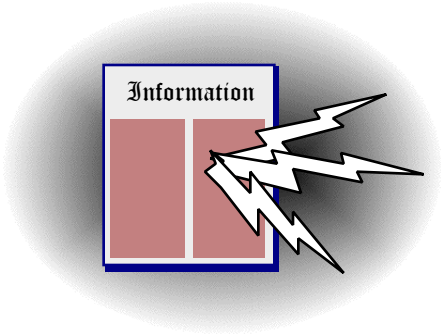
Information Warfare: a Consequence of the Information Revolution

MYRON L. CRAMER

ABSTRACT *Information Warfare is a consequence of the changes brought about by the Information Revolution. This paper distinguishes the older military terminology that is often associated with the term "Information Warfare" from concepts that are relevant to commerce. Within the Information Warfare model, an organization's information systems are viewed as a high leverage factor in the competitive process. To better understand this role, I describe Information Warfare in terms of five perspectives which may be thought of as the constituent elements of Information Warfare: information collection, protection, denial, management, and transport. For each element I examine its role in the competitive process.*

Introduction



This paper defines Information Warfare (IW), provides some historical background and context, and describes its applicability to business. An underlying element of the "Information Age" is that information carries more value than in previous periods of history. Information Warfare involves achieving and maintaining an information advantage over competitors or adversaries. Since competitive advantages can impact an organization's success or failure, it is important to understand the factors that affect this balance, and to understand the framework created by the new technologies and the new paradigms.

Background

Military Roots

The terminology of IW has its roots in military operations and many of its elements have been part of military doctrine for many centuries, including terms such as psychological operations, operations security, tactical deception, and electronic warfare.[1] But although the military drapes IW in the robes of the past, the modern concepts of IW are of recent evolution, born of the changes that have been driven by the new technologies. In current military doctrine, the information space or "infosphere" is considered the fifth battlespace together with land, sea, air, and space. The military considers this infosphere a "place" where primary battles may be fought and has actually issued a Field Manual on Information Operations.[2] Although there may be legal, regulatory, and ethical reasons for a business analogy not to exist, both anecdotal evidence and the results of a recent survey conducted by a Senate subcommitee indicate that the extent and seriousness of cybercrime is more than may be publically appreciated.[3]

Myron L. Cramer is at the Research Institute, Georgia Institute of Technology, Atlanta, GA 30332-0840, USA.

New Information Technologies

Much has been written about the Information Revolution and the societal impact that has been resulting from the increasing role of information and information systems in the endeavors of individuals, businesses, governments and non-governmental organizations. This revolution is built upon a framework of many individual elements, such as those listed in Table 1, which contribute to an aggregate effect that is highly synergistic in its effect on society, and which enables effects such as those described by futurists (e.g., Alvin Toffler[7]) and other researchers.

Table 1. New Information Technologies[9]

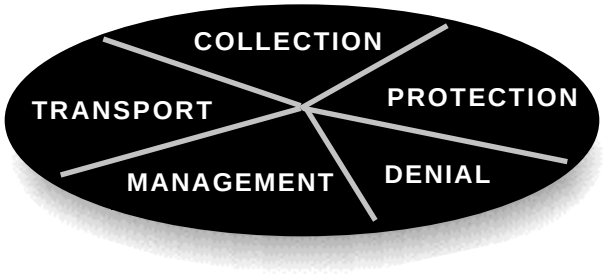
Computer-Aided Design	Fax Machines
Paperless Manufacturing	Scanners
Groupware	Pen Notebooks
Online Services	Flash Technology
Document Management	Advanced Fiber Optics
Customer Service Technology	Wireless Technology
Point-Of-Sale Terminals	Video-conferencing
Servers	Graphics Technology
Networks	Data Compression
Databases	Object Orientation
Printers	Virtual Reality
Voice Recognition	Geographic Systems
Storage Protection	

It is important to recognize that these new developments are only technologies, that of themselves are neither good nor bad; they can be used for great benefit, or can lead to disaster if used without consideration for their potential consequences. One key difference comes from an understanding of the commercial perspective of Information Warfare.

