IAnewsletter

The Newsletter for Information Assurance Technology Professionals

Volume 3 Number 4

USPACOM

Theater Network Operations

Ensuring Information Superiority for the 21st Century

also inside—

- A Retrospective on Computer Network Defense
- Where There's Smoke, There's Fire...
- Keys to the Kingdom
- Law Enforcement & Counterintelligence Support to CND

contents

on the cover

ia initiatives

in each issue

IAnewsletter

Editors
Robert P. Thompson
Robert J. Lamb
Creative Director
Christina P. McNemar
Information Processing
Robert F. Scruggs
Information Collection
Page Y. Eastman
Inquiry Services
Peggy O'Connor
Contributing Editor
Ellen Loeb

IAnewsletter is published quarterly by the Information Assurance Technology Analysis Center (IATAC). IATAC is a DoD sponsored Information Analysis Center, administratively managed by the Defense Technical Information Center (DTIC), Defense Information Systems Agency (DISA).

Inquiries about IATAC capabilities, products and services may be addressed to:

Robert P. Thompson
Director, IATAC
703.289.5454

We welcome your input! To submit your related articles, photos, notices, feature programs or ideas for future issues, please contact:

IATAC
ATTN: Christina P. McNemar
3190 Fairview Park Drive
Falls Church, VA 22042
Phone 703.289.5454
Fax 703.289.5467
STU-III 703.289.5462

E-mail: iatac@dtic.mil
URL: http://iac.dtic.mil/iatac

Cover and newsletter designed by
Christina P. McNemar

Distribution Statement A:
Approved for public release;
distribution is unlimited.

United States Pacific Command

Theater Network Operations

Ensuring Information Superiority for the 21st Century

Brigadier General (P) James D. Bryan, USA
Commander, JTF–CND and Vice Director, DISA
Mr. Patrick Gorman

"We are not smart enough to predict the future, so we have to get better at reacting to it more quickly."

—General Electric adage

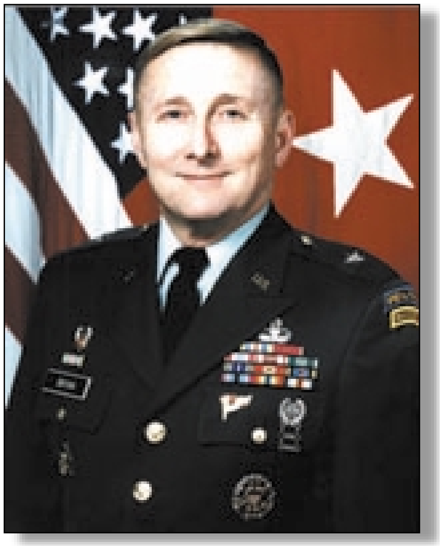
Information superiority enables the realization of Joint Vision 2010 concepts by transforming the traditional battlefield functions of move, strike, protect, and sustain into the operational concepts of dominant maneuver, precision engagement, full-dimensional protection, and focused logistics. These emerging operational concepts are presumed to take advantage of particular advances in sensor-to-shooter linkages and general advances in computing and information transport. The resulting construct gives us a glimpse of network-centric warfare, a concept that asserts that in the future the primary means of generating and sustaining combat power will be a seamless joint network of sensor, information, and engagement grids that links sensors, command and control (C2) centers, and shooters. This seamless global information grid (GIG) will implement network-centric warfare concepts of speed of command, self-synchronization, and massed effects. It is also a critical precursor to a knowledge-centric force in which context and content coordination enhance C2 to enable decentralized decision making and self-synchronized operations.

The movement from a platform-centric to a network-centric warfighting environment, however, will increase the number of users, nodes, and links, significantly increasing demand on computers and data networks.

This explosion of command, control, communications, computers, and intelligence (C4I) requirements will increase the demand and criticality of network troubleshooting, network management, dynamic bandwidth management, information and network protection, and spectrum management. These functions will move from their traditional low-visibility support role to a critical high-visibility warfighting capability. In short, the network will become a weapon system and should have a command relationship commensurate with that of normal operational forces.

21st Century Warfighting Environment

Whereas warfare in past conflicts was often a sequence of semi-independently unfolding events that could be planned for at a deliberate pace, future conflict will be conducted at an unprecedented pace with great fluidity. The 21st century warfighting environment will require a new mentality for mastering the command of a vast array of forces operating at these greater speeds, over larger spaces. The campaign of the future will consist of a seamless web of interdependent actions conducted in parallel rather than a sequence of independent actions. This new technology-driven approach to warfare will require new processes and organizations. The enhanced military capabilities of speed, range, unprecedented accuracy, lethality, and strategic mobility expressed in Joint Vision 2010 are predicated on United States achievement of information superiority. However, the rapid advances in computer processing and information transportation technologies that are the foundation of information superiority are creating new vulnerabilities and challenges for the U.S. military. Foremost among these challenges is the need to man-



age the explosion of information and proliferation of networks while protecting both the information and the networks that carry it.

The increased emphasis on achieving information superiority is causing a proliferation of complex webs of interdependent links and an explosion in the number of computers, and data, voice, and video networks, supporting the warfighter. The movement toward split-based operations, in which many warfighting functions are performed in the rear in support of more agile forward-based forces, is blurring the lines between joint task force (JTF) forces, networks, and, base, post, camp, and station command, control, communications, and computer (C4) systems. Moreover, this greater dispersion and increased connectivity will demand an unprecedented amount of bandwidth, both wired and wireless, to support joint and coalition military operations.

