Information Assurance: Structure From the Fog,

A Dynamic Information Defense Solution in a Dynamic World

1Lt Antoine C. McNeal, USAF

Introduction

Information-in-War has always been a critical component in warfare, capable of enabling militaries to increase operational efficiency. In the last decade and a half, information systems have become heavily relied upon to augment and even transform military capabilities.[1] The foundation of today's military paradigm rests in the singular belief that militaries that are able to gain Information Superiority through control of the Information Domain (ID) will achieve strategic advantage over their adversaries.[2] Bruce Berkowitz, a research fellow at the Hoover Institution at Stanford University and senior analyst at RAND espouses that "the ability to collect, communicate, and protect information is the most important factor defining military power. In the past, armor, firepower, and mobility defined military power, but now it often matters less how fast you can move or how much destructive force you can apply. Stealth trumps armor, precision trumps explosive force, and being able to react faster than your opponent trumps speed."[3] Ultimately a unit's reaction is based on their preparedness, which is a product of information systems.

Upon realizing the power of information systems, militaries scrambled to upgrade antiquated systems and launch new programs. Regrettably, this innovation occurred with little regard for defensive measures. Although, in recent years Information Assurance (IA) awareness led to monumental advances in doctrine and policy, a void still exists and more progress must be made. Information Assurance is defined as, "[i]nformation operations that protect and defend information and information systems by ensuring their availability, integrity, authenticity, confidentiality, and non-repudiation."[4] Ultimately, the introduction of IA has provided some clarity and resulted in the institution of some isolated defensive programs, but despite efforts, there is still much ambiguity on how to defend the Information Domain and on what level. This confusion drives the need for an integrated, cohesive, and clear Information Defense Architecture (IDA) that serves as a universal maxim for defensive posturing in the Information Domain.

Information defense is often perceived as a critical tradeoff between security and usability; this suggests system security enhancements will result in a decrease in effectiveness. For example, a system owner may decide to isolate his/her system to decrease vulnerabilities and enhance the system's security posture. Although, isolation is an option available to system owners, it is not viable considering the high demand for system intercommunication in the twenty first century. Such a strategy is plausible as a last resort, but not feasible for systems that ensure critical combat capabilities. Therefore the aim in the Information Domain is to create dynamic defensive information architecture to mitigate vulnerabilities, provide redundancy, and enhance mission capabilities by ensuring information availability. The approach for presenting the method for attaining Information Assurance in the Information Domain is to first define the problem and need for an information defense solution, then present a basic understanding of the Information Domain, followed by an exploration of the proposed IDA.

Defining the Problem and Need for an Information Defense Solution

The Current Status

To frame the discussion of security in the ID, it is important to identify problematic areas that are in need of improvement.

Centralized Control and the Slow Propagation of Information: A centralized control hierarchal structure, in a time critical environment, can blind systems to known threats and debilitate the mitigation of vulnerabilities. For example, the Air Force's information management structure centralizes most control at the Major Command, Service, and Department of Defense (DoD) levels. After the firewall is breached during a base attack, base administrators' primary means of securing the Base Information Infrastructure (BII) is to block the attacker's IP address and report the activity to both the Major Command and Service Computer Emergency Response Teams (CERTs). The Major Command's response is to deny access to rogue IP addresses and then pass information to the DoD CERT and the Joint Task Force Global Network Operations (JTF-GNO) center—who then shares information with other services. Also, there are Theater Network Centers and Theater CERTs, but they are often disheveled in the communication chain.

The slow propagation of information caused by the lag time between discovery of the exploitation and the sharing of information with other services and organizations, results in a vulnerability gap. Considering an attacker can gain another IP address within a matter of seconds—by attacking through another computer or by changing the IP address of the identified computer—the vulnerability gap can easily be exploited. The result is a cat and mouse game, whereby the defender is consistently one step behind the attacker, with no effective preventative options. Only decentralizing authority and the institution of lateral reporting procedures will enhance the ability of systems to combat real-time threats.

