Data	Control			Offensive	Support
• Location • Parameters • Function • Architecture • Network	• Users • Data flow • Msg timing	• Video • Text • Voice • Image • Digital	• Link setup messages • Common channel signaling	• Data sources • Relays • Fusion points • Processing points • Data storage • Data conversion •Interpretation/decision	• Comms • Data • Computer	• Block information • Corrupt information • Saturate node • Delay information • Insert information • Relay information • And so forth	• Obtain intelligence • Relay intelligence • Control attack • Use intelligence • Use information, • And so forth

each item on the list as being relevant to IW. Furthermore, the process automatically develops the position and role of each capability in the IW concept. Finally, the organization shows how the capabilities, attack techniques, and target elements interrelate, and it allows us to develop integrated and accurate descriptions of IW capabilities.

Table 2 shows a top-level view of this breakdown or template. In the table, connections between logical and physical target elements are not shown, and relations between attack/supporting actions and target elements are shown in words rather than as connections (for example, "relay information" and "relay intelligence" actually refer to one type of action applied to two target elements). A complete template can be developed that divides this structure into a set of tables and diagrams that show the relations explicitly.

The table does not show the lowest levels of detail. Other items can be added at the lowest (bulleted) level shown, and that is not the final level. It actually is another row in the hierarchy that can be subdivided into different types. The nodes and links clearly can be broken out further, and attack actions in particular are to be subdivided. For example, the "block information" action actually includes actions such as destroy source, destroy node, saturate node, and jam link, which can be further broken down to specific types of nodes and links and to specific types of information. The table also does not show defensive actions and their relations to the attack actions. A fully detailed template has a separate entry for each type of action and each type of target element.

In the table, the term "intelligence" refers to information describing elements of the target system. This information may be developed by the IW support activity, as by SIGINT measurements or network probes, or it may actually reside within the target system, alongside the user information. The latter case is exemplified by an Internet host that maintains a database of other hosts and users. It is this information that an IW attacker needs to develop or retrieve in order to focus the attack or assess the damage.

Note that there are two forms of such intelligence, physical and operational. Physical intelligence provides target parameters and structural or architectural information on target

networks. Operational information identifies users, data flow patterns, system status, and so forth. Both targeting and damage assessment need both types of intelligence.

The "information" category refers to the contents of the adversary's information systems, and it is divided into data (the actual information that the adversary eventually interprets) and control information that supports network operations. Sophisticated attacks on control information can be a serious threat to modern computer and communications nets. The "data" category is broken down by type, because the type of data usually defines the technical capabilities required for an attack. A complete template, however, also organizes data by the type of knowledge it represents (sensor data, situation data, own-force data) because this is what determines the functional and operational effects of attacking the data.

The attack actions include offensive measures and supporting measures, as shown in the table. The attack measures are not limited to blockage or degradation of information. One may insert false information into the adversary's information systems. One may also use (or misuse) information obtained from the adversary, as indicated by the entry "relay information." Passing on or publishing information that an adversary wants to conceal is a classic IW measure. The supporting measures may involve the target or may be self-contained within the IW system, such as return of collected information or command and control for the IW operation. The function "use information" refers to exploitation of collected information, and it is as important a function as denying information to the adversary. (There has always been the often painful tradeoff between jamming and listening.)

It should be noted that this template is an overall guide, not a rigid description. Not all IW systems or IW attacks will incorporate all elements of the template. What the template provides is a framework to guide the search and interpretation of relevant capabilities, and the evaluation of the completeness and sophistication of a country's IW capability or concept. For capabilities analyses, the template shows what capabilities to look for, what indirect capabilities might exist, and what supporting capabilities must be identified before a primary capability can be assessed as effective. For doctrine analysis, the template's presentation of relations and supporting elements is compared against the country's understanding of IW to evaluate the completeness and sophistication of their doctrine.

NOTES

1. Col. O. Jensen, "Information Warfare—Principles of Third-Wave War", *Air Power Journal*, winter 1994.
2. *Defense News*, 12-18 June 1995.
3. USAF position, quoted in *Aviation Week & Space Technology*, 10 October 1994.
4. J. Arquilla, "The Strategic Implications of Information Dominance", *Strategic Review*, summer 1994.
5. *US Naval Institute Proceedings*, May 1993.
6. W. Schwartau, *Hackers, Sniffers, Worms, and Demons*, book extract via the Internet.
7. *US Naval Institute Proceedings*, August 1992 and May 1993.