The complexity of the future warfighter's network demands will be compounded by the potential fragility of the global networked environment. ELIGIBLE RECEIVER, the first large-scale exercise to test our ability to respond to an attack on our information infrastructure, demonstrated that hostile forces could penetrate the national infrastructure and DoD networks, and could affect DoD's ability to perform certain missions. These findings were validated in 1998 by Solar Sunrise, a series of attacks targeting DoD network domain name servers. Both ELIGIBLE RECEIVER and *Solar Sunrise* clearly demonstrated that in the current interconnected environment, everyone in DoD resides in a shared risk environment. In a networked world, an event anywhere eventually reaches everywhere through ripple effects.

The demands of the future warfighting environment and the explosion in both number of users and level of connectivity are leading to the following trends:

- **Greater Complexity—**The sheer number of systems nested within systems makes it difficult to readily isolate and understand events, determine cause and effect, and select appropriate courses of action.
- **Greater Interdependency—**Information flows and networks that previously were relatively isolated along organizational lines have become interdependent because of the demand for fully integrated joint operations and the drive toward C4I interoperability.
- **High Tempo—**Improved information processing systems and networking capabilities have significantly decreased decision time and increased the operations tempo, forcing the Joint Force Commander to rapidly sense, decide, and respond to his environment with minimal delays. Timely and assured information delivery is no longer a luxury but a critical warfighting necessity, providing a competitive edge in warfare.
- **Decreased Predictability—**Increased global-level complexity and interdependence, and rapid rates of technological change make it difficult to prepare and plan for unforeseen events through traditional organizations and procedures. The competitive advantage will now go to those who can quickly and accurately anticipate and respond to rapidly unfolding events.

The 21st century warfighting environment demands new capabilities to improve the agility, speed, and accuracy of the operational forces. Achieving information superiority is at the core of these capabilities, and providing assured delivery and protected information is critical to obtaining information superiority.

Commander's Challenge

"...a failure in one part of the infrastructure affects the delicate and complex balance of the entire interconnected system. Unfortunately, the number of these types of events seems to be increasing at the same rate as our reliance on information technology."

—Mr. Arthur L. Money[1], Assistant Secretary of Defense for Command Control, Communications, and Intelligence (ASD/C3I)

Operational Challenge

The emerging network-centric warfighting environment and the advent of knowledge-centric decision making has caused the Defense Information Infrastructure (DII) to evolve into a complex web of information processing and transport systems, which are monitored and controlled by different organizations from geographically dispersed locations. Under these circumstances, it is very difficult for combatant commanders, like the Commander in Chief, U.S. Pacific Command (USCINCPAC), to maintain cognizance over the various critical information systems and networks that support operations in their theaters. Unfortunately, the number and complexity of the networks that can provide information to a theater are rapidly outstripping our ability to manage those networks, protect them against intrusions and attacks, and effectively manage available bandwidth.

Currently, the Commander in Chief (CINC) has only limited ability to view the status and performance of the theater information grid and has no fusion and analysis ability to determine potential joint operational impacts of network outages and attacks, no dynamic ability to determine action alternatives, and no established C2 structure for prioritizing and executing a theater-wide response to network failures and attacks.

Desired Operational Capabilities

Joint Vision 2010 defines information superiority as “the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary’s ability to do the same.” Achievement of information superiority is based on meeting three primary challenges: Battlespace awareness (J2), information operations (J3), and information transport and processing (J6). Information transport and processing (ITP) also comprises four desired operational capabilities (DOC): assurance, capacity, interoperability, and information management.

- **Assurance (DOC ITP-1):** Defending against information threats and providing the warfighter with high-quality information services when needed to meet the dynamically changing demands of the future.
- **Capacity (DOC ITP-2):** Providing the warfighter with a flexible, adaptive network to transmit and receive the right volume of information at the right time and the right place.
- **Interoperability (DOC ITP-3):** Providing universal transaction services that allow the warfighter to exchange and understand information unimpeded by differences in connectivity or language, on a real-time basis, regardless of location.
- **Information Management (DOC ITP-4):** Managing an assured, real-time, scalable information flow throughout the infrastructure.

A key to meeting these challenges is the global information grid (described in more detail below). However, the current stovepiped environment, which is characterized by scores of separately managed, noninteroperable networks with varying levels of network management, configuration management, and information protection, makes it difficult to visualize, manage, and protect this grid with any degree of effectiveness or efficiency. Moreover, management of most of the networks that compose the GIG is conducted as an administrative rather than an operational function, with uncertain chains of command. Most of the associated technologies and procedures reflect a Service-centric rather than a joint network-centric warfighting perspective.

NETOPS Background

“In order for the U.S. to exert, to the maximum extent possible, the power of our military forces in future operations, all military entities and functions must be part of a common integrated information infrastructure.”

—Defense Science Board, 1998 Summer Study Task Force on Joint Operations Superiority in the 21st Century

Global Information Grid

The DII, together with its supporting policies, plans, and programs, was conceived in the early 1990s to align basic information processing and transport services with DoD's functional area applications and common applications. The alignment was intended to improve the ability to execute joint military operations and the efficiency of key underlying mission support tasks. However, achievement of information superiority and other operational tenets of Joint Vision 2010 requires a new assured, network-centric and knowledge-centric paradigm that treats information as a critical warfighting resource. The need for an affordable, interoperable, protected information grid is emphasized in the 1996 Information Technology Management Reform Act (ITMRD also known as Clinger-Cohen), the 1997 Quadrennial Defense Review (QDR), and Presidential Decision Directive 63, (PDD) Critical Infrastructure Protection (CIP).

The GIG is an ASD/C3I initiative aimed at improving security and interoperability while reducing costs, by moving from an infrastructure (DII) to an enterprise (GIG) approach to achieve information superiority. The GIG is envisioned as a globally interconnected, end-to-end set of information capabilities associated processes, organizations, and personnel for collecting, processing, storing, disseminating and managing information on demand to warfighters, policy makers, and support personnel. The GIG includes all owned and leased communications and computing systems and services, software (including applications), data, security services, and other services necessary to achieve information superiority. It provides capabilities from all operating locations, including bases, posts, camps, stations, facilities, mobile platforms, and deployed sites.

