Rethinking Defensive Information Warfare

Geoffrey S. French, General Dynamics
10455 White Granite Drive, Suite 400
Oakton, Virginia 22124
geoff.french@gd-ais.com

Abstract

Although the origins of information warfare lie in the defense of critical computer systems, defensive information warfare (DIW) per se has advanced little beyond an information assurance model. Information assurance is an integral part of any military organization's operations, but it falls far short of meeting the needs for robust defense of critical command-and-control (C2) computer networks against a sophisticated adversary. By looking at the ways that militaries have responded to challenging defensive situations in the past, some insights can be made into the nature of IW and potential application of conventional operations. This paper examines defensive tactics and strategies—from the German defense in depth that emerged from World War I to the American Active Defense that developed in the Cold War—and proposes a new mindset for DIW that draws on these operational concepts from military history.

Introduction

Many military theorists who have discussed information warfare (IW) rightfully point out that the United States, because of its civilian and military dependency on information technology (IT) systems, is vulnerable to attacks on those systems.[1] In fact, some argue that the United States is the most vulnerable of any nation. It makes sense, then, that even though the U.S. military has not yet launched a computer network attack against enemy IT systems in a conflict, the defense of its own networks has been a high priority.[2] It would follow that the U.S. military therefore must have a rigorous program for defen-

[1] See, for example, the scenarios presented in B. Berkowitz, "Warfare in the information age," In: *Information Age Anthology Volume I*, D.S. Alberts and D.S. Papp (eds), (Washington D.C.: DoD C4ISR Cooperative Research Program, 2001) and Center for Strategic and International Studies, *Cybercrime ... Cyberterrorism ... Cyberwarfare* (Washington D.C.: CSIS Press, 1998).

[2] A cyber attack is not the only means of offensive information warfare. By the U.S. Department of Defense definition of information operations, many activities could count as offensive actions, such as the use of leaflets, the distribution of food, and press conferences. For the purposes of considering threats to computer networks, this paper will focus on attacks that degrade, disrupt, deny, or destroy those networks.

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
JUN 2004		**00-00-2004 to 00-00-2004**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Rethinking Defensive Information Warfare	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **General Dynamics,10455 White Granite Drive Suite 400,Oakton,VA,22124**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**		**102**	

sive information warfare (DIW; also referred to as IW-D), with specific tools and techniques designed for exclusive use in war. A review of its doctrine and planning, however, shows the opposite. In the field of DIW, the U.S. military draws no distinction between what is done in peace and in war, and offers little outside of generic information assurance. This philosophy may have advantages in seeming to carry a perpetually high degree of readiness, but it disintegrates under close inspection. A review of the current concepts in DIW and an examination of the underlying principles show that they are inadequate for the defense of critical command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) networks in a conflict with a sophisticated adversary.

Current Concepts in Defensive Information Warfare

As with other concepts related to information-age warfare, DIW can mean several things, depending on the context.[3] Unlike some of these concepts, however, DIW has not been explored to the same extent. There are relatively few official documents that discuss it and little published literature on the topic. To set a foundation for an in-depth exploration, it is important to understand DIW in doctrine, theory, and practice.

Doctrine

The U.S. Department of Defense (DoD) defines DIW as a subset of defensive information operations (IO). Defensive IO consists of:

> The integration and coordination of policies and procedures, operations, personnel, and technology to protect and defend information and information systems. Defensive information operations are conducted through information assurance, physical security, operations security, counter-deception, counter-psychological operations, counterintelligence, electronic warfare, and special information operations. Defensive information operations ensure timely, accurate, and relevant information access while denying adversaries the opportunity to exploit friendly information and information systems for their own purposes.[4]

This definition is discussed in depth in Joint Publication 3-13, "Joint Doctrine for Information Operations," which devotes the third chapter to defensive IO. Joint doctrine focuses primarily on operations security (OPSEC) and risk management. The chapter emphasizes identifying assets, vulnerabilities, and protective measures, and the steps to restore systems if attacked. The text devoted to response includes law enforcement activity, diplomatic actions, economics sanctions, and military force. Succinctly, defensive IO is meant to provide "protection, detection, restoration, and response."

[3] See, for example, the discussion of *value* and *shared awareness* in R.E. Giffin and D.J. Reid, "A Woven Web of Guesses," presented at the 8th International Command and Control Research and Technology Symposium, Washington D.C., June 17–19, 2003.

[4] U.S. Department of Defense, Joint Pub 3-13, Joint Doctrine for Information Operations, 1998, GL-5. This term and its definition are approved for inclusion in the next edition of Joint Pub 1-02.

This same vision is reflected in the U.S. Air Force Doctrine Document 2-5, "Information Operations." In fact, the concept is further diluted. In place of the term *defensive IO*, the Air Force uses *defensive counterinformation* operations, a wider-ranging term to include counter propaganda and public affairs, in addition to the DIO activities outlined above. In this implementation, the defensive concept encompasses the protection of any information-based process in military activity, but loses a distinct role in wartime altogether. Remarkably, Air Force doctrine does not address response to cyber attack in any way except in an example where the Air Force Computer Emergency Response Team (AFCERT) recommended blocking certain e-mail and web page attacks from Air Force networks.[5]

The limitation of this definition is the mindset it represents, where the emphasis is on passive monitoring and basic OPSEC procedures. This shortcoming is acknowledged in the Joint Information Operations Planning Handbook, which states that so little has been written on full spectrum defensive IO planning that it "leaves one with the distinct impression that Defensive IO equals IA [information assurance] and CND [computer network defense]."[6] Unfortunately, the document does not offer any additional ideas, adhering to the same generic risk management methodology. U.S. doctrine regarding DIW is at best poorly conceptualized. In attempting to account for every possible threat to information, it provides almost no guidance for response to a cyber attack in wartime conditions or preparations for improving defense prior to an attack. In this light, DIW doctrine leaves the military with little information concerning network defense in war.

Theory

In many areas of the military arts, doctrine can lag behind theory. Individuals who are outside of the military establishment (or inside, but on the fringe) have more freedom to discuss new concepts and write about the potential implementation of new tools or new organizational concepts. In some cases, this is a necessity, as new technologies are introduced from the outside and must be adapted for military use (e.g., the airplane). In others, the military itself forges the new path (e.g., the submarine). IW theory tends to follow the former, where many people discuss potential implementation of IW concepts. Given the state of DIW doctrine, one might expect to find more or different ideas in the literature. Unfortunately, DIW theory is not far ahead of doctrine at all.