A Business Perspective

In this discussion, organizations are discussed generally; they can be any commercial business, government entity, or military unit that operates in any competitive or adversarial environment or scenario containing at least one opponent. With the increased value of information comes the need to approach it in new ways. Information Warfare has many aspects. To appreciate these it is important to discuss Information Warfare from several perspectives which may be thought of as the constituent elements; these are: *information collection, protection, denial, management, and transport.* Together, these define options, risks, and opportunities; how an organization chooses to implement and prioritize these elements is its Information Warfare strategy, which will impact its competitive position. This is illustrated in Figure 1.

Figure 1. Information Warfare Mix



Information Collection

An organization needs a variety of information to support is operations. These needs include planning its activities, executing its plans, monitoring its progress, and reporting its results. Information *collection* includes the entry points for information into an organization from both internal and external sources. Issues include quantity (completeness), quality (accuracy), and timeliness of this information. Business examples of collection systems include point-of-sale (POS) systems, market surveys, government statistics, and internal management data. Military examples of collection systems include tactical radars and other sensors.

The increased reliance on information has resulted in an increasing appetite for data and new collection systems. By example, grocery stores introduced automated scanners to speed up the check-out process and improve its accuracy. Then they issued customers "discount and check-cashing cards" that allowed them to correlate customers with their purchasing habits.

Information Protection

Once information is collected by an organization, the next logical consideration is how to protect it. The vulnerability of the "Information Infrastructure" is widely discussed and publicized and is one important aspect of protection. *Information protection* addresses two types of threats: information *compromise* and *destruction.* Compromise involves a competitor gaining access to an organization's proprietary data. Destruction involves the loss of these data (or loss of access to these data) as the result of mismanagement, accident, or a hostile attack by an adversary.

Information Compromise. An organization's information includes items that may have a high value to a competitor. Examples include future plans, product technical data, customer lists, personnel files, and financial records. This type of data needs to be protected from disclosure to competitors by controlling how, where, by whom, and when it is generated, stored, or accessed. The specific data being protected in these ways are often identified in some distinguishing manner and labeled as proprietary, sensitive, or classified. In some cases, formal control systems are established to encourage the desired behavior among employees. An often over-looked area involves the protection of non-proprietary data of a seemingly harmless nature. These data, when combined with other information available to a competitor may become important. For example the travel schedules of key executives may be a tip-off of pending business activities such as mergers or new customers. Protecting information of this nature is sometimes referred to as *operations security*. An internal organization chart or phone directory can be valuable to an adversary's recruiters in identifying and contacting key staff. These people will bring with them their knowledge of ongoing programs, products, and customer contacts.

Information Destruction. With the increasing use of collection systems have come new opportunities for information attacks by adversaries for either purposes of compromise or destruction. The adversary's purposes in making these attacks may include obtaining competition-sensitive information or hindering (sabotaging) an organization's operations. In the fast-paced and global economy of the Information Age, organizations may resort to actions and methods that would be considered improper, unethical, or illegal in previous generations. The new information system technologies actually encourage this behavior by lowering the technical threshold to be crossed to a level available to virtually anyone with a personal computer and a telephone. The level of automation is such that intrusions are difficult to detect or trace, tempting the perpetrator with a low likelihood of being caught and large rewards for success.

Information Denial

Information denial includes measures *beyond normal protection* to specifically target an adversary's collection systems. There are two types of denial: *direct attacks* on the adversary's information systems, and *providing misinformation* to its systems to deceive and induce the adversary to take actions that are not to its advantage.