The Watch Officer in the Pacific Command Theater C4ISR Coordination Center (TCCC) during the Y2K rollover.

The GIG initiative is divided into three “thrust” areas: resourcing the enterprise, aligning the technology base, and enterprise operations. Enterprise operations are composed of computing and communications (networks, computing, and interoperability) and enterprise management (network management, information dissemination management, and information assurance). Guidance and policy memorandums have been created for each of the three thrust areas.

Network Operations

Network operations (NETOPS) is a Joint Chiefs of Staff (JCS) C4 (JCS/J6) initiative to institutionalize networks as a warfighting resource under CINC combatant command authority. At its heart is an organizational, procedural, and technological construct for ensuring information superiority and enabling speed of command for the warfighter. NETOPS will link widely dispersed network operations centers through a command and organizational relationship; establish joint tactics, techniques, and procedures to ensure a joint procedural construct; and establish a technical framework to create a common network picture for the Joint Force Commander. Functionally, NETOPS is a theater-wide approach to providing assured network access, assured information and network protection, and assured information delivery at the strategic, operational, and tactical levels through a coevolution of doctrine, processes, and technology. The goals of JCS/J6 NETOPS are as follows—

- Establish C4I network management and network defense as ongoing military operations
- Provide the unified CINCs with network situational awareness
- Implement control and management capabilities that achieve end-to-end distributed control while providing a common view and joint use of network management information
- Implement positive control over, and security of, networks through a network operations hierarchy
- Provide the unified CINCs with authoritative direction over network resources, in coordination with Defense Information Systems Agency (DISA) and the Service Components of the Unified Command, as a function of the GIG.

Theater Network Operations is the ASD/C3I and JCS/J6 pilot program established to develop the organizational, procedural, and technological construct for implementing NETOPS across the U.S. Pacific Command (USPACOM) area of operations. The implementation of NETOPS at USPACOM is already providing lessons concerning the proposed constructs, it will also assist in determining resource implications for managing the operational environment in this manner, with an eye to applying similar concepts and lessons across DoD. A primary goal of USPACOM NETOPS is to operationalize and professionalize the network by using a tiered command relationship within the combatant commander's Theater Information Grid (TIG).

NETOPS Functional Elements

Network operations is defined as the ability to monitor, coordinate, manage, and control the GIG through a three-tiered command hierarchy. It comprises three mission areas: telecommunications network management (TNM), for assured network availability; information assurance (IA), for assured information protection; and information dissemination management (IDM), for assured information delivery to the right person, at the right place, at the right time. This comprehensive ability will manifest itself in an organizational, procedural, and technological framework that allows the CINC J6 to effectively execute CINC priorities while fulfilling tasks identified to sustain the GIG.

Telecommunications Network Management (TNM)

TNM includes the range of transmission systems, wired and wireless, that carry voice, data, and video throughout the theater. It includes switched networks, Internet Protocol (IP) based data networks, video teleconferencing (VTC) networks, satellite communications (SATCOM) networks, wireless networks, and intelligence community networks that support intelligence, surveillance, and reconnaissance functions. The major components of TNM are network management, SATCOM management, and frequency spectrum management.

- Network management comprises all measures necessary to ensure the effective and efficient operation of networked systems. The goal of network management is to provide the services and applications of a networked system with the desired level of quality and to guarantee availability and a rapid, flexible deployment of networked resources. Network management comprises the functions of fault, configuration, accounting, performance, and security (FCAPS) management.
- SATCOM management is the day-to-day management of all apportioned and nonapportioned SATCOM resources, including appropriate support when disruption of service occurs.
- Frequency spectrum management ensures that the CINC and subordinate commanders have cognizance over all spectrum management decisions that affect the area of operations. Spectrum planning and management involve the efficient employment of the electromagnetic spectrum, including acquisition, allocation, assignment, protection, and utilization of radio frequency resources. This includes cognizance over the automated distribution of management products, such as the Joint Standard Operating Instructions (JSOI). This function is performed by all military Services, sub-unified commands, and JTFs. Planning at the installation level at overseas locations frequently includes host nation coordination.

Information Assurance (IA)

IA capabilities help ensure the availability, integrity, identification, authentication, confidentiality, and nonrepudiation of friendly information and information systems while denying the adversary access to the same information and systems. These capabilities reside throughout the TIG. As a subset of Defensive Information Operations (DIO), IA includes providing for restoration of information systems by incorporating protection, detection, and response capabilities. Protection capabilities include communications security (COMSEC), computer security (COMPUSEC), and information security (INFOSEC) devices such as network guards and firewall systems that are used by all transport and service providers in the theater. Detection includes the ability to sense abnormalities in the network through use of intrusion detection systems. Timely attack detection is key to initiating network restoration and response capabilities. Response incorporates restoration as well as other information operations response processes. Capability restoration relies on established mechanisms for prioritized restoration of the minimum essential networks.

Information Dissemination Management (IDM)

IDM provides the right information, at the right place, at the right time, in accordance with the commander's policies and optimizing use of information infrastructure resources. It is a subset of information management that addresses awareness of, access to, and delivery of information. IDM involves the safeguarding, compilation, cataloging, storage, distribution, and retrieval of data; manages information flow to users; and enables execution of the commander's information policy.

IDM divides information into two types: planning and survival. Planning information is used to determine future action and is generally not time sensitive. It is used by planners and decision makers throughout the battlespace and is normally stored in databases, Web pages, or files. Survival information is extremely time sensitive and requires immediate action, such as attacking the enemy, avoiding attack, and preventing fratricide. Survival information is normally forwarded over tactical networks and datalinks to tactical commanders and individual weapon systems.

