Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

The Future of Information Warfare

The present war against terrorism, precipitated by the decidedly low-tech use of airplanes on September 11, is raising the awareness of corporations and individuals in regards to the security of business and personal information. The attacks of September 11th showed what happens when the information flow of our society is disrupted. Many realize now that disruption of the exchange of business and personal information could be a primary weapon of attackers, and not just the secondary effect of other actions.

Copyright SANS Institute
Author Retains Full Rights

AD

The Future of Information Warfare
Carter Gilmer
GSEC Practical Assignment Version 1.2f

Military Description of Information Warfare

The present war against terrorism, precipitated by the decidedly low-tech use of airplanes on September 11, is raising the awareness of corporations and individuals in regards to the security of business and personal information. The attacks of September 11th showed what happens when the information flow of our society is disrupted. Many realize now that disruption of the exchange of business and personal information could be a primary weapon of attackers, and not just the secondary effect of other actions.

The idea of warfare using information as a weapon is not new. The obvious place to start getting a handle on the definition of information warfare is the military:

> **information warfare** – Information operations conducted during time of crisis of conflict to achieve or promote specific objectives over a specific adversary or adversaries. [Dept. of Defense, p.209]
>
> **information operations** – Actions taken to affect adversary information and information systems while defending one's own information and information systems. [Dept. of Defense, p.209]

These definitions are rather bland and general, to be sure. The military's focus on information historically has been its use in aiding the destructive capabilities of conventional weapons. The nightly news showed us the abilities of computer guided missiles during the Gulf War, and even the foot soldier has computer-aided gear such as weapon-sighting systems.

The Many Facets of Information War

Warfare has historically been the domain of nation-states, or at least groups of displaced people fighting an oppressive government. Now, both small, loosely organized groups and individuals can (and are) conduct information warfare on a vast array of targets.

The critical point to remember when reviewing the military's treatment of information as a weapon is that IW is much more than using information to aid conventional destruction. Warfare has lost its material nature, and information has become an end in itself. As governments, businesses, and individuals become increasingly reliant on data storage and movement, the potential for serious economic harm resides in the information itself.

As the economic value shifts out of material goods and into the information itself, the means of attacking also shifts. Simply destroying the infrastructure used to store and transmit data has an effect on our ability to immediately use the information the data represents. For sure, the physical devastation experienced at the World Trade Center destroyed many repositories of information and the mechanisms used to access said information. Yet, this crude attack did not

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

destroy that information totally. For example, using an extensive system of backups, the New York Board of Trade resumed commodities trading less than one week after the attacks; one of the directors boasted that they could have resumed trading that very same day! [Gibson, p.1]

For maximum effectiveness, then, information warfare will come to be characterized by methods designed to corrupt or misuse the information itself. The next section develops a hierarchy of attack methods used for IW. Then, the current situation is assessed and the future trends examined. The defenses necessary for the future are discussed, and the paper concludes with some points on the changing philosophy of warfare.

Hierarchy of Attacks

As information becomes an end in itself for attacks, there are several species of attack possible. The following diagram shows a hierarchy of methods used in an information war, along with the associated skill level required on the part of the attacker, and the possible direct economic benefits to the attacker.

Profits	Method	Skill
Low	Destroy Records	Easiest
↓	↓	↓
	Disrupt Service	
	↓	
High	Illicit Use of Info	Hardest

Merely destroying information is the most basic form of attack in information warfare. Physical destruction can be included in this category, along with worms, viruses, Trojan horses, etc. designed to simply delete data. Even more obscure weapons such as High Energy Radio Frequency (HERF) guns and nano-machines fall into this first category. The aggressor that uses such methods never actually obtains the information being destroyed. Obviously, the attacker cannot use the information for personal gain. Viruses and related ilk do not need to be very sophisticated when the sole purpose is destruction.

Moving to the idea of disruption of service, the skill required increases, as does the potential economic benefit. An attacker may be able to develop more complex forms of the software weapons mentioned above that target only certain software programs or hardware devices. The entity under attack may not be able to simply resort to using backup data or hardware, as those may also come under the same attack, rendering them useless. The attacker may be just a group of hackers testing their skills; in such case, economic gain probably would not be an incentive. Imagine, however, governments or corporations designing software weapons that only harm a rival's equipment or programs. The aggressor would remain functional while the victim loses clients or suffers an international crisis.