Lack of Cohesion: The current information hierarchy is managed through an ad hoc amalgamation of relationships. The lack of cohesion is apparent in the lack of collaboration by similar information systems. Operating in this manner turns a singular vulnerability into a system-wide weakness and recurring problem allowing the same vulnerability to be exploited in multiple systems on a number of separate occasions. The lack of cohesion stems from a failure to view all information systems, regardless of platform, as interrelated instead of a collection of independent systems. Although actual defensive techniques need to remain unique since every type of information system has distinctive defensive requirements, the overarching construct should be the same. This would enable a higher degree of information sharing, since threats to one system will often affect other systems. It will provide clear and comprehensive direction on how all information systems should defend their assets. Ultimately information systems that lack "jointness" invite information leaks, repeated information breaches, and the compromise of intelligence. Therefore, an integrated and cohesive defensive architecture is essential to combat any and all adversarial aims in the Information Domain.

In the past decade the focus has been on improving information security in computer systems and networks. This is important, but the same desire should extend to all information systems by viewing and defending them as one integrated system. If not, a variety of different defensive methods and procedures will inundate any Information Environment (IE) with extensive overhead required to run and maintain the defensive systems. It will spawn a sluggish and ineffective defensive architecture. Such an environment is not favorable and should be prevented.

Nearsighted Defense: A myopic or "nearsighted defense" occurs when the scope of defense efforts is extremely narrow, and interfaces between external systems are neglected. For example, Service CERTs do an inadequate job because they don't focus on the entire ID; they focus their efforts on organizations with computer networks directly connected to the Unclassified but Sensitive IP Router Network (NIPRNet) and Secret IP Router Network (SIPRNet). The result is the classification of all systems that do not connect to the NIPRNet or SIPRNet as being "isolated."

This assertion is dangerous considering many "isolated" systems connect to external users outside the DoD, both domestic and foreign organizations. In many cases an attacker could easily gain access to these systems by using externally "isolated" users as conduits to gain entry into DoD systems. Systems with nearsighted defense have a strategic vulnerability; fortunately, ameliorative measures to ensure adequate interface security and institute comprehensive patch management practices can mitigate this phenomenon.

The Increasing Threat

The ID is vast and the only way to prevent attacks is to isolate systems from the Information Domain. For most systems, isolation is not feasible; thus, defensive systems must be capable of combating enemy attacks. As new defensive systems arise, new methods of attack will follow, resulting in a cyclic rotation of defend-attack, defend-attack…. Information Defense Architecture is crucial to combat the threats in this attack-rich environment. The result is an environment where enemies with the desire and technological skill have inherent global reach capabilities. They are able to aggress against information systems from afar, with minimal effort and equipment.

The ID has some unique characteristics that lead to threats. First, ID activities happen on an accelerated timetable. In the physical domains threats are determined by the amount and quality of enemy offensive capabilities; but in the ID an enemy's ability to inflict destruction is based on knowledge, which is more difficult to detect than traditional military assets. Thus, the enemy is inherently more deceptive and is assumed to be all non-trusted system users.

Threat Gap: To characterize the increasing threat, attention is directed towards the ever increasing Threat Gap. Since the inception of large-scale commercial networks the number of reported computer incidents in the US has risen drastically, going from 252 incidents in 1990 to

137,529 in 2003.[5] Attack capabilities in the Information Domain increase effectiveness daily, as aggressors create new inventive and complex ways of penetrating information systems; while the defensive capabilities increase at a slower rate because not enough resources and attention are focused on solving the disparity in capability, resulting in a Threat Gap. The Threat Gap is depicted in the figure below and illustrates the almost exponential increase in attacker sophistication and complexity since the advent of the information age and the slow linear increase in the sophistication and complexity of defensive capabilities. The below tables 1 & 2 illustrate the exponential increase in attacker sophistication.

Carnegie Mellon University Computer Emergency Response Team

Reported Network Incidents

Year	Number of Reported Network Incidents
1999	9,859
2000	21,756
2001	52,658
2002	82,094
2003	137,529

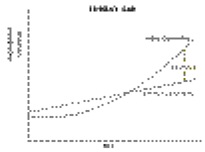
Table 1.[6]

Carnegie Mellon University Computer Emergency Response Team
Reported Application Vulnerabilities

Year	Number of Reported Network Incidents
1999	417
2000	1,090
2001	2,437
2002	4,129
2003	3,784

Table 2.[7]

To further illustrate the problem, Dan Wolf the Information Assurance Director for the National Security Agency cited DoD networks as being scanned at an average rate of 17,000 non-solicited scans per hour.[8] The gap will continue to widen until information defense technology and strategies can improve at a greater rate than attacker capabilities.