The National Defense University press published the major work on the issue (titled *Defensive Information Warfare* by David Alberts) in 1996. Alberts looks at the topic broadly to include the threat of attacks on civilian infrastructure. This breadth is reflected in his definition of DIW: "all actions taken to defend against information attacks, that is, attacks on decision makers, the information and information-based processes they rely

[5] U.S. Air Force, Doctrine Document 2-5, "Information Operations," 2002, p 19.
[6] Joint Forces Staff College, "Joint Information Operations Planning Handbook,"(Norfolk, Virginia: National Defense University, 2003), p. VI-3.

on, and their means of communicating their decisions."[7] It is also manifest in his solution: general deterrence is seen as the major contributor to U.S. DIW efforts.

Alberts does provide direction for other aspects of a national DIW strategy. Although he admits that, "there is poor ability to identify which assets are critical because attacks on seemingly insignificant systems can cause cascading failures in critical systems,"[8] his approach is to rank systems from unimportant to critical, and then defend them with increasing levels of effort. The "lowest defenses block common or 'everyday' attacks. More sophisticated attacks are faced with more stringent defenses, and strategic attacks face the most intricate defense."[9] (Alberts refers to this as "defense in depth.") Although appealing at a high level, the book does not solve the basic problems that are at the heart of IW: in an interconnected sector of networks defended at their perimeters, it is tremendously difficult to separate the most critical assets from the least valuable, and to differentiate the common attacks from the strategic. In the end, the reader is left without a clear idea of how to implement such a strategy on any level.

A 1999 RAND report by Robert H. Anderson and colleagues attempted to pursue a more detailed approach in this direction. Although *Securing the U.S. Defense Information Infrastructure* has a similar theme as *Defensive Information Warfare*, its analysis is more focused in that it addresses only DoD systems for command, control, communications, and intelligence (C3I), while providing categories for vulnerabilities and mitigation strategies. Within that set of systems, it attempts to define a "minimum essential," but Anderson quickly concedes that "any attempt to mark off part of the information infrastructure as 'minimum essential' quickly dissolves into the realization that just about everything must be included."[10] Without resolving that dilemma entirely, the authors introduce a six-step process, the first two dedicated to identifying critical functions, and the systems that rely on them. The remaining steps are to identify vulnerabilities, identify countermeasures, implement countermeasures, and test countermeasures.

Anderson and colleagues argue that their process cannot be a centralized effort, but instead requires local implementation. As importantly, the book discusses defense in depth (albeit with a different definition than Alberts) "in which multiple levels of such hardening and monitoring are employed to catch perpetrators penetrating the initial system defenses."[11] One potential additional defense the authors discuss is a honeypot (see Box 1) This honeypot would be used to "detain perpetrators long enough to allow better understanding of their sophistication, modus operandi, and interests, and to allow trace-

[7] D.S. Alberts, *Defensive Information Warfare* (Washington D.C.: National Defense University Press, 1996), p 4.
[8] D.S. Alberts, *Defensive Information Warfare* (Washington D.C.: National Defense University Press, 1996), p 36.
[9] D.S. Alberts, *Defensive Information Warfare* (Washington D.C.: National Defense University Press, 1996), p 40.
[10] R.H. Anderson, P. M. Feldman, S. Gerwehr, B. Houghton, R. Mesic, J.D. Pinder, J. Rothenberg, and J. Chiesa, *Securing the U.S. Defense Information Infrastructure: A Proposed Approach*, (Santa Monica, Calif.: RAND, 1999), p 9.
[11] R.H. Anderson, et al., *Securing the U.S. Defense Information Infrastructure: A Proposed Approach*, (Santa Monica, Calif.: RAND, 1999), p 9.

back of their access route."[12] Although Anderson approaches the problem from the bottom up (vice Alberts' top-down approach), he and Alberts arrive at the same hopeful conclusion that a risk management approach can secure DoD's networks.

By comparison, the Defense Science Board presents a much darker outlook in its two reports on this topic. Its 1996 report called for improvements in basic capabilities such as damage control and impact assessments; its 2001 report starkly concluded that "DoD cannot today defend itself from an Information Operations attack." Although the conclusions are similar, the Defense Science Board took different approaches in its reports. The first looked broadly at the national information infrastructure and took threats to the economy and civilian functions into account. It found DoD's ability to defend this infrastructure lacking, making recommendations for DoD to improve tactical warning for IW attack, capacity for damage control during the attack, and tools to assess the impact of an attack afterward.[13] Importantly, this concentration on DoD ability to respond to a wartime attack is missing from both Alberts and Anderson, whose approaches address general attacks at any time.

The second Defense Science Board report looked more narrowly at DoD's information infrastructure, but also explored its dependence on civilian telecommunications. Using Joint Vision 2020 as its departure point for DoD's near-term capabilities and needs, and looking in particular at the Global Information Grid (GIG), the Defense Science Board found (again) that DoD did not have adequate programs and planning to defend this infrastructure from a sophisticated adversary. Its recommendations included stronger architecture for the GIG, increased capability to detect intrusions, and increased research and development on security technology.[14]

Box 1: Honeypots

Honeypots are "systems designed to be compromised by an attacker. Once compromised, they can be used for a variety of purposes, such as an alerting mechanism or deception." A honeynet is a network of honeypots used "to learn the tools, tactics, and motives" of an attacker.

Honeypots and honeynets are found most commonly as security research tools, typically as independent servers or networks that hackers attack at random. Observations from such research can identify the intentions or techniques used by the attackers, and the results are published on such community sites as the Honeynet Project, found at http://project.honeynet.org.

Source: The Honeynet Project, *Know Your Enemy* (Boston: Addison-Wesley, 2002).

[12] R.H. Anderson, et al., *Securing the U.S. Defense Information Infrastructure: A Proposed Approach*, (Santa Monica, Calif.: RAND, 1999), p 52.
[13] Defense Science Board, Information Warfare – Defense (Washington D.C.: Office of the Under Secretary of Defense for Acquisition and Technology, 1996).
[14] Defense Science Board, Defensive Information Operations (Washington D.C.: Office of the Undersecretary of Defense for Acquisition, Technology, and Logistics, 2001).

Although basic protective measures are essential to military operations, and risk management is a proven tool for limiting vulnerability of critical assets, these elemental documents (both in doctrine and in the literature) fall short of providing a vision for defensive cyber-based activity in wartime. This lack of vision is reflected in the current U.S. operational concepts as implemented.

Practice

Given the lack of distinction in doctrine between peacetime and wartime operations, and the basic risk management approach outlined in the literature, it is understandable that there are few plans for DIW operations. The strength of the current DoD approach is that it emphasizes the importance of daily defense and individual events. Its basic weakness is that it fails to acknowledge that different tactics and strategies are needed in wartime circumstances. In other words, DoD would argue that it is currently engaged in DIW operations (or, more specifically, defensive IO or—more nebulously—defensive counterinformation operations). This CND would consist of monitoring for intrusions, identifying viruses and worms, patching systems and applications, enforcing user authentication and privileges, and incident response. Incident response can include the forensic investigation, intelligence analysis, and legal or counterintelligence investigations or operations. This serves DoD well in peacetime, but these approaches do not stand up to scrutiny when considered in a wartime environment.