NETOPS prescribes a tiered organizational task structure corresponding to the levels of war established in the Universal Joint Task List (UJTL): National, Theater, Operational, and Tactical. This approach provides a network C2 structure that corresponds to existing C2 structures for operational forces in the theater. However, the following core capabilities should exist at each level: a C2 capability that can respond to and report network outages and attacks; the ability to operate and manage the information transport infrastructure; the ability to operate and manage information flow; and the ability to operate and manage information and network defense systems.

NETOPS Implementation

"Information is like eggs, the fresher the better."

—General George S. Patton

"The central problem is not collecting and transmitting information, but synthesizing it for the decision maker."

—Richard Burt, former Ambassador to West Germany and former Assistant Secretary of State for Europe

Approach

USPACOM NETOPS implementation is based on a spiral, phased development approach with three planning horizons: near-term, mid-term, and far-term. Near-term planning focuses on achieving essential operational capabilities (i.e., the ability to perform today's mission to support the CINC and JTF commanders). Tasks in this planning phase are stop-gap measures to obtain situational awareness over the theater information grid and to implement a command relationship over subordinate network operations centers. Mid-term planning focuses on achieving the desired operational capabilities described in Joint Vision 2010 Information Transport and Processing. This phase employs a network-centric approach to bring together the disparate technologies and capabilities in a coordinated manner. Far-term planning aims to achieve Revolution in Military Affairs (RMA) related capabilities and focuses on current Defense Advanced Research Projects Agency (DARPA) technology and planned process reengineering to create an enterprise-wide network operations and security capability. The goal is a knowledge-centric capability that will allow the CINC to command the TIG. Implementation of PACOM Theater Network Operations links near-term essential operational needs to far-term future operational capabilities in each of the NETOPS functional areas: telecommunications network management, information assurance, and information dissemination management.

Near-Term Goals and Objectives

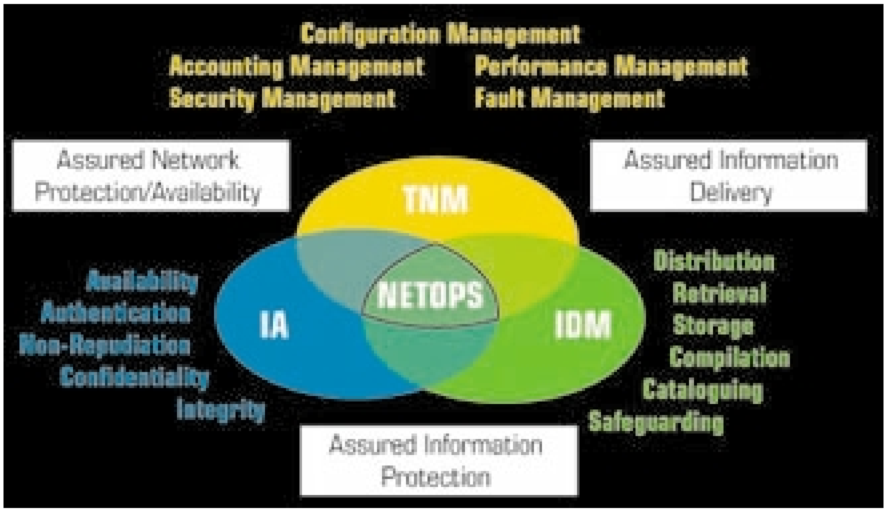
The near-term (0 to 18 months) goal is to make network, IA, and information application status visible to the CINC. The principal focus in this phase is to create a network common operational picture (NETCOP) that provides end-to-end visibility of mission-critical networks and information systems. The near term phase focuses on incorporating existing organizations and procedures into a coordinated theater-wide capability. The near term relies heavily on leveraging existing technologies (either already in place or programmed for fielding) to provide an essential operational capability within an 18-month planning horizon. Near-term objectives are as follows—

- Create a common view of theater-wide network, IA, and application (Global Command and Control System [GCCS]) status through a NETCOP **(Observe)**
- Implement the ability to quickly understand potential operational impacts of network outages, degradations, and attacks through a TIG mission-critical database **(Orient)**
- Develop course-of-action techniques to aid in the decision-making process **(Decide)**
- Institute a C2 mechanism to coordinate theater-wide response to network outages, degradations, and attacks **(Act).**

Mid-Term Goals and Objectives

Mid-term (0 to 36 month) goals are to implement the desired operational capabilities established by Joint Vision 2010: defend against information assurance (IA) threats; provide the warfighter with a flexible, adaptable network for transmitting and receiving the right volume of information at the right time and the right place (TNM); and manage an assured, real-time, scalable information flow throughout the infrastructure (IDM). The aim is to create a network-centric infrastructure that uses interoperable network and information management and protection tools and employs standard processes to enable near-real-time collaboration and response capabilities. Mid-term objectives are as follows—

- Create an integrated view of network, IA, and C2 application status through the integrated NETCOP (I-NETCOP) **(Observe)**



- Link the TIG mission-critical systems database to I-NET-COP **(Orient)**
- Develop semi-automated course-of-action decision-support tools to decrease decision time and increase decision accuracy **(Decide)**
- Implement a virtual collaboration capability linking geographically dispersed network managers to decrease implementation time (Act).