Attacks: The information highlighted above only illustrates the computer related attacks, but again the Information Domain is much more comprehensive than only computers. There are countless numbers of Radio Frequency interferences at Remote Satellite Tracking Stations that have been attributed to outside sources; in some cases we do not know whether the cause was hostile or friendly. Computer & network attacks are covered below because they are tracked well and publicized; although, it must be clear that computer & network attacks only represent one type of attack that can occur in the Information Domain. Most computer & network attacks are small-scale and occur daily, but they only have a temporary effect on military and civilian operations. An example is the defacement of over 2,000 websites, including a US Navy site by a 17 year old French high school student in July of 2003.[9] Another more serious example is of a Malaysian counterfeit ring that hacked into a bank's computer system in Nebraska and attacked its Visa Check program, stealing debit card numbers on 24 July 2003.[10]

A few large-scale attacks do occur but often are not publicized because of apparent national security repercussions. Those that are publicized help illustrate the ongoing threat that lingers. For example, Col Ted Dmuchowski, director of information assurance for the Army's Network Technology Enterprise Command confirmed that an attacker gained control of a military server in March of 2003.[11] There are countless examples of large-scale denial of service attacks, viruses and worms such as the Mellisa, Blaster, Slammer, and Welchia. Most of these attacks were global in 3 minutes. Although some of the above examples are not significant events, from a military standpoint, they demonstrate the potential chaos that can be inflicted by a tech-savvy opponent. These attacks constitute an increasing threat, especially considering the capabilities required to launch these types of attacks are easily available to terrorist and lone aggressors around the world.

State Actors: States have realized the promise of information attacks and are devising ways to leverage power through use of the Information Domain. Another source of threats comes from state actors, many of whom have attempted to hone their attack efforts by creating hacker schools to teach hackers and develop their skills. In 2003, China joined a number of other states in the inception of government sponsored hacker schools. In fact, Chang Mengxiong former Senior Engineer at the Beijing Institute of Systems Engineering stated that "[m]ilitary battles during the 21st century will unfold around the use of information for military and political goals…. Information warfare will be the most complex type of warfare in the 21st century, and it will decide who will win and who will lose the war."[12]

Single Point of Failure: As the military transforms and creates a more efficient force, the challenges of forging a secure and robust information architecture increase. For example, information assets are being combined into conglomerate mainframes, which create "one-stop shop" vulnerabilities in information systems. The disadvantage is that it also could be used to assist information aggressors in their data collection efforts if such a system is compromised. For example, the GIG has challenges associated with its security infrastructure and will be a tremendous vulnerability if an adequate security posture is not in place by its completion. Also, the Air Force's Intelligence Data Handling System (IDHS) contains massive amounts of information — support imagery, C3I analysis, and much more. If an enemy was able to gain access to such a system, the outcome could be catastrophic in military and civil sectors. In addition, the use of more "Commercial Off The Shelf" software by the military, in order to reduce developmental cost, increases the likelihood of information defense challenges; because commercial software typically does not have security that is adequate for systems dealing with sensitive information.

Combating the Threat is Essential

"[O]ne who knows the enemy and knows himself will not be endangered in a hundred engagements."[13] Sun-Tzu realized the importance of information over 2,000 years ago and his timeless advice is even more pertinent today. As war tactics progress in lethality and efficiency, militaries are able to inflict more damage with less effort. Therefore it has become more important to gain knowledge of enemy plans and positions, in order to prevent costly engagements by anticipating and thwarting enemy plans through the exploitation of information. Information warfare has begun and the US has yet to establish an adequate Information Defense Architecture.

As non-state and rogue actors realize the disparity between their power and that of conventional militaries, they will resolve to fight on a different front using new tactics. Soon they will seek easier and more advantageous methods of causing disaster, and IW will be their tool because of its ability to yield asymmetrical advantages when used to attack other information systems. Also, with global interconnections increasing daily, a states' reliance on information-in-war and the ability for low-tech and/or poorly funded adversaries to attack information systems makes the ID an adversary rich environment. Such a hostile environment constitutes an undeniable threat to military, public, and private information systems; thus it is essential to national security and all military operations to employ effective means of combating these threats.