Fundamental Flaws in Information Assurance

By the accepted definition (in doctrine, theory, and practice), DIW would consist essentially of information assurance, albeit rigorously enforced. In its ideal state, information assurance means that the following conditions are true:

1. There are no flaws in the hardware or software running on a specific system.
2. There are no implementation or configuration flaws in the system's network.
3. All patches and anti-virus or intrusion-detection signatures have been updated.
4. Only authorized users have access to a specific system.
5. Those users have only the privileges that they need to do their job.
6. No one is acting against the organization's interest.

The basic principles of information assurance—maintaining the confidentiality, integrity, and availability of network services and data—serve most systems well. In an everyday environment, the majority of system compromises result from user error or the exploitation of a known vulnerability for which a patch or remedy exists. When a hostile, sophisticated adversary is introduced, however, information assurance processes cannot stand up to systematic challenge. Information assurance is based on the theory that network security is attainable in principle, that the conditions above will work out for the positive. If any one fails, however, the security of the entire system will be breached. Unfortunately, none stand up under close inspection.

Flawed Hardware and Software

Casual experience shows that the first condition is false. Technical sites are updated daily with the latest discovered flaws. This is true of operating systems (such as Windows and Linux), basic network services (such as Domain Network Service and Simple Network Management Protocol), and applications (such as Microsoft Internet Information Service). The fact that flaws in these are discovered on a regular basis implies that there are more. From a logical standpoint, CND analysts must accept the premise that flaws exist that have yet been discovered or announced, and—more importantly—that it is possible that those flaws are currently being exploited without their knowledge.

The Failure of Signature-Based Defenses

Acknowledging that flaws exist and that exploits will follow leads directly to the need for network defenses, but the most common defenses are also philosophically flawed. Both anti-virus software and most intrusion detection systems are based on recognizing the activity or characteristics of known malicious code (the code's *signature*). This can be the name of an executable, the size of an e-mail attachment, the port a worm uses, or any other number of characteristics. By definition, these are created *after* the malicious code is detected and analyzed. This explains why an Internet worm can be caught by a firewall or anti-virus, yet its immediate variant cannot. Malware writers sometimes make only minimal changes in a worm to alter its signature. Regardless, from a logical standpoint, network engineers must accept the premise that even rigorous application of signature files will not protect their networks against malicious code that has not been encountered before. For large outbreaks, it is can be a small amount of time—a matter of hours—before the signature update is ready. Unfortunately, with recent malware, worms have propagated worldwide within minutes. Both the Slammer worm (MS-SQL Server Worm) and MyDoom.A saturated the Internet before the signature file updates were available. If a malware writer were to target a specific organization with a customized worm, a signature may never exist. So the CND analyst must admit that the network—although protected against all past worms and hacker tools—may well be defenseless against the worm released tomorrow and the hacker with a brand new exploit.

The Failure of One-Time Authentication

Even if the network engineers have properly configured their networks, installed the most recent patches, and updated the very latest anti-virus signatures, CND analysts cannot assume that no exploits will succeed from the outside. A quick review of the users who are logged into the system show that they are all legitimate, but this, too, is a logical trap. The overwhelming majority of networks today require a one-time authentication: typically a user name and a password. Countless studies, however, have demonstrated the weakness in this system.[15] The tension between easily remembered passwords and suffi-

[15] For an illustrative example, see the Infosecurity Europe press release from April 15, 2003, "Office workers give away passwords for a cheap pen," www.infosec.co.uk/page.cfm/T=m/Action=Press/PressID=3.

ciently secure passwords tends to break along the lines of convenience. Most passwords are still easily guessed. Others are too complex, and written down near the computer. Unless the organization has rigorous review of passwords and enforcement of rules that infuse some security into the system, one-time authentication remains—and will remain—weak. Unfortunately, the trends point to consolidation of one-time authentication, manifest in "single sign-on," which allows users to log in to numerous systems through a single set of keys activated with one password. Ultimately, all the network administrator really can attest with certainty is that everyone logged in has an authentic user name and password. Whether the people using those accounts actually correspond to their owners is a completely separate issue. If an intruder can guess a password, obtain the password through malicious code, or change the password through social engineering, the intrusion detection system may have nothing at all to detect. From a logical standpoint, CND analysts must accept the premise that simple user authentication is weak, and that it is possible that unauthorized users are currently using the network without being detected.

The Reality of Complexity

Even with the very simple scenarios described above, the security of the network can be considered to be straightforward. In practice, the network is vastly more complex. Hardware components can have default logins. Some users log in from home or while on travel. The computers they are using may have some flaw that the network engineer cannot control or they may be running outdated anti-virus software. Outside organizations have connectivity to parts of the network. The interaction of operating systems and hardware cause unforeseen consequences for security. C4ISR networks will be just as complex. The GIG and the systems it supports (such as the Global Combat Support System and the Joint Global Command and Control Systems) will involve tactical radios, satellite and air communications, and fiber optic backbones. It is meant to connect DoD intelligence and combat assets around the globe, and support coalition forces as needed. Each entry point, data exchange, and dependency will complicate the GIG's security.

Of course, there are a number of technical solutions to individual security problems. Some anti-virus and intrusion detection software is behavior based. Some software will make a baseline of a user's normal activity and report anomalies that could reveal unauthorized use of the account. Public Key Infrastructure (PKI) and smart cards can build in additional layers of authentication. Even so, each of these processes rely on humans and security often suffers. Digital certificates have been stolen.[16] Users allow others to log in with their accounts. Administrators download unauthorized tools or software. For a network that is actually being used, the complexity is very high, and this erodes security. The information assurance model, therefore, can never attain its ideal state; too many conditions simply cannot be met. Yet current DIW doctrine and theory puts information assurance at the heart of its risk management-based strategy.

[16] National Infrastructure Protection Center, "Warning not to accept VeriSign Microsoft digital certificates dated January 29–30, 2001," Advisory 01-006, March 23, 2001.

The Limits of Risk Management

The basis for risk management is that organizations make conscious decisions about what risks they will accept and which they will mitigate. This works well for many processes, and for physical security. For digital security, however, the logic fails. Too many real-world examples demonstrate that networks connected to the Internet can be compromised from the outside. Too many cases of insider activity illustrate the damage that legitimate users can do. These risks may be acceptable if the organization has the time to identify and mitigate the intrusions and compromises. This luxury, however, will not be available in wartime; even a small amount of wrong information in a C4ISR system "can have a major impact on the quality of situational understanding and lower the chances of high-quality military decisions."[17] The consequences of a successful cyber attack, therefore, are unacceptably high. Defenses cannot be built around a reactive, perimeter-based philosophy.