Far-Term Goals and Objectives

Far-term (0 to 60 month) goals are to implement future operational capabilities that enable knowledge-centric enterprise information management and protection capability across the theater. This capability includes seamless and interoperable network, IA, and information visibility using standardized tools and enterprise-level processes. The ability to command the theater information grid is predicated on the ability to merge planning and survival information management through an enterprise-wide network and information management system. Far-term objectives are as follows—

- Create an integrated view of network, IA, application, and operational (GCCS) status that is scalable and accessible across the theater at all echelons **(Observe and Orient)**
- Integrate automated course-of-action decision-support tools and virtual collaboration systems to support a near-real-time analysis and collaboration capability **(Decide and Act).**

Conclusion

"All successfully adapting systems have something in common: they transform apparent noise into meaning faster than apparent noise comes at them."

—Stephan Haeckel, Director of Strategic Studies, IBM Advanced Business Institute

The ability to implement a joint communications grid with adequate capacity, resilience, and network management capabilities to support the operational concepts of Joint Vision 2010 is key to achieving information superiority. As recent operations in the Middle East (Desert Fox), Europe (Kosovo), and the Pacific have demonstrated, the lack of real-time visibility and control of networks, manual and latent network management capabilities, and a fragmented IA architecture have emerged as significant operational challenges to support of the warfighter. NETOPS is an attempt to provide organizational, procedural, and technological solutions to these challenges, in order to achieve information superiority.

The basic goal of NETOPS is to improve overall performance through more timely reporting and responses to network attacks and failures, enhanced situational awareness of network and IA status, and improved decision making. These collective improvements should increase the effectiveness, efficiency, and robustness of the GIG. NETOPS will ensure greater coordination, management, and control capabilities that will allow end-to-end distributed control while providing a common view and joint use of theater information processing and transport assets.

Brigadier General (P) James D. Bryan is the Commander, JTF–CND and Vice Director for DISA. He was most recently Director for Command, Control, Communications and Computer Systems, USPACOM, Camp H. M. Smith, Hawaii. He graduated from Jacksonville State University with a B.S. in Education and was commissioned as a Second Lieutenant in the Regular Army. He earned his Master of Adult Education degree from North Carolina State University and was inducted into the Phi Kappa Phi National Academic Honor Society.

Patrick Gorman is a Program Manager for the Pacific Network Operations initiative at Camp H.M. Smith, Hawaii. He graduated with a B.A. from the University of Maryland and an M.A. from the George Washington University. He may be reached at gorman_patrick@bah.com

Endnote

1. Statement before the Senate Armed Services Committee Subcommittee on Emerging Threats and Capabilities: Information Warfare and Critical Infrastructure Protection.

A Retrospective on Computer Network Defense

Major General John Campbell, USAF
Central Intelligence Agency

I recently relinquished command of the Joint Task Force–Computer Network Defense (JTF-CND) to Brigadier General (P) James D. Bryan, U.S. Army. Dave's dual assignment as CJTF-CND and Vice Director for the Defense Information Systems Agency (DISA) follows his most recent assignment as the J6 for U.S. Pacific Command (PACOM). With his communications background and recent experience in a command with one of the most active information assurance (IA) programs in the Department of Defense (DoD), Dave is exactly the right person to take command of the JTF-CND. As I leave, I thought it would be worthwhile to share some of my observations about where we've been, where we are, and where we need to go to continue to strengthen DoD's cyber defenses.

We have made some real progress in the past 2 years. To use a tired metaphor, the glass is definitely more than half full; but the empty part represents a significant challenge. Although I am convinced that the real threat we must prepare for remains the organized, structured, well-resourced state-sponsored attacker, it is clear that the danger from the individual hacker is increasing and represents a real concern for the security of DoD networks. We are increasingly seeing sophisticated tools and techniques that can not only cause significant damage in their own right but also cause us to adopt defensive measures that amount to self-inflicted denial of increasingly critical network services.

I would like to take a moment to look back at some key events that have shaped DoD's approach to this mission area and at some of the significant decisions resulting from those events. For good or bad, we have made progress in DoD, primarily when events have demonstrated that a serious threat exists. But even in these cases, progress has not come easily. Determined leadership by a few key individuals—most of all, former Deputy Secretary of Defense (DEPSECDEF) John Hamre—has helped us overcome organizational inertia and institutional bias, which have slowed development of an effective DoD-wide defensive structure.

Watershed Events

Although our cyber vulnerabilities had been recognized before, exercise ELIGIBLE RECEIVER 97 (ER97) in June 1997 clearly demonstrated our lack of preparation for a coordinated cyber and physical attack on our critical military and civil infrastructures. The timing of ER97 resulted in incorporation of many of its observations into the October 1997 Report of the President's Commission on Critical Infrastructure Protection (PCCIP). This report recognized the growing vulnerabilities of the nation's critical infrastructures, including telecommunications, banking, transportation, and government services. The PCCIP report also influenced the development of Presidential Decision Directive 63 (PDD-63) in May 1998. PDD-63 set goals for securing the national infrastructure, established a national structure to manage challenges, recommended a national center to "warn of and respond to attacks," required the Government to serve as the model, and sought voluntary private-sector participation in critical infrastructure protection.

The observations of ER97 and the PCCIP were reinforced in February 1998 when a series of cyber intrusions called *Solar Sunrise* generated significant concern about the security of DoD's networks. Although these intrusions were eventually traced to teenage hackers in northern California, *Solar Sunrise* clearly demonstrated the reality of what previous exercises and studies had predicted. Most important, *Solar Sunrise* clearly demonstrated that we had not answered the basic question "Who's in charge of the defense of DoD networks and systems?"