Understanding The Information Domain

There are six domains or levels in which military operations can occur. Land, sea, air, and space are recognized and accepted as the four basic military operating domains. The fifth domain, cyberspace, germinated from the information age and consists of the vast interconnections of networked computer systems, both public and private.[14] The Information Domain is the sixth domain and is often confused with cyberspace, because it is regularly mentioned in conjunction with networks and computers; but the two are not synonymous. The ID is an overlapping domain, which has a high profile in cyberspace but it also exists in the land, sea, air and space domains, as illustrated in figure 1. More specifically, the ID describes a medium that allows the transfer of information through scientific means whether it is through data-links that connect a group of aircraft, information systems that connect forward air controllers to air battle managers, or the transfer of encrypted information over the SIPRNet. Next, an understanding of the composition of the ID is needed to better comprehend viable proposals for its defense, as presented in this paper.

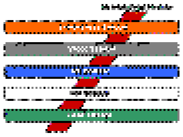


Figure 1. Domain Layout

The dissection of the Information Domain beyond the nominal domain layout yields a clear construct as to how the domain functions. For those reasons, a top down approach is taken to explain the ID.

Within the ID there are many different independent information networks, called Information Environments, which contributes to its complexity. An IE is best described as "[t]he aggregate of individuals, organizations, or systems that collect, process, or disseminate information; also included is the information itself."[15] IE is the environment in which information systems operate but the actual end-to-end connections of information systems constitute the Global Information Grid (GIG).[16] The figure below illustrates the ID and how IEs exist within the domain. The arrows that protrude from each Information Environment represent the information extending outside of an environment (i.e. Information Operations). Note, that some arrows partially or completely overlap illustrating inter-environmental interfacing, while some IEs do not interface. Also, Information Environments are in no apparent order; they constantly move throughout the ID creating and severing interfaces as necessary.

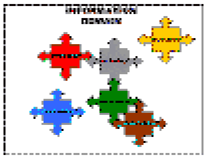


Figure 2. Information Domain

Understanding the inner workings of the IE is critical to understanding approaches to defending the ID. Figure 3 shows the internal structure of the Information Environment and illustrates the interconnection of systems that transmit information.

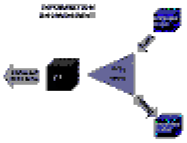


Figure 3. Information Environment

It is important to highlight that the above model holds true for all Information Environments regardless of the organization. Although figure 3 shows only two information systems, an IE consists of an infinite number. These systems generate the information that Command and Control (C^2) needs to reach desired goals. The illustration depicts information as being routed from information systems to an intelligence service either through the pushing of information from the system to the intelligence service or the pulling of information by the intelligence service from the system. The intelligence service then filters and triages information before forwarding information to C^2. Command and Control then takes the information through the Observe-Orient-Decide-Act process (OODA loop) to make decisions. The outputs from C^2 are Information Operations (IO) which are actions taken to affect an adversary's information and information systems without compromising one's own.[17] Reconnaissance missions, satellite surveillance, the encryption of phone messages, and network system attacks are a few examples of IOs (which are highlighted by arrows in figure 2). These operations extend outward from the main body of the IE as active arms that interact with other environments.

Information Defense Architecture Construct

The proposed solution to defend this domain is an integrated and cohesive IDA. Exploring this architecture is best explained in conjunction with discussions of the Information Environment, which is where the defensive construct is applied. It is important to first understand that the goal is not to create an indomitable fortress, because that is impossible; the goal is to great a dynamic shield that can adapt to attacks. A brief overview of the IDA illustrates that the foundation revolves around defending individual systems through the implementation of Information Fences. **Information Fences** (INFOF) are unique programs, policies, or actions applied to information systems to guard against specific threats. In an effort to create a robust and layered defense, each system contains multiple INFOFs that overlap to form **Information Walls** (INFOW), which provide a cohesive defense. Next the INFOWs are combined through information sharing, coupled with the ability for dynamic restoration of attacked or infiltrated systems, yields an **Information Shield** (INFOS). The INFOS is the pinnacle of information defense. The shield provides an integrated and cohesive defense for any IE. Next, exploring the INFOF, INFOW, and INFOS concepts in more detail will give further credence to the simplicity and benefit of this architecture.

Information Fences

In any Information Environment each element or system and its interfaces perform unique functions and require tailored defenses. Information fences provide a unique solution to a particular system threat. An example of INFOFs currently functioning in the US military IE is the information classification system that labels information as: for official use only, secret, and top secret in an effort to guard against the threat of exposing information to unauthorized parties.