During a conflict, C4ISR networks will be priority targets for a technologically advanced adversary. To limit DIW to information assurance or risk management would place it entirely in the reactive mode of passively waiting for and then responding to countless exploits. Making the assumption that networks are secure and depending on them to operate normally is to invite failure. Logic demands that CND analysts and network engineers anticipate exploits they have not seen, malfunctions that they did not foresee, and constant attacks. From this standpoint, DIW requires a different philosophy for its operations.

A New Basis for Defensive Information Warfare

Just as a commander would not use force protection concepts as a basis for defending a geographic area from an invading force, DoD should not use risk management as its basis for DIW. It should instead look at military history and doctrine for conventional defensive operations. Using that information to assess the situation for defending a C4ISR network, a commander should see that there are two major challenges. First, for the reasons above, a perimeter defense is unlikely to succeed. Second, he has almost no ability to counterattack. This is due to the fact that incoming attacks are difficult to trace past the attacking host, which is unlikely the point of the attack's origin.[18] Moreover, the rules of engagement are still unclear. This could be interpreted as a disadvantage in firepower, and fortunately, there are corresponding tactics and strategies upon which a commander can draw. Most prominent among these are the German defense in depth that emerged from World War I, the American Active Defense that developed in the Cold War, and Serbian use of deception and denial against NATO in the 1999 Kosovo campaign.

[17] D.S. Alberts, J.J. Garstka, R.E. Hayes, and D.A. Signori, *Understanding Information Age Warfare* (Washington D.C.: Command and Control Research Program, 2001), p. 86.

[18] Digital attackers typically run their operations through a series of compromised sites to obscure the actual origin and complicate legal or counterintelligence investigations.

Defense in Depth

A commander considering the defense of the digital perimeter should examine the lessons learned from trench warfare. Toward the end of World War I, German Army commanders realized that the philosophy of rigid defense of forward trenches could be maintained only with an enormous loss of life. As an alternative, the Germans developed a defense-in-depth strategy. This assumed that the outermost defenses would be breached; the personnel was limited, therefore, to lightly manned outposts. The second line, built around machine-gun nests, disrupted the momentum of the attack, slowing its progress while a third line brought fire on the enemy. This allowed a reserve to counterattack and restore the perimeter.[19] This defense allowed the outnumbered Germans to maintain both fronts until the American Expeditionary Force irreversibly shifted the balance of power. Although modern commanders must not weaken their digital perimeters, they must realize that they are likely to be penetrated. Careful thought, therefore, must be put in the second and third lines of defense.

As mentioned above, however, information assurance and DIW has already seized upon the term defense in depth. Unfortunately, this concept has several interpretations, yet little coherence. For some, it simply means that information security policies are more rigorously enforced on certain systems. For others, it means that policies and procedures are considered to be a layer of defense that supplements technical defenses.[20] In practice, poorly designed defense in depth means that a system has different defenses for different entry points, and if any fails, then the system's security is compromised.

Drawing on the conventional defensive operations returns the focus to the need for multiple technical means for identifying anomalous activity that assume the other means have failed. Behavior-based anti-virus and tools that monitor user behavior are useful tools in this capacity, but honeypots, located behind the perimeter, may be the best solution. Because no user has a genuine need to access the data on a honeypot, any activity triggers an alarm. In this way, they can detect the activity of an intruder that has successfully penetrated the firewall and other security systems or an insider with authorized access conducting unauthorized activities.

There are multiple courses of action that a counterintelligence officer can take at this point. In peacetime circumstances, an officer can dedicate the resources to allow the intruder to continue as if unobserved, hoping to glean information about tradecraft and purposes of the intruder. In wartime, this may not be possible. Honeypots require a major investment in time from counterintelligence analysts and system administrators to ensure that the intruder is kept within constrained segments of the network and to analyze the intruder's activities and effects. A more immediate benefit would be to immediately cut off the intruder, letting the adversary know that the operation was detected. The adver-

[19] W.S. Lind, "The theory and practice of maneuver warfare," In: *Maneuver Warfare: An Anthology*, R.D. Hooker, Jr. (ed), (Novato, CA: Presidio, 1993), p. 6; J.M. House, *Combined Arms Warfare in the Twentieth Century* (Lawrence, Kansas: University Press of Kansas, 2001), pp. 40–43.

[20] D. Luddy, "Defense in depth: A practical strategy for achieving Information Assurance in today's highly networked environments," (Ft. Meade, Maryland: National Security Agency, undated).

sary may then treat the tools and techniques used to gain access to the system as burned, thereby denying the adversary further use. If possible, analysts could use the information from the honeypot to create signatures to detect the activity and increase the perimeter defense across DoD. Honeypots tend to be used in very small numbers or as stand-alone systems in a honeynet. In wartime, networks should have many honeypots, maximizing the chance that an intruder would encounter one. This would serve to detect the enemy's efforts better, slow the progress of all further cyber operations, and potentially deny enemy attention to specific systems. Deployment should be controlled locally so that commanders can decide how much time and resources to invest in the operation.

Active Defense

A commander considering the inability to counterattack beyond his or her own perimeter has many historical points to contemplate. In fact, this is a situation to which many U.S. adversaries have had to adapt, and some have done so quite well.[21] The U.S. military faced this problem in the Cold War, where it struggled with the question of how to defend Western Europe from a Soviet invasion.[22] Because NATO faced a numerically superior foe, it was expected and presumed that simple hardened defenses would be overrun. Defenses based on a straightforward exchange of fire would also fail because the numerical imbalance translated into a Soviet advantage in firepower. In the 1970s, General William DePuy led the creation of the Active Defense. The strategy sought to funnel the invading forces, through terrain and hardening of prepared positions, into ground most suitable for long-range artillery bombardment and counterattack. This would help commanders ascertain the enemy's main point of attack and allow him to concentrate limited resources to meet it. The ground forces had to be especially mobile in order to reinforce where needed, quickly capitalize on opportunities to strike, and—just as importantly—return to the hardened defenses before the next wave of the enemy appeared.[23]

Although Active Defense may not be as easy to translate into a digital defense as defense in depth, there are key concepts to apply. The first is hardened, prepared positions. In typical information assurance terms, hardening refers to deactivating unneeded protocols, closing unneeded ports, and ensuring that default logins are disabled. It can also include encryption and digital signatures. A better method for hardening a system would be to use a restrictive rather than a permissive operating system. Operating systems are built to run all programs, with the exception of those specifically forbidden (typically, known malware). In contrast, rigid execution control means that all executa-

[21] R.H. Scales, Jr., "Adaptive enemies: Achieving victory by avoiding defeat," *Joint Forces Quarterly,* Autumn/Winter 2000 (No. 23):7–14.
[22] For a broad discussion of the American response to Soviet numerical superiority, see J.A. Engel, "Cold War at 30,000 Feet" (2001, PhD Dissertation, University of Wisconsin-Madison), pp. 62–66.
[23] P.H. Herbert, "Deciding What Has to Be Done: General William E. DePuy and the 1976 Edition of the FM100-5, Operations," Leavenworth Paper No. 16, (Ft. Leavenworth, Kansas: Combat Studies Institute, U.S. Army Command and General Staff College, 1988), pp. 79–85.

bles are forbidden except for an allowed set.[24] This set can be further identified by a one-way hash that ensures that the code has not been altered. DoD should consider drastic changes to its critical networks, including the operating systems.