Several significant decisions resulted from these events. In the interagency arena, PDD-63 laid the foundation for the formation of the National Infrastructure Protection Center (NIPC). NIPC is sponsored by the Department of Justice (DOJ) and the Federal Bureau of Investigation and includes representatives of DoD and other departments of the Federal Government. Although the NIPC has received some criticism for its law enforcement–centric approach, DOJ deserves credit for stepping up to the plate and sponsoring this badly needed capability. On the DoD side, staffing originating with the ER97 observations and reinforced by the *Solar Sunrise* activities, culminated, in December 1998, in a recommendation by the Chairman of the Joint Chiefs of Staff (CJCS), approved by the Secretary of Defense (SECDEF), to establish the JTF-CND. The SECDEF charter, signed December 4, 1998, tasked the JTF-CND with "coordinating and directing the defense of DoD computer systems and computer networks." The JTF opened its doors in December 1998 and achieved full operational capability in June 1999. While the JTF is physically located at DISA headquarters and DISA provides significant logistical and technical support, DISA is not in the JTF chain of command.

It is important to recognize that the JTF-CND was designed originally as a "gap filler" organization, that is, to quickly field a DoD defensive capability pending thorough staffing, via the Unified Command Plan (UCP) process, of the proper long-term responsibility for CND. As most know, UCP99 assigned the CND mission, effective October 1999, to the U.S. Space Command (USSPACECOM). Several organizational constructs were considered in building the USSPACECOM CND implementation plan. The Commander in Chief, U.S. Space Command (CINCSPACE eventually decided to retain the JTF-CND as his operational command for CND while building a long-term robust CND capability at Colorado Springs to perform strategic planning, analysis, and resource functions. It is worth noting that the JTF headquarters has relatively little organic capability, with only 24 authorized positions. We perform our mission by leveraging the capabilities of our components: the DISA Global Network Operations and Security Center (GNOSC), the DoD Computer Emergency Response Team (CERT), and our four service components. The components provide the real capability for reporting, analysis, and execution of remedial actions. Additionally, the augmentation provided to our intelligence and law enforcement sections has significantly improved our capabilities. Recognizing the significant activity under way at USSPACECOM headquarters, I would like to briefly discuss the progress of the JTF-CND and offer some observations about the state of the CND mission.

Successes

JTF-CND provided DoD with a focal point for dealing with cyber threats and answered the "Who's in charge?" question. During the *Melissa* virus incident in March 1999, the JTF-CND, in cooperation with the DoD CERT was able to quickly assess the threat, develop a defensive strategy, and direct appropriate defensive actions. Where damage to the private sector totaled in the hundreds of millions of dollars, DoD experienced relatively little effect and no operational impact. After USSPACECOM's assumption of command of the CND mission, two other events demonstrated the value of centralized responsibility and authority. The February 2000 Dis-

tributed denial-of-service (DDOS) attack, which by most estimates slowed the Internet by 20 percent and shut down a number of the most popular Internet sites, including Yahoo, E-Bay, among others, and the May 2000 *Loveletter* worm, estimated to have cost billions worldwide. These attacks vividly demonstrate the increasing ability of an individual hacker to cause significant damage to the worldwide cyber infrastructure. In the case of the DDOS event, DoD was not directly targeted, but the organization we have developed allowed us to maintain situational awareness of the attacks' progress and to ensure that we understood the status of DoD systems. In the case of *Loveletter,* although we were initially caught off guard by the speed of the developing attack, we were able to provide CINCSPACE with an assessment of the situation and to direct proper remedial actions to minimize damage to DoD. In this case, as in the *Melissa* incident, DoD suffered no operational impact, although significant numbers of DoD users suffered self-inflicted denial of service because of initial actions, including disabling E-mail services and disconnecting from the Internet. The *Melissa*, DDOS, and *Loveletter* incidents clearly demonstrate the increasing threat that individual hackers represent to DoD's business processes and even its command and control systems.

In consideration of this threat environment, I would like to offer some thoughts on the current state of CND and where we need to improve.

CND Is a Partnership

Effective CND must be a partnership between network operations, law enforcement, and intelligence. Before 1998, these communities operated independently, with little strategic perspective or coordination. The formation of the JTF-CND provided a nexus for cooperation and an operational focus, and assignment of mission responsibility to CINCSPACE further emphasized the importance of our networks as weapons systems. The intelligence and law enforcement communities have invested significant resources in the CND mission, and the command, control, communications, and computer (C4) community is emphasizing the network operations (NETOPS) concept, which gives regional warfighters greater visibility and control over their networks. We need to make sure this partnership remains balanced—too much emphasis on one area will come at the expense of others. Within the JTF-CND, we have a law enforcement/counterintelligence center, which is staffed full-time by representatives of the service and defense law enforcement organizations. We also maintain a robust intelligence section, with liaison officers from the Defense Intelligence Agency and the National Security Agency who can tap the resources of the intelligence community. These resources and capabilities, combined with the NETOPS expertise of DISA's Global Network Operations and Security Center and the DoD CERT, give us an effective CND team.

Senior Leadership Emphasis Is Critical

Effective CND is hard work. It requires people and effort, and competes with other activities. In this process, the NETOPS/intelligence/law enforcement team will, properly, respond to the priorities established by senior leadership. I am encouraged by the emphasis that senior uniformed and civilian leadership of the department—from the CJCS and service chiefs, through the senior communicators, to field commanders—are placing on such things as Information Assurance Vulnerability Alert (IAVA) compliance and the Information Operations Condition (INFOCON) process. As an example, the Air Force now treats network incidents like aircraft accidents, with a formal investigation and a report to the responsible commander. This process recognizes the critical nature of our information systems by treating them like other weapons systems and providing commanders with the same degree of visibility and control.