An example of an INFOF policy in action occurred in 2001 when the US Navy EP-3E airborne reconnaissance plane collided with a Chinese fighter jet over the South China Sea and made a forced landing on China's Hainan Island. The US information defense policy to destroy intelligence-gathering equipment in compromising situations is an example of an INFOF.[18] Another example, depicted in figure 4, illustrates a base level computer network firewall

(INFOF) blocking unauthorized external entities (attackers) from gaining access. However, this firewall does not prevent internal users from sending sensitive information out of the system, which reemphasizes the role of an Information Fence as a defensive mechanism for a specific threat. Thus, in order to have an effective defensive construct, another step must be taken to account for the multiplicity of threats. Information Fences must conjoin to become Information Walls.

Figure 4. Information Fence

Information Walls

As previously mentioned, Information Fences are designed to guard against specific types of attacks; so to defend a system comprehensively, multiple layers of fences are required. INFOFs have cumulative properties, the more defensive agents in place (fences) the stronger the defense; as a measurement the number of fences should at a minimum equal the number of threats. The amalgamation of a collection of INFOFs spawns the foundation for the Information Wall. As an example, Information Security (INFOSEC), network security, encryption techniques, and the classification system are all programs that function as INFOWs; because each is comprised of a collection of specific defensive techniques (INFOFs) that function to provide a higher level of security or protection for the systems they are designed to defend.[19] There are four basic characteristics of an effective INFOW. First, it ensures system availability. Next, it provides mechanisms to guarantee data integrity. Also, IFOWs must be capable of authentication, which ensures that only desired communication takes place. Finally, it is essential that an INFOW provide confidentiality by protecting transmitted data from passive attacks such as eavesdropping.

If an Information Wall is constructed with Information Fences for all known vulnerabilities, the system will be secure until an adversary can attack an unrealized vulnerability—for which there is no fence—or until the attacker can improvise attack methods to penetrate any INFOF. In the diagrams below, three fences overlap to illustrate how a wall encloses an information system to block all adversarial attacks.

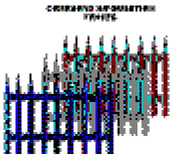


Figure 5a. Information Wall

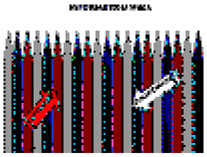


Figure5 b. Information Wall

Although figures 5a and 5b illustrate the effectiveness of an INFOW at defending its systems, it does not constitute a comprehensive defense because the interfaces between systems remain vulnerable. In Figure 6, the push and pull arrows represent the interfacing of information between the systems and an Intelligence Service; the figure depicts an absence of defensive systems (INFOW) around the interfaces, to illustrate their vulnerability. For example, if Space Command obtained sensitive information through a surveillance satellite (system A) and their method of passing that information to the National Reconnaissance Office (system B) for processing is by way of mail; it is easy to see that regardless of the strength of the INFOWs A and B, the information is vulnerable because of the weakness of the mail system's defensive capabilities (interface vulnerabilities exist).

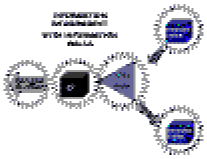


Figure 6. Information Walls in the Information Environment

Therefore protecting the interfaces between systems is just as critical as defending the systems. What good does it do to have two perfectly secure information walls around two systems, only to have information compromised in transit? To eliminate interface vulnerabilities between systems, additional walls have to be put in place. An example of an interconnection INFOW is the Airborne Information Transmission (ABIT), which provides a secured data link relay to move imagery and other intelligence information from collection platforms to ground stations and/or other airborne platforms.[20] Figure 7 illustrates the addition of interface INFOWs to secure the transmission of information between systems, which results in a comprehensive system of Information Walls, which is also considered to be an Information Shield in its embryonic stage.

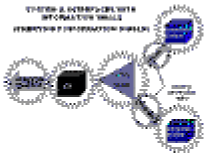


Figure 7. Systems and Interfaces with Information Walls

Information Shield

As depicted above, the Embryonic INFOS is not yet complete. As previously asserted, adversaries are flexible in their attacks, thus an evolving enemy easily conquers a rigid defense.

This begs that flexibility be included in the construct of the IDA. Giving the INFOS dynamic capabilities through information sharing and a maintenance program adds the flexibility that is needed to constitute a cohesive Information Defense Architecture.