The second lesson commanders might glean from Active Defense is the need for mobility. This principle can also be enacted in cyberspace. In peacetime, an adversary can quietly perform reconnaissance on a network, identifying its routers, gateways, servers, firewalls, and other components outside of the DMZ. This will provide them with IP addresses, configuration, and baseline traffic of a network. In wartime, it would be in the interests of certain networks to be able to change its address, configuration, and perhaps even equipment. This would neutralize any past reconnaissance that an adversary may have gathered. If these changes are made on a sufficient number of systems, it will require the enemy to review all reconnaissance information, even that done of systems that have not changed. One possible method for enacting this digital mobility would be to have an unused set of IP addresses at the disposal of DoD. Ideally, rather than have the IP blocks suddenly becoming active when needed, traffic could be artificially produced so as to simulate activity in peacetime. A prearranged, simultaneous change to DoD's DNS and BGP tables would activate the change when needed.

Deception and Denial

A U.S. commander should also look at lessons learned from the adversary's standpoint to see adaptation to a disadvantage in firepower. One example is the air war over Kosovo. In 1999, NATO launched air operations over the Former Republic of Yugoslavia in an effort to prevent then-President Slobodan Milosevic from killing or forcing the removal of ethnic Albanians from Kosovo. NATO commanders hoped the operation would produce the desired results in two days. Instead, the air campaign lasted over two months. NATO air strikes were never able to target Serbian military assets effectively, regardless of increased numbers of aircraft in theater or lowering the acceptable altitudes of certain attack fighters.[25] Rudimentary deception and denial tactics such as camouflage and simple decoys worked well, as did more the sophisticated tactic of exposing a real target to surveillance and replacing it with a decoy for the warfighter to destroy.[26] Eventually, NATO expanded its target set to include civilian infrastructure to bring pressure on Milosevic.[27] Regardless, Serbian forces simply avoided U.S. firepower by countering its ISR.

[24] For an introduction to executable control lists see A.E. Smith, "Staying alert with executable control lists," Iris Associates Inc, 1999. For a more robust executable control concept see M. Peretti, "Authenticated Execution," SecureWave, 2002.
[25] P. Sheets, "Air war over Serbia," In: *Lessons from Kosovo: The KFOR Experience*, L. Wentz (ed), (Washington D.C.: DoD Command and Control Research Program, 2002).
[26] T.L. Thomas, "Kosovo and the current myth of information superiority," *Parameters* XXX(1):13–29.
[27] P. Sheets, "Air war over Serbia," In: *Lessons from Kosovo: The KFOR Experience*, L. Wentz (ed), (Washington D.C.: DoD Command and Control Research Program, 2002).

In the digital realm, there are some tools that allow deception. Some proponents will put honeypots in the category.[28] It should be noted, however, that these bring deception to bear after the intruder has penetrated the network. It would bring a greater benefit to the commander to focus the deception outside of the firewall, preferably countering the adversary's scanning and probing that comes prior to an attack. The adversary's reconnaissance must identify what the perimeter network assets are, what operating systems they are running, what services are available to outside networks, and what ports are being used. To use an analogy from conventional operations, deception and denial efforts targeted at this reconnaissance will be the farthest forward that a defender can block the attack.

Digital deception and denial can be achieved in a number of ways. Ideally, all incoming scans and probes are diverted to a simulated network that will respond with authentic but incorrect information. Some software allows simulated responses that are generated by a store of known responses. This may be satisfactory for very low-level attackers, but will not deceive a more sophisticated adversary. It will be important for simulations to be as authentic as possible. The decoy network can also take several shapes, showing a realistic composition of components or an unrealistic architecture. There are advantages to each. Realistic-looking networks may absorb more of an adversary's time; an unrealistic-looking network may cause the adversary to turn his attention elsewhere. Ideally, this capability would be controlled centrally so that a higher command can observe the effects of certain deceptions and avoid causing unintended consequences such as funneling the adversary toward a network that DoD would rather be left alone. If orchestrated properly, this capability would be coupled with the others outlined above. Instead of waiting passively for a cyber attack to arrive, DoD could counter adversary targeting and reconnaissance. Instead of trusting that the perimeter defense will check every attack, multiple layers of defense will anticipate, contain, and counter penetration of C4ISR networks.

Conclusions

Over the last few years, the concept of IW has lost much of its emphasis on war, especially when thinking about defensive operations. When the Defense Science Board stated that DoD could not defend itself from an IO attack, however, it was not referring to an enemy propaganda campaign. DIW needs to focus on countering adversary cyber attacks against DoD C4ISR assets, to include the GIG, in a wartime environment. Although there are fundamental differences between digital and conventional defenses, there are many principles and strategies that can be adapted to DIW. One of the best aspects of the American military has been its openness in discussing strategic issues and its willingness to implement lessons from military history. It needs to reinvigorate both of these aspects with regard to DIW, which is in danger of stagnating with its logically flawed doctrine and practice.

[28] Fred Cohen & Associates, "The deception toolkit," available at http://all.net/dtk/dtk.html.

GENERAL DYNAMICS
Advanced Information Systems

Rethinking Defensive Information Warfare

Geoffrey S. French

Overview

- **Current state of DIW**
  - Doctrine
  - Theory
  - Practice
- **Fundamental Flaws in Information Assurance (IA)**
  - Technical and logical shortcomings
  - Limits of cyber risk management
- **New Basis for DIW**

DIW Defined

Joint Pub 3-13

The integration and coordination of policy, personnel, and technology to protect information and information systems.

IA, physical security, OPSEC, counter-deception, counter-psyops, CI, EW, and special information operations.