The pinnacle of information warfare is the illicit use of information. Instead of destroying data, or denying others access to the data, the attacker obtains from and/or modifies information about the victim. There are numerous scenarios here, all of which could potentially be quite lucrative to an attacker. Such examples range from a lone attacker assuming the identity of someone else

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

to corporations obtaining inside data about their competitors to governments shutting down the economic system of an enemy. The more specific the information is, the more difficult it will be for an attacker to interpret the information out of context. Also, while it is easy to simply destroy data or services, to actually retrieve information leaves trails behind which give away the operations of the attacker. These trails can be erased, of course, but is more time-consuming and difficult—meaning there are more chances for an attacker to slip up when trying to retrieve information for subsequent use.

Current Focus

The focus in current attacks remains mainly at the easiest two levels in the above hierarchy. Both the complexity of current commercial off-the-shelf (COTS) applications, and the sheer number of products mean there are many, many more holes available for an attacker to use. Statistics from CERT/CC show that the number of reported vulnerabilities has risen from 171 in 1995 to 1,820 in the first three quarters of 2001. [CERT, p.1] As expected with the increase in vulnerabilities, the number of incidents has also increased. CERT/CC reported just 132 incidents in 1989, but has already reported 34,754 incidents in Q1-Q3 of 2001. [CERT, p.1] These attacks extend beyond the commercial sector, too. In 1996, the GAO estimated that Department of Defense computer systems were attacked 250,000 times per year, and that only one out of every 500 attacks was detected. [GAO, p.1]

We are experiencing a situation where systems have become so complex that software and hardware vendors must run the infamous "Red Queen's race," where they must constantly keep refining their products just to stay even with the advances made in attack methods. For example, when denial of service (DoS) attacks first appeared, the attack technology was spread to involved computers manually. Now, attackers have placed the attack tools as part of the payload of a virus or worm. Automated propagation of DoS tools enables people or groups with less initial resources to launch attacks. Surprisingly, this automatic deployment became a DoS attack *itself* in the Code Red/Nimda events!

Many of the information warfare attacks that are publicized appear to be the efforts of individuals or small groups; as mentioned previously, information warfare is an especially attractive offensive option for less empowered people. That IW is increasingly characterized by terrorist-like methods has been exacerbated by the growth in the use of technology, the Internet in particular. The large and costly disruptions of a DoS attack come for a small price in equipment and supplies, and, as the number of Internet connections grows, the difficulty of orchestrating such an attack decreases. It is almost ironic that those who are the heaviest users of advanced information technology are also the most susceptible to information warfare attacks. The distributed nature of the Internet allows attacks to come from nearly anywhere, and those individuals/corporations/governments with the most reliance on networking present the largest target. Of course, firewalls and intranets may reduce the exposure of the most critical systems of one entity to intrusion, but denial of service attacks mean that even the most fortified system may be affected because of the lack of security elsewhere in the world. Furthermore, remember that "netwar," war over the Internet, is only one choice for an information warfare attack. Those entities with large amounts of stored information still must contend with those who might destroy or steal that information through more conventional means.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Three Types of IW

At this point, the reader is starting to get the idea that information warfare certainly includes the familiar offensive techniques used for years (e.g., bombing a data center), but extends to include a much larger set of actions that apply at several different levels in our society. The author Winn Schwartau approached information warfare by dividing it into three categories: personal, corporate, and global. [Schwartau, p.17] The main concern in each of these levels, respectively, is privacy, espionage, and terrorism. These categories highlight the third, and most problematic stage of IW, the usage and misappropriation of information. For an attacker at each one of these levels, stealing a personal identity, a corporate plan, or a national security secret would be immensely more profitable than just destroying that information. Writing in 1994, Schwartau stated that information warfare costs the United States up to $300 billion per year. [Schwartau, p.16] Even this old figure shows the magnitude of information war's impact, especially when one considers the amazing growth the computer sector has experienced since 1994.

The takeaway thought from this is that in order to meet the challenge of information war attacks, we must think in a different manner. Although we have many military-sounding terms with "war" in them, the highly structured organization and philosophy of the military is not going to be able to deal with these new threats adequately. Information is the thing we want to protect, but it has no material nature or location. Not only is information the object of attacks, but it can also be the means of attack. The possible economic destruction from an IW attack shows that nebulous enemies can damage any nation's total security; the military may not be able to defend the nation's infrastructure or even strike back if the attackers are distributed worldwide.

Therefore, in preparing for the future in which acts of information warfare are certain to continue and grow more significant, there are certain preparations needed on each of the three levels.