The Role of Law Enforcement and Counterintelligence

Law enforcement and counterintelligence have critical roles in DoD's computer network defense. Because the law assumes that an intruder into DoD systems is a U.S. citizen and is entitled to the rights provided by U.S. law and the Constitution, almost every cyber incident is initially investigated as a law enforcement problem. Although this does not prevent DoD from taking aggressive action to protect its networks and systems, it does limit the role of intelligence agencies and requires investigative actions to be conducted in accordance with the laws protecting individual rights. This makes a close relationship with the law enforcement community very important to the nation's overall CND effort. Recognizing this need, DoD's Defense Criminal Investigative Organizations [Air Force Office of Special Investigations (AFOSI), National Crime Intelligence Service (NCIS), Defense Criminal Investigative Service (DCIS), U.S. Army Criminal Investigation Department (USACID), and U.S. Army Military Intelligence (USAMI)] volunteered to provide a team of law enforcement officers and counterintelligence officers to staff a law enforcement/counterintelligence center at JTF-CND headquarters. With the exception of one rotating officer who acts as a liaison to the CJTF, the law enforcement/counterintelligence team members report individually to, and receive direction from, their service command structures and maintain the confidentiality required by their investigative processes. The Law Enforcement/Counterintelligence Center allows us to coordinate overall activity, maintain awareness of the progress of investigations, and coordinate activities across multiple services and agencies. The law enforcement expertise that these officers provide also give us a much closer relationship with NIPC than we would otherwise have had. The law enforcement/counterintelligence relationship is one of the real success stories of the past year.

The Threat Environment

The most recent DDOS and virus incidents are a "good news/bad news" story. The bad news is that these incidents happen, and they are incredibly fast and destructive. The good news is that we have a process for responding to such incidents and that our response is improving. Despite the good news, we need to take several steps to better position ourselves for responding to fast-spreading viruses and other attacks.

- **Early Warning—**We need an early-warning network designed to detect and report events, like viruses, that are likely to "follow the sun" or spread westward with the workday. One way to do this is to use the Y2K model, with organizations in the western Pacific and Europe acting as the early warning sensors. This early warning capability will provide us with a few hours of preparation time before the start of the business day in the continental United States.
- **Rapid Notification—**We need a way of rapidly notifying DoD organizations of significant cyber events, just as we do for other time-sensitive events. A quick-reaction teleconference system is probably the answer, and in fact, USSPACECOM is developing such a process. In addition, if we are to be prepared for serious virus events, we must also be prepared for some false alarms.
- **Involving the Private Sector—**We need to involve the private sector in the early warning process. Just as DoD has worldwide organizations that can serve as early warning sensors, so do many private sector organizations with global operations.
- **Virus Protection—**We need standard virus protection measures that we can invoke in response to viruses. One thing we should not do is preemptively disconnect E-mail systems or sever access to the Sensitive but Unclassified Internet Protocol Router Network (NIPRNET). Because more and more of our administrative and support systems depend on E-mail connectivity, disconnecting from these systems amounts to a self-inflicted denial of service, which should be used only in extremes.

We need more applications that are more virus resistant and better awareness of the virus threat. A few software improvements, such as controlling mass E-mailings, would go a long way toward preventing the spread of viruses.

Private Sector Information Sharing

Government and the private sector need the ability to share information about ongoing attacks, system status, and defensive and remedial actions, for several reasons. First, we need to work together to enable early detection of viruses and worms, where a quick reaction is critical to damage limitation. Second, we need to exchange information in order to assess the scope and intent of a cyber attack. ER97 demonstrated the interrelated nature of the infrastructures of DoD and the private sector. We need to be able to rapidly understand the "big picture," spanning both the federal and the private sectors. Third, DoD shares common systems and common vulnerabilities with the private sector, including an increasing reliance on Web-based communications and commercial software systems. Finally, we in DoD must be able to pool resources with the private sector to develop defenses when a cyber event occurs. The Information Sharing and Analysis Center (ISAC) concept laid out in the national PPCIP plan is a start; today we have ISACs for banking and finance and telecommunications, and we are developing close bilateral relationships with them. But ISACs are needed for all the critical infrastructure sectors, with an aggressive information-sharing process through the NIPC. Some new legal protection, like that provided for the Year 2000 (Y2K) rollover, may be required for the participating ISAC members. There is legislation pending that would provide this.

CND versus CNA

As we allocate scarce resources between computer network attack (CNA) and CND, we need to ensure we tackle the basics first. While CNA holds out great long-term possibilities, we need to get the CND piece right first. My reason for this viewpoint is twofold. First, while we can pick the time and place for execution of CNA, we have to protect our networks, across the Defense Information Infrastructure (DII), all the time. Second, the consequences of failure are greater for CND than for CNA. Today, CNA is a marginal, albeit growing, capability, and the failure to execute it well, or at all, will not be a deciding factor in the next conflict. However, our ability to mobilize, deploy, and employ our combat forces depends on the computer networks of the DII. Command and control, logistics, transportation, medical, personnel, and general administrative and support systems depend on the connectivity provided by the DII networks. Failure to defend them carries the risk that we will not be able to get our forces to the fight, employ them once they are engaged, or support them in the field.

That said, CND and CNA are inextricably related, and to do either well requires an appreciation of the other. Therefore, I believe it is important to maintain a close relationship between these areas. First, the techniques we use as offensive tools may someday be used against us, so offense and defense must be coordinated. We can do a better job of defense if the defenders understand offensive tools and techniques. In addition, we eventually will need to expand our defensive capabilities to include active defense, or counteroffensive tools capable of taking the fight back to the attacker. Today, legal and policy restrictions limit our ability to use even the limited technical capabilities we possess, but eventually, as those capabilities improve, we will need a commensurate operational command and control structure, and an appropriate legal and policy environment.