Ensure access while denying adversaries the opportunity to exploit friendly information and information systems for their own purposes

DIW Explained

- OPSEC and risk management
- Protection, detection, restoration, and response

DIW Expanded

- Defensive counterinformation
- Counter propaganda and public affairs
- Protection of any information-based process in military activity

DIW Doctrine

- **Emphasis is on passive monitoring and basic OPSEC procedures**
- **Generic risk management methodology**
- **No guidance for**
  - preparations for improving defense prior to an attack
  - response to a cyber attack in wartime conditions

DIW Theory: NCI Focus

- **1996 NDU Study**
  - Addressed defense of national critical infrastructure (NCI) as well as military
  - Acknowledges that poor ability to identify which assets are critical
  - Recommends raising level of defense to meet the sophistication of the attack

DIW Theory: DII-Focus

- **1999 RAND study**
  - Addressed Defense Information Infrastructure
  - Called for definition of “minimum essential”
  - Acknowledged that “just about everything must be included”
  - Set up six-step risk management process

Defense Science Board Studies

- **1996 Report**
  - Looked at both DII and NCI
  - Called for improvements in basic functions (warning, damage assessment)
- **2001 Report**
  - Looked at DII
  - Called for stronger architecture in the Global Information Grid, better intrusion detection, and increased R&D

DoD cannot today defend itself from an Information Operations attack

Defense Science Board, 2001

Current State of Practice

- **Expansion of term, focus on day-to-day operations and computer network defense (CND)**
  - Monitoring for intrusions
  - Identifying malware
  - Installing patches
  - Incident response
- **Emphasis on IA**

Is IA a Solid Foundation?

- **Based on ideals**
  - Flawless software
  - Flawless implementation and configuration
  - Up-to-date patches and signatures
  - Access limited to authorized users
  - Users have appropriate privileges
  - No one undermining security

Hardware and Software

- **In reality**
  - Operating Systems (e.g., Windows)
  - Fundamental Services (e.g., BIND)
  - Applications (e.g., IIS)
- **Flaws exist**
  - Not just announced and patched vulnerabilities
  - Undiscovered flaws

The patch model for Internet security has failed spectacularly.

Caida, 2004

Signature-Based Defense

- **Anti virus, intrusion detection, firewalls**
  - Rules are set up to identify known characteristics of existing exploits or malware
- **By definition, reactive**
- **Cannot stop the zero-day exploit or the latest worm**

Authentication

- **Most networks require simple authentication**
  - Username
  - Password
- **Passwords are notoriously insecure**
- **Moving toward “single sign-on”**
- **Poor verification of authorized use of network**

The Reality of Complexity

- **In theory, network security should be straightforward**
- **In practice, it is complex**
  - Interactions of hardware, software
  - Mobile users
  - Personal equipment
- **There are individual solutions to each problem, but each solution has its own vulnerabilities and problems**

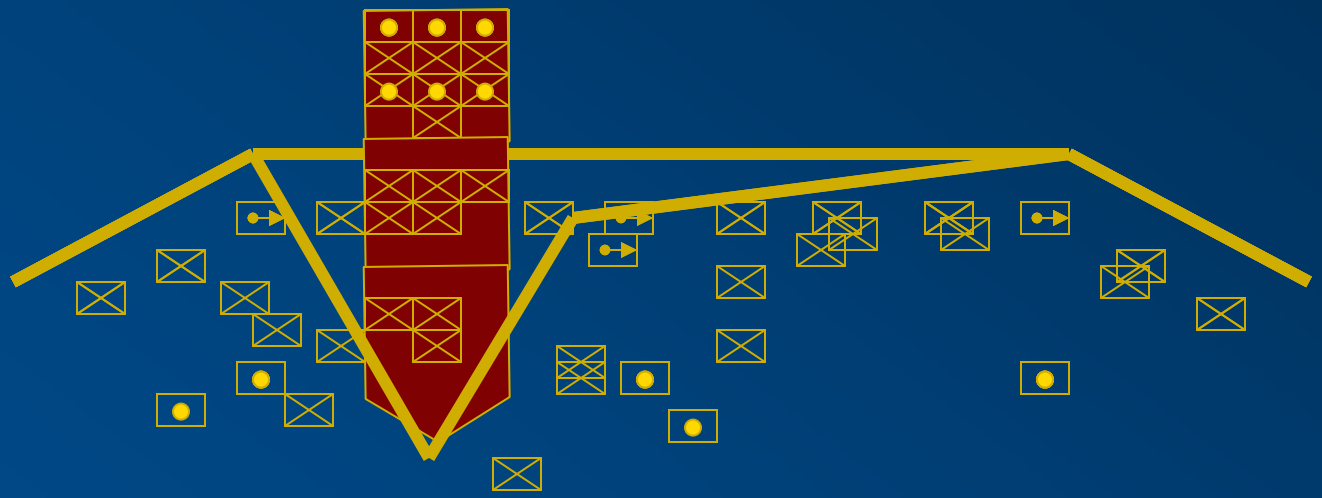
Implications for Risk Management

- **Poor definition of "critical" assets**
  - May be no differentiation
- **In peacetime, risk may be acceptable**
  - Time to investigate intrusions
  - Personnel to respond to incidents
- **In wartime, the risk is unacceptable**
  - Against a sophisticated adversary, IA certain to fail
  - A small amount of wrong of unavailable data can have a large impact on military decisions

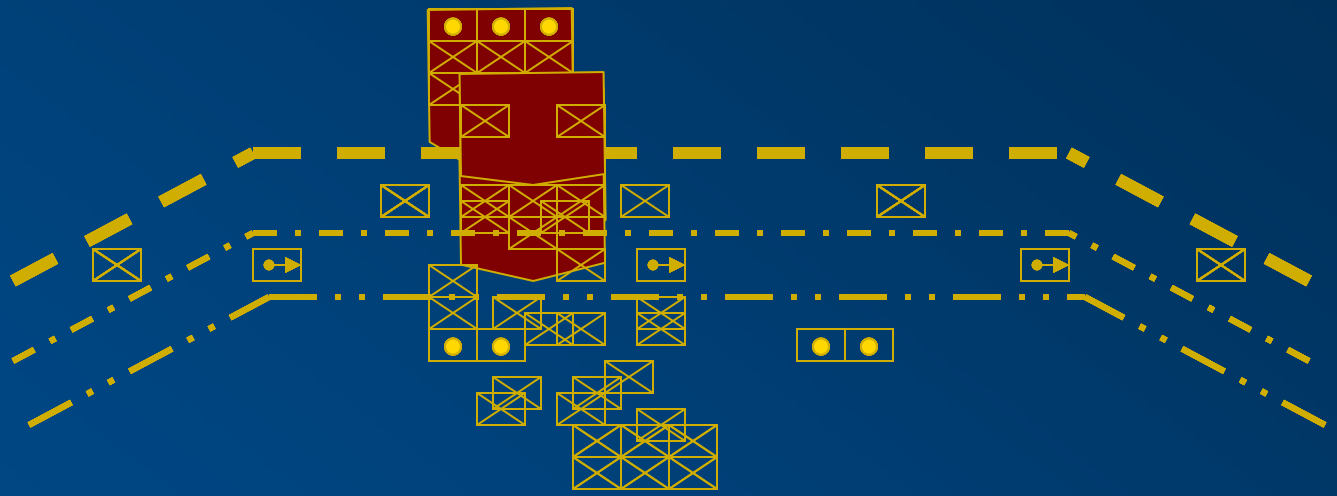
New Basis for DIW

- **Examine military history**
- **Draw analogies**
  - Perimeter defense unlikely to succeed
  - Limited ability to counterattack
- **Historical examples**
  - German defense in depth from WWI
  - American active defense from Cold War
  - Serbian defense of NATO Kosovo air campaign