Direct Attacks. For the military, direct attacks include *electronic warfare* (jamming) of sensors and radio links. In business, analogous forms of direct attack are possible to attack the *integrity* or *availability* of a competitors systems. Through the Internet, all of an organization's networked computers are connected by high speed links not only to each other, but also to every competitor around the world. Through standard Internet protocols such as the file transfer protocol, "FTP," the entire contents of a computer can be copied or replaced within minutes. Integrity attacks include introduction of corruption into data or software so that the targeted competitor will not be using the information or processes it expects. Availability attacks include many methods of interfering with the normal operation of a competitor's networked systems so that they will not be operational when the competitor needs them. Direct attacks on an adversary's computer networks are a highly risky and usually illegal activity; nevertheless, the current state of the Internet makes attacks difficult to trace and international intrusions difficult to prosecute. Since direct attacks are an element of Information Warfare that an adversary may choose to employ as part of its strategy, they must be considered in formulating strategy and in planning protection.[4,5,7,8]

Misinformation. Besides direct attacks, there are safer ways to corrupt an adversary's data bases. These rely on providing false information to the targeted competitor's collection systems to induce this organization to make bad decisions based upon this faulty information. Consider the "vaporware" example in which a software developer, Company A, gets information about a new product being developed by a competitor, Company B. Although it has no comparable product in development itself, Company A issues a press release describing its own "superior" (but fictional) product. In response to Company A's press announcement, Company B thinks that it has lost its market lead and puts its development efforts elsewhere. Even after Company B brings the real product to market, its lead can be effectively lost when potential customers postpone their purchases waiting for the fictitious product from Company A. It is the author's observation that this example may have become commonplace in today's software market. The military versions of this type of denial operation include tactical deception and psychological operations (PSYOP). In all of these cases, the true situation is concealed, while evidence is generated and made available of a fictional reality. In the Information Age, we can expect these

practices to become increasingly commonplace. Organizations need to protect themselves from these practices by anticipating them and by controlling the quality of their information sources. They also need to be ready to respond quickly to counter an adversary's misinformation. Company B would have done this in the vaporware example cited by issuing its own press release about the inferiority and immaturity of Company A's imitation product, or with money-back guarantees to purchasers of its product.

Information Management

An important element of Information Warfare is *information management.* This is evolving as a new discipline since it involves combinations of computer science and management. The underlying concept is that with the increasing value of information in business, a competitive advantage can result from improved management of this resource. There are many aspects to this element including the selection and introduction of information technologies and the methods for controlling data within information systems. We have seen the transition to distributed computing through increased use of personal computers in business. This has resulted in a decentralization of computing and data resources within organizations and the loss of central control. This creates many issues for corporate data managers, including questions of "Where is the data?", "Who has it?", and "Which version is the most current?" Other issues include deciding which data to retain (archive) for future reference, and how to store these archived data so that they will be readable by future systems. As an organization's intellectual property exists increasingly in electronic forms, it is harder to manage using traditional methods (such as paper records) and may be more easily misplaced, lost or discarded. Automated solutions are important elements.

Information Transport

An essential element of Information Warfare is *information transport.* Transport involves moving data from points of collection to points of storage or use. The speed with which this is done affects the timeliness of the data availability and therefore the responsiveness of the organization to situations. Since this responsiveness can be a big factor in the competitive process, the speed and efficiency of an organization's transport capabilities can be an important factor in the organization's survival or failure. An example is an organization's ability to use Internet e-mail to provide time-critical bids or proposals to a customer and thus beat competitors whose express delivery packages may still be en route. Competitive transport systems must be fast, reliable, and controlled. Transport considerations must be viewed within the overall Information Warfare perspective, since the same efficiency that facilitates rapid message and data transportation also may be used by a competitor to download proprietary data bases in seconds or minutes.

Information Warfare Strategies

An Information Warfare Strategy is an organization's relative mix of efforts among the five elements (information collection, protection, denial, management, and transport); this balance, whether explicitly selected or the result of separate investment and operational decisions affects the organization's competitive posture. Significant factors include market opportunities, likely competitor actions, and current competitive situation.