Making the Information Shield Dynamic

Real-time information sharing is the key to constructing a dynamic INFOS that can accommodate rapidly changing needs. Establishing open communication lines between systems ensures that an information system that has been attacked quickly notifies other information systems. A good way to ensure positive information sharing is to establish an INFOS Manager. He or she is responsible for receiving all reports of attacks and pertinent information surrounding those attacks and ensures information is disseminated to systems that could possibly be affected (similar to CERT procedures). The caveat is that individual systems are constantly being attacked and there must be a classification system to prevent the INFOS Manager from being overloaded with information, thus slowing up the response time for critical attacks. This high degree of information sharing will eliminate the aforementioned problems of successful redundant attacks, and will serve to connect all the defensive walls into one seamless defensive structure. Once the multiple INFOWs are combined with fluid communications, the result is the INFOS illustrated in the figure 8 below. The fluid communications caused the INFOWs to move away from their singular mission of protecting one system, to functioning as a component in the overall shielding of an IE.

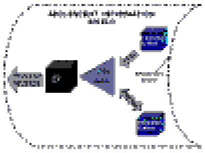


Figure 8. Adolescent Information Shield

The next phase of creating the INFOS is to incorporate dynamic agents to foster a more robust and mature shield. Making an INFOS dynamic requires the creation of a maintenance program capable of maintaining the integrity of an Information Shield by being able to swiftly **detect, identify, repair,** and **adapt** components of an information system in real time. This four-step **Patch Cycle** gives the shield an organic-like quality enabling it to detect and identify changes in the security state, repair damage, and adapt the system before it is compromised. Figure 9 shows the continuous process that the INFOS cycles through to search and repair the shield.

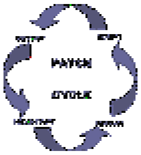


Figure 9. Patch Cycle

●**Detection:** Requires methods and sensors to continually monitor the health of the INFOS. The detection methods and sensors must be reliable but not predictable. They must determine when and what type of attack took place. A predictable detection system would allow an adversary to easily bypass the detection methods and create a backdoor into a system.

●**Identification:** Is the battle damage assessment step that involves determining, what INFOF(s) were affected, how it happened, and who is responsible.

●**Repairing:** Is the process of taking the appropriate measures to fix any damage to an information asset and/or INFOFs caused by an attack.

●**Adaptation:** Involves permanent modification to the attacked system's INFOFs which bolsters the defense of its INFOSs. Also, adaptation includes the sharing of information enabling other systems to adapt to the potential threat before an attack.

It is important to note that in order for the Patch Cycle to be effective its execution must be decentralized, because without a speedy response, the Patch Cycle, although still useful, will not be preventative. Once the Patch Cycle is incorporated into the defensive construct the shield is completely dynamic and results in a mature Information Shield as depicted in figure 10 below.

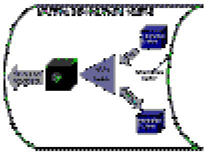


Figure 10. Mature Information Shield

Conclusion

In conclusion, in the information age, the ability to defend information systems is imperative for sustained operations and waging war. As previously mentioned, since the beginning of warfare, Information-In-War has been used as a key component in giving militaries advantages over their adversaries. In the twentieth and twenty-first centuries the complexity and effectiveness of information systems spawn the desire to disrupt them and has resulted in the need to defend the ID. As stated by Secretary of Defense, Donald Rumsfeld, "[w]e need to make the leap into the information age, which is critical to the foundation of our transformation efforts; and the ability of forces to communicate and operate seamlessly on the battlefield will be critical to our success.[21]

Part of such a leap includes having reliable Information Assurance for systems in the Information Domain; which is done through the creation of a dynamic Information Defense Architecture, such as an Information Shield. Furthermore, as technology improves and enemy capabilities are enhanced, the threat gap will continue to increase resulting in more vulnerabilities in the ID. Industrial powers and rogue states are organizing complex hacker schools, which combined with the maturity of the next generation of politically motivated computer savvy global youth, will create an omnipresent threat. Traversing through the ID will be like walking through a minefield with armor (Information Shield) as the only defensive mechanism. As these non-conventional forces gear up for future battle, in the Information Domain, it has become paramount that the

United States bolsters its defensive information posture to protect itself within a hostile domain. The institution of the GIG is a productive first step, but the fight cannot only be won by the speed and control in which information systems operate; it must be won by preventing the enemy from disrupting those operations. The threat gap is widening and the future security of the United States is at risk; defensive preparation must intensify to avoid a possible Information Age Pearl Harbor.[22]

Notes

1. An Information System for the purposes of this architecture is any controllable system that can be used to facilitate, collect, process, share, defend, degrade, or disrupt information.