WWI Perimeter Defense



WWI Defense in Depth

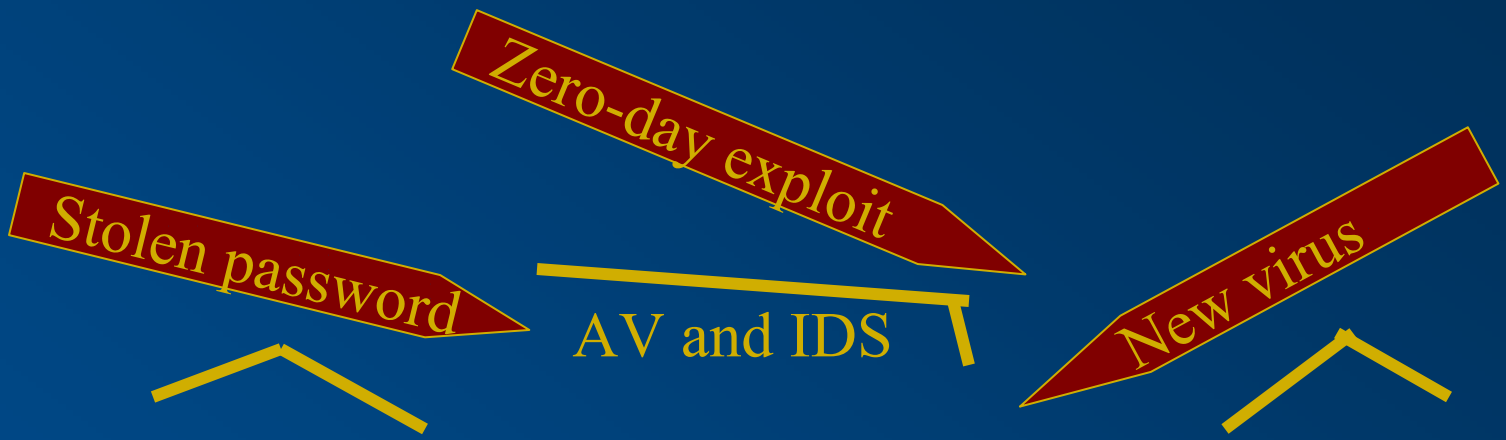


Lessons Drawn

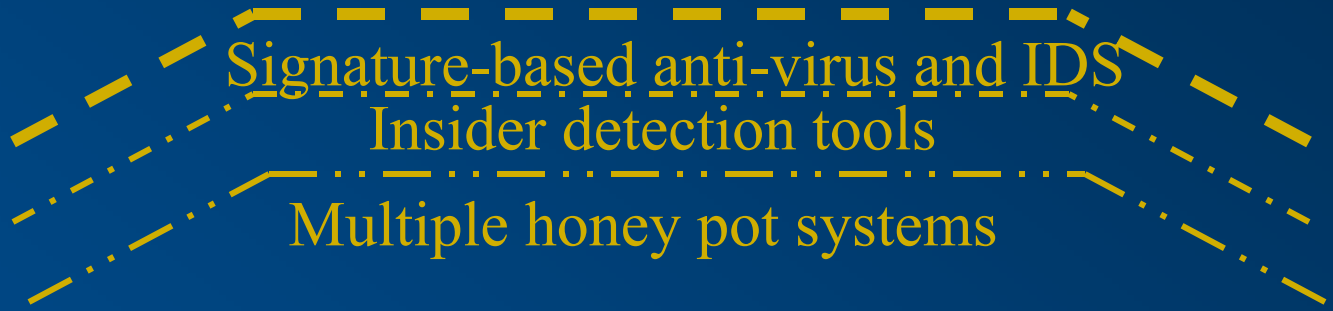
- Even with forward-deployed forces, perimeter will be penetrated
- Detection and reaction are part of defense