Distribution of Resources is Beneficial

In the discussion so far, distribution of resources has turned out to be a double-edged sword. The New York Board of Trade found that distributing its information (data backups) geographically saved it from business failure on September 11th. Yet, the distributed nature of the Internet allows attackers to cloak their true locations and identities, foiling law enforcement efforts. So what is the best policy? The answer is best illuminated in an analogy concerning the games chess and Go. Chess starts with equal opposing armies and the pieces move according to assigned ability toward the one goal of capturing the opposing king. Both sides start at full strength, and usual strategy emphasizes moving and capturing pieces in such a way to control the center of the board. Go, on the other hand, starts with an empty board, and all pieces ("stones") have equal significance. Once placed, a stone is only moved when opposing stones surround it. The object for the player is to use linkages between the stones to surround territory on the board. Go emphasizes building networks of power, and the sides and corners of the board can often be more important than the center. [Arquilla, p.16]

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Go's emphasis on networking is much more like the current world of computer systems. Power is distributed across many locations in both information warfare and Go. To effectively handle the distributed threats of infowar, individuals/corporations/governments cannot responds as if playing chess, with the linear development of weapons of varying power. Just as there is no king in Go, information warriors do not have a central location of power. The best way to respond to threats from a networked enemy is to use the network's properties to gain equal standing. Centrally located sources of information (conglomerated power) are doomed to fail against a distributed enemy.

Defenses against IW

The networked world turns out to a blessing and curse; only by wholly embracing the ideas of networking information can various entities reap the benefits of networking and still respond effectively to the unique threats of information warfare. Still, talking generally about reducing centralized locations of power does not give a specific idea of what can be done in the future to meet the ongoing threats of information warfare. David Brin, writing about privacy in our society, made note of the problems networking causes and the necessary changes in society's structure to handle the new threats. He gives numerous action points:

1) Pursue research to create mapping programs that find points of vulnerability in the Internet.
2) Increase development of encryption based validation and verification systems.
3) Insist that organizations with vital records have a distributed backup system.
4) Use teams of security testers (hackers) both inside and outside of organizations to test vulnerabilities.
5) Encourage society to distribute locations of services and expertise, so that critical services can absorb local damage similar to the way the Internet routes around outages.
6) Reduce the reliance on hierarchical power structures, with the accompanying levels of secrets. [Brin, p.318]

This last point is the most radical change, and will be the most difficult to implement. A huge percentage of governments and corporations still operate on the pyramidal power structure, where power and authority flow from the top down. There have some widely publicized attempts in corporations to "flatten" the power structure, but the newsworthiness and novelty of such attempts indicates that this is still not the prevalent approach. The entire branch of the military is hierarchical in nature; this is the root of the military's ultimate ineffectiveness in dealing with a networked threat.

A perfect example of networked organization succeeding where hierarchical organization failed is seen in the Napster and Gnutella file-sharing services. Napster used centralized servers to enable the free sharing of files (mostly digitized music), which raised the question of copyright infringements. Due to the political and economic power of the recording industry, these central servers were shut down for a period of time, ending the file swapping. Gnutella achieves the same end (file sharing), but does so without any centralized servers coordinating the activity--

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

everything is done via the network. The same questions of illegality still exist, but there is no one location that can be shut down to prevent the file swapping from occurring, and thus, it continues briskly.

Note that I have not listed any specific programs, virus detectors, firewalls, and etcetera that can help stop the economic loss resulting from information warfare activity. Certainly, all of these will be useful and necessary to protect users at all three levels from information warfare. The point is, any specific software applications or hardware devices will need to be constantly updated to meet new threats; to list them specifically here is to be out of date almost immediately. The critical changes needed are in the manner in which we treat, store, and exchange information. The existence of networks, and our increasing reliance on their use, means that we need a more fundamental change.

Paradigm Shift Necessary

The general security structure that has been built (at least in the United States) is one that focuses on the means of conflict much more than the objective of conflict. Think about it: we naturally assume that secrets should be kept secrets, and most of the energy in computer system security is spent on firewalls, virus scanners, et al. John Rothrock, writing in an essay on trust and security in the context of information warfare, points out that fully dealing with IW may mean changes in how we as a society understand and deal with conflict itself. He asks the question, do we as a society want to make the shifts necessary to control information securely? [Rothrock, p.223]

Rothrock goes on to note that IW means that our society must be able to act in three interdependent arenas: (1) offensive action against the enemy's information capabilities; (2) defensive protection of our own information capabilities; and (3) capabilities to *use* information more effectively than our enemies. [Rothrock, p.225] He points out that this means often times responding to attacks from those with far less advanced information structures, with the attending problems (e.g., the current action in Afghanistan). The military has long focused primarily on the offensive arena, using hierarchical secrecy to deal with the second sphere. Rothrock wonders how the typical response of hierarchical secrecy will mesh with the openness and convenience that everyone has come to enjoy in the networked world.