12. Information Domain is a non physical domain that extends across the land, sea, air, space, and cyberspace domains.

13. Bruce Berkowitz, The New Face of War (New York: The Free Press, 2003), 21.

14. Air Force Basic Doctrine (AFDD) 1, Air Force Basic Doctrine, September 1997, 81.

5. Carnegie Mellon University CERT Coordination Center, "CERT/CC Statistics 1988-2003," 22 January 2004, on-line, Internet, 15 April 2004, available from http://www.cert.org/stats.

6. Dan Wolf, "Fighting the Net: Securing Today's Battlefield" (presentation at the 8th Annual Information Assurance Workshop, Atlanta Ga, 5 February 2004), on-line, Internet, 2 May 2004, available from http://www.cert.org/stats/cert_stats.html#incidents.

7. Dan Wolf, "Fighting the Net: Securing Today's Battlefield" (presentation at the 8th Annual Information Assurance Workshop, Atlanta Ga, 5 February 2004), on-line, Internet, 2 May 2004, available from http://www.cert.org/stats/cert_stats.html#incidents.

8. CNN, "Police: Teen Hacker Hit 2,000 Sites" 12 July 2004, on-line, Internet, 13 July 2004, available from http://www.cnn.com/2003/TECH/internet/07/11/young.hacker.ap/index.html.

9. Associated Press, "U.S. bank hit by international hackers: Counterfeit Ring Hacks Nebraska Bank's Computer," 24 July 2003, on-line, Internet, July 27, 2003, available from http://www.cnn.com/2003/TECH/internet/07/24/bank.hack.ap/index.html.

10. Bob Sullivan, "US Military Computer Attacked," 19 March 2004, on-line, Internet, 7 April 2004, available from www.tecrime.com/llartH12.htm

11. Chang Mengxiong, "The Revolution in Military Affairs Weapons of the 21st Century," Chinese Views of Future Warfare, ed. Michael Pillsbury (Washington D.C.: Government Printing Office, 1998).

12. Ralph Sawyer ed., Sun Tzu, The Art Of War, (New York: Barnes and Nobel, Inc., 1994), 135.

[13] Winn Schwartau, Information Warfare, Cyber terrorism: Protecting Your Personal Security in the Electronic Age, 2nd ed. (Thunder's Mouth Press, NY, New York, 1996).

[14] Information Operations: Doctrine, Tactics, Techniques, and Procedures, Joint Publication 3-13, November 2003, 1-2.

[15] Defense Information Systems Agency, "Global Information Grid," 24 February 2003, on-line, Internet, 10 March 2004, available from http://www.disa.mil/ns/gig.html

[16] Air Force Basic Doctrine (AFDD) 1, Air Force Basic Doctrine, September 1997, 81.

[17] Rogers Worthington, "Benefits to China Downplayed," Chicago Tribune, 5 April 2001, on-line, Internet, August 15 2003, available from http://www.globalsecurity.org/org/news/2001/010405-aries7.htm.

[18] INFOSEC is the "[r]esult of any system of policies and procedures for identifying controlling, and protecting from unauthorized disclosure." From Air Force Basic Doctrine (AFDD) 1, Air Force Basic Doctrine, September 1997, 81.

[19] William Stallings, Cryptography and Network Security Principles and Practice, 2d ed. (New Jersey: Prentice Hall. 1999), 7-11.

[20] John Pike, "Airborne Information Transmission System (ABIT)," 2 December 2002, on-line, Internet, 29July 2003, available from http://www.globalsecurity.org/intell/systems/abit.htm.

[21] David A. Denny, "Rumsfeld Sees Urgent Need to Transform the U.S. Military," 31 January 2002, on-line, Internet, 20 May 2003, available from http://www.usembassy-israel.org.il/publish/peace/archives/2002/february/020101.html.

[22] David Alberts, "Defensive Information Warfare," August 1996, on-line, Internet, 20February 2003, available from http://www.ndu.edu/inss/books/Books%20-%201996/Defense%20Information%20Warfare%20-%20Aug%2096/ch12.html.