Network Perimeter Defense

Network Perimeter Defense



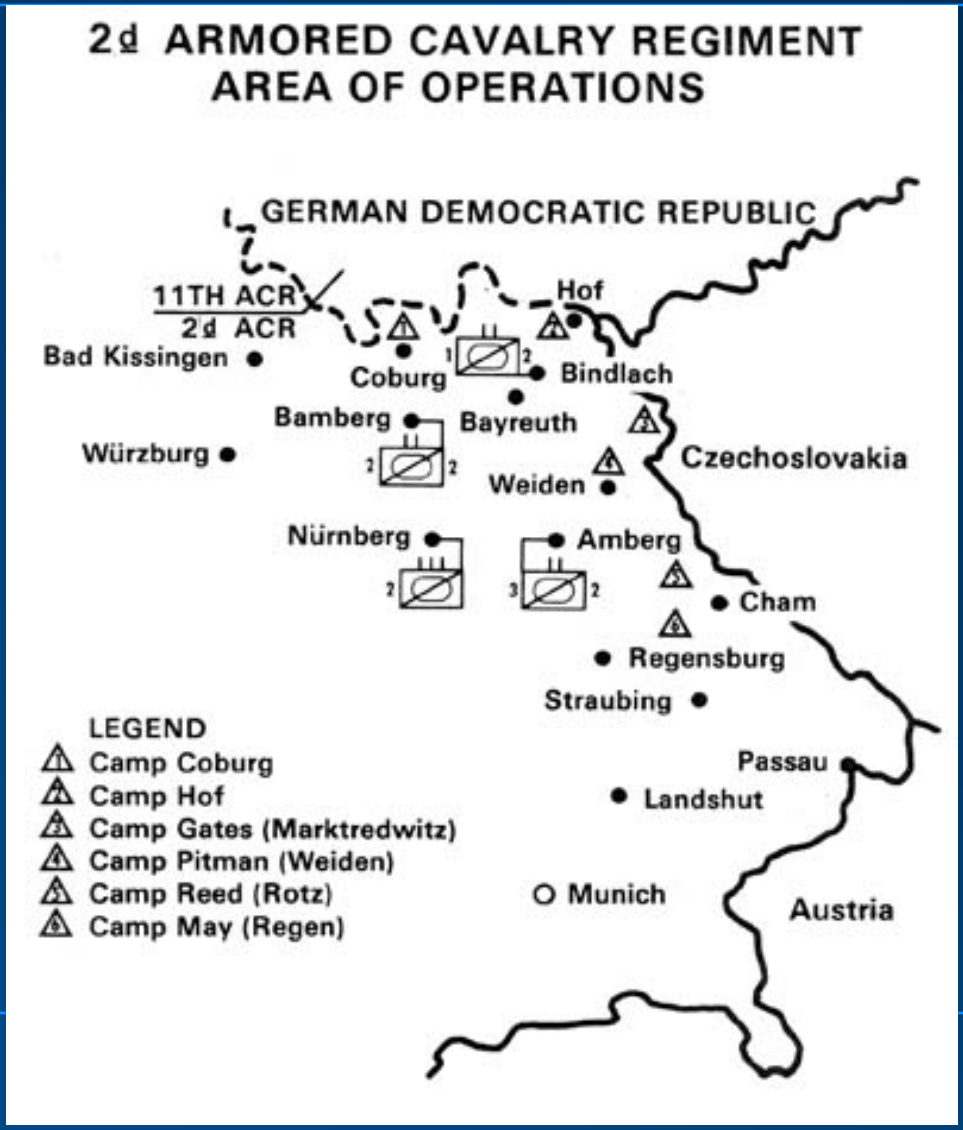
Network Defense in Depth



From Forward Defense to Active Defense

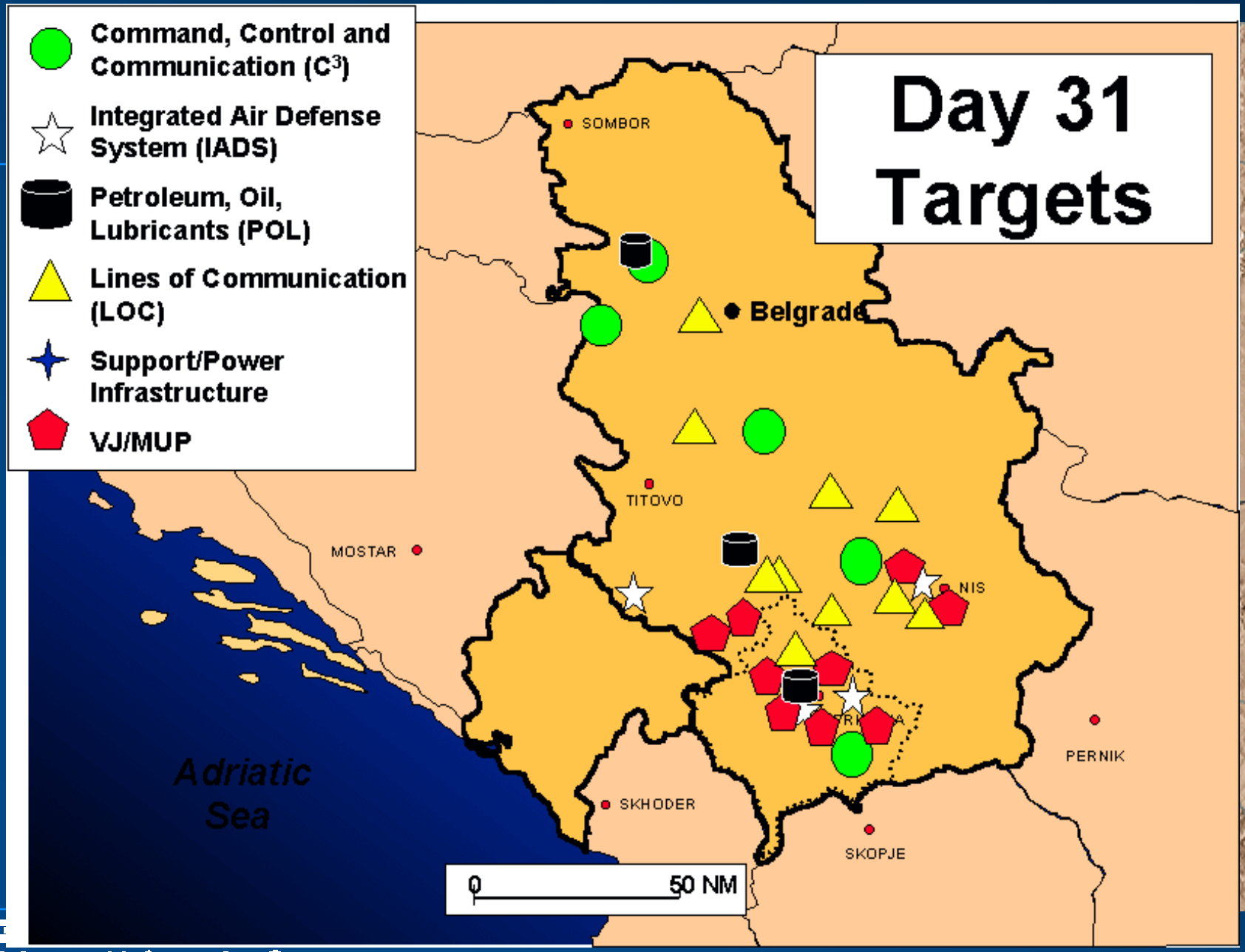
- **US faced numerically superior foe**
- **Active Defense**
  - Firepower disadvantage
  - Knew forward positions would be overrun
  - Response: hardening combined with mobility

Cold War: European Defense



Active Network Defense

- **Hardening**
  - Locked down operating system
    - Rigid execution control
- **Mobility**
  - Countering adversary reconnaissance
  - Changes in
    - IP addresses
    - Configuration (including DNS and BGP)
    - Equipment



Advanced Information Systems

Source: Global Security

Lessons drawn

- **Deception and denial**
  - Neutralize enemy firepower advantage by countering intelligence, surveillance, and reconnaissance

Network-based Deception

- **Not necessarily honeypots**
- **Targeted at adversary reconnaissance**
  - Simulated responses
  - Diverted traffic to real networks
- **Should be tailored**
  - Could draw in adversary
  - Could discourage adversary
- **Should be centrally controlled**

Integration

- **If combined**
  - Counter pre-crisis adversary reconnaissance with mobility
  - Counter reconnaissance during crisis or war with deception
  - Detect insider threat and network penetration
  - Harden certain systems to better protect critical systems
- **Prepare DoD systems for war**

Summary

- IW has lost emphasis on war
- DIW has lost any concept of escalation for crisis or conflict
- Military history can illustrate adaptations in the face of adversity
- DIW needs to look to military history to reinvigorate review of strategic needs