Postures

Incorporating Information Warfare into operational missions involves many choices. These choices are driven by competitiveness consideration. The aggressiveness shown by competitors in collecting information will affect the need for protection and denial. There are many possible postures an organization can take, each of which reflects the results of different attitudes toward the Information War. I illustrate these differences by considering five extreme positions where a single Information Warfare element is dominant.

Defensive. A heavily defensive posture is characterized by an emphasis on *information protection* including significant access-control and limited external system interconnections. This posture might be appropriate for a dominant market leader or an organization that benefits from the status quo. This strategy will have advantages in an environment containing emerging adversaries who are pursuing strategies to attack the leader or to change the current situation.

Offensive. The offensive posture is characterized by an emphasis on *information denial* including attacks on the market leader. This posture might be taken by organizations that are dissatisfied by their current standing and who may be desperate to take down their stronger adversaries.

Quantity. The quantity posture is characterized by an emphasis on supreme *information transport* capability. An organization adopting this posture places its confidence in its ability to move and use massive amounts of information over large well-established infrastructure. It depends upon the sheer volume and timeliness of its data to make attacks impractical. This posture will work best when the value of the organization's information is widely distributed and is of low sensitivity.

Quality. The quality posture is characterized by an emphasis on *information management.* A practitioner of this posture gains its advantage by its ability to manage its information needs better than its competitors. Compared with these competitors, its investments may be more modest, but they are wisely made. It makes better use of less information, and optimizes its use of modest protection. This posture may have advantages in a highly competitive, cost-sensitive market.

Sponge. The sponge posture is characterized by an emphasis on *information collection* and an insatiable thirst for large amounts of information. Practitioners of this posture may have adopted a follower strategy in which they quickly bring products to market based upon the innovations of others. They gain their competitive advantage by saving in research and product development. To avoid being left behind, they must monitor the activities of other more innovative adversaries and survey market responses so that once they can decide to follow a given initiative, they an quickly catch up in the marketplace using their previous market presence.

Game Theory

A more scientific treatment of strategy analysis is possible through Game Theory. In a competitive environment, the optimum strategy may depend on what the competition is doing, as is illustrated in Table 2.

Table 2. Game Theory Option Matrix

		Player A		
	Benefit/ Cost	Option 1	Option 2	Option 3
Player B	Option 1	0	High	Low
	Option 2	High	0	High
	Option 3	Low	High	0

In this example, Options 1, 2, and 3 are progressively more expensive in terms of capital investment in information system technologies. Each option provides a relative market share benefit over a competitor investing less.

Summary

In this paper I examined Information Warfare as a consequence of the changes brought about by the Information Revolution. This consequence positions an organization's information systems as a high leverage element in the competitive process. To better understand this role, I discussed five perspectives of Information Warfare: *information collection, protection, denial, management, and transport*. From each perspective I examined its role in the competitive process, and discussed concepts for designing a balanced information warfare strategy.

References

1. Alan D. Campen, The First Information War: The Story of Communications, *Computers, and Intelligence Systems in the Persian Gulf War; an Anthology of Studies of Communications in the Gulf War*, 1992.
2. Department of the Army, *Information Operations, FM 100-6*, 1996
3. WarRoom Research, *Safeguarding Corporate America and the National Information Infrastructure*, report for the President's Infrastructure Protection Task Force and the Federal Bureau of Investigation, January, 1997
4. National Research Council's System Security Committee, *Computers at Risk: Safe Computing in the Information Age; an unemotional examination of the threat and our vulnerabilities.*
5. Winn Schwartau, *Information Warfare: Chaos on the Electronic Superhighway*, ISBN 1-56025-088-7 First Edition, Thunders Mouth Press, 1994
6. Clifford Stoll, *The Cuckoo's Egg: Tracking a Spy through the Maze of Computer Espionage*, Doubleday, 1989.
7. Alvin Toffler, *Future Shock*, Random House, New York, 1970
8. U.S. General Accounting Office, *Economic Espionage: The Threat to US Industry*, GAO/T-OSI-92-6, 1992
9. *U.S. News & World Report*, "The New Information Technologies," May 2, 1994