Rothrock's points about change are useful, but they seem to again focus too much on the military power structure. IW is a problem of national security, but it is also a problem of personal and corporate security as well. In our current mode of thought, the chase has been toward a means of creating and verifying secrecy. Yet, there has been a general groundswell in the West against the veil of secrecy in corporations and government, which seems to answer Rothrock's above question negatively.

David Brin suggests that using secrecy is counterproductive, since it by nature creates vulnerabilities in our information infrastructure on which information warriors focus. Brin's solution is to start a movement away from secrecy toward what he calls a "transparent society," where cash flow and secret ledgers are open for all to see. [Brin, p. 321] Our society will probably definitely become more open as network organization begins to replace hierarchical organization, but Brin's solution is not so easily implemented. Just as the populace loathes

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

secrecy in governments, the people are clamoring for more privacy in their personal lives. Shifting secrecy to the personal sphere will only make that sphere the lucrative one for information warriors. As a society, we will ultimately decide the balance between openness and privacy, between convenience and security, knowing that the decisions made for each of Schwartau's spheres synergistically affects the other spheres.

List of References

Arquilla, J., and Ronfeldt, D. "Information, power, and grand strategy: In Athena's camp." In Athena's camp: Preparing for conflict in the information age. RAND. Santa Monica, CA. 1997.

Blyth, T. "Cyberterrorism and private corporations: New threat models and risk management implications." <http://www.terrorism.com/documents/iw-privatrisk.pdf>.

Brin, D. The transparent society: Will technology force us to choose between privacy and freedom? Addison-Wesley, Reading, Massachusetts. 1998.

CERT Coordination Center. "CERT/CC statistics 1988-2001." http://www.cert.org/stats/. November 27, 2001.

Department of Defense Dictionary of Military and Associated Terms. Joint Pub 1-02. http://www.dtic.mil/doctrine/jel/new_pubs/jp1_02.pdf. April 12, 2001.

GAO Report. "Information security: Computer attacks at Department of Defense pose increasing risks." http://www.us.net/softwar/gao.html. May 22, 1996.

Georgetown Essays on Information Warfare, edited by Denning, D.E. < http://www.cs.georgetown.edu/~denning/infosec/iw-essays/>. Vol. 1, Spring 1999.

Gibson, Stan. "Lessons learned speed WTC recovery." ZDNet News. http://www.zdnet.com/zdnn/stories/news/0,4586,2813977,00.html. September 21, 2001.

Haeni, R. E. "Information warfare: An introduction." http://www.guest.seas.gwu.edu/~reto/infowar/info-war.html. January 1997.

Harreld, H., and Fonesca, B. "Guarding against cyberterrorism." http://www.infoworld.com/articles/fe/xml/01/10/22/011022fealert.xml. October 22, 2001.

Houle, K. J., and Weaver, G. M. "Trends in Denial of Service attack technology." http://www.cert.org/archive/pdf/DoS_trends.pdf. October 2001.

Information Warfare Research Center. http://www.informatik.umu.se/~rwhit/IW.html. November 2001.

Information Warfare Site. http://www.iwar.org.uk/. December 2001.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Insititute for the Advanced Study of Information Warfare. http://www.psycom.net/iwar.1.html. December 2, 2001.

Rothrock, J. "Information warfare: Time for some constructive skepticism?" In Athena's camp: Preparing for conflict in the information age. RAND, Santa Monica, CA. 1997.

Schwartau, W. Information warfare: Chaos on the electronic superhighway. Thunder's Mouth Press, New York. 1994.

Whittaker, R. Information Warfare. < http://www.informatik.umu.se/~rwhit/IW.html>. May 1998.

© SANS Institute 2001, Author retains full rights

Last Updated: May 22nd, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	**Cyberjaya, MY**	**Jun 03, 2013 - Jun 08, 2013**	**Live Event**
SANS Pen Test Berlin 2013	**Berlin, DE**	**Jun 03, 2013 - Jun 08, 2013**	**Live Event**
Industial Control Systems Security Training - Houston	**Houston, TXUS**	**Jun 10, 2013 - Jun 15, 2013**	**Live Event**
Security Impact of IPv6 Summit 2013	**Washington, DCUS**	**Jun 14, 2013 - Jun 16, 2013**	**Live Event**
SANSFIRE 2013	**Washington, DCUS**	**Jun 14, 2013 - Jun 22, 2013**	**Live Event**
SANS Canberra 2013	**Canberra, AU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
Mobile Device Security Summit 2013	**OnlineCAUS**	**May 30, 2013 - Jun 06, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**