Policy and Regulatory Requirements

The legal and policy environment in which we operate is complex and constantly evolving. Lt Col Charlie Williamson, my Staff Judge Advocate, recently published an article in the *IAnewsletter* (Volume 3, Number 1) that provides a good overview of this sensitive area. Some imperatives are immediately obvious. First, we need international agreements for expeditious pursuit of those who have violated the law. Second, we need authorities to allow law enforcement agencies to rapidly conduct electronic surveillance of those involved in cyber attacks. We also need legislation to encourage information sharing between the Federal Government and the private sector, in particular to protect proprietary information and shield sensitive information from Freedom of Information Act (FOIA) requests. Finally, in DoD, we need to work with the policy and legal process to secure a more active electronic defense, including appropriate rules of engagement. We have been actively involved in discussions with DOJ since ER97, and several legislative initiatives are on the Hill today, so we are making progress, but slowly.

Common Operational Picture (COP)

As we operationalize and normalize CND, we will have an increasing need to provide the warfighter with a real-time picture of the electronic battlespace so that he or she can understand and visualize the status of networks and quickly develop and execute courses of action to defend them. We have called this effort the information assurance common operational picture (IA COP), and more modestly, the IA situational awareness tool. Under DISA direction, we will be ready to incorporate some initial situational awareness tools into the

Global Command and Control System next year. This is a small step; much work—and considerable resources—must be expended to develop an IA COP for the warfighter of the future.

Information Operations Condition (INFOCON)

The Joint Staff instituted the INFOCON process last year. This is clearly a step in the right direction. INFOCON gives us a means of reacting defensively under attack, or proactively to set a DoD-wide defense condition when the indications and warning process indicates a developing threat. We have exercised INFOCON a few times and found that, while the basic process is sound, there is considerable room for improvement in several areas. First, we need to flesh out the measures to provide more specificity. Second, we need to develop more specific criteria for entering and exiting each INFOCON level. Finally, we need to understand the cost and mission impact of more advanced INFOCON levels. We cannot afford to routinely implement a self-imposed denial of service as a defensive measure. USSPACECOM has taken on the challenge of improving the INFOCON process and held a DoD-wide conference in June to address these issues. INFOCON is the right tool; we just need to improve and exercise it.

An issue related to INFOCON is the vulnerability of the NIPRNET and the Secret Internet Protocol Router Network (SIPRNET) to intrusions from the Internet. I have frequently heard suggestions that DoD should disconnect from the Internet, either permanently or as a defensive measure in the event of an attack. It has become apparent, however, that many of our mission-critical SIPRNET and NIPRNET systems—for example, the Global Transportation Network—receive information from the Internet. There are also technical questions, since some DoD "dot.mil-to-dot.mil" traffic in fact flows through the Internet. We need to improve our understanding of the dependencies and technical network factors and develop some basis for decision making in this area. We then need to test the disconnection process before we adopt this as a defensive tool. DISA is currently conducting a study to answer some of these technical questions.

System Administration and Configuration Control

The IAVA process was developed in 1998, at the direction of the DEPSECDEF, when it became apparent that we had no way of rapidly implementing time-critical system patches across DoD and providing control of compliance. Today, the IAVA process, run by DISA, provides a way of achieving these ends. Unfortunately, the process has still not completely penetrated DoD. An analysis of 1999 root-level intrusions in DoD shows that 94 percent of the intrusions could have been prevented if accepted security practices had been followed and existing IAVAs had been implemented. In other words, although we are better off than we were a year ago, we must do better. Making the needed improvements will require command emphasis, since IAVA compliance competes with other mission-critical activities for the time of our system administrators. There have been promising developments in this area. In June CINCSPACE assumed responsibility for the IAVA program. In addition, CJCS recently directed "commanders at all echelons" to emphasize IAVA compliance.

Conclusion

I remember all too clearly sitting in the DEPSECDEF's conference room in February 1998 during the Solar Sunrise discussion and being asked the basic question I asked earlier in this article: "Who's in charge?" We have come a long way since then. We have someone in charge (CINCSPACE) and the beginnings of a proper defensive force. In October, USSPACECOM will assume the CNA mission and begin developing a robust offensive force to complement our defensive capability. The future is truly exciting. We just need to keep our eye on the ball and ensure that we properly support this developing mission area. I wish all of you in the CND/IA mission the very best of luck.

Maj Gen John Campbell was commissioned through the Air Force Reserve Officer Training Corps in 1969 at the University of Kentucky. He is a command Pilot with more than 3600 flying hours and has commanded a fighter squadron, a fighter group, and two fighter wings. He was the first Director of Information Operations on the Joint Staff, and was assigned as the Commander of JTF-CND and Vice Director, DISA in November 1998. On 9 June 2000, he assumed duty as the Associate Director of Central Intelligence for Military Support in the Central Intelligence Agency.

U.S. Special Operations Command Builds New NOSC

Major John J. Jordan, USA
U.S. Special Operations Command

Recognizing that advances in computer and security technology require nearly simultaneous advances in the monitoring capability of the new technology, the U.S. Special Operations Command (USSOCOM) recently rebuilt its Network Management Office into a Network Operations and Security Center. The NOSC, as it is called, monitors USSOCOM's local area networks, wide area networks, and network security.

What separates the USSOCOM NOSC from other NOSCs in the Department of Defense (DoD) is the fact that it monitors networks at all classification levels. USSOCOM is the first command in DoD to combine intelligence systems and common user systems under one organization. This groundbreaking combination has given users in all communities true "one-stop shopping" for their computer and communications needs and has enabled DoD to achieve dramatic savings in money and manpower.

Before their unification under the NOSC, two entire computer staffs ran USSOCOM's systems. This meant two sets of systems administration contracts, two hardware maintenance contracts, two processes for configuration management, and two processes for information assurance. By combining these efforts, USSOCOM was able to develop one systems administration and systems engineering contract and one server hardware contract and to combine both configuration management and information assurance processes to satisfy all users. This consolidation allowed immediate savings of $1.3 million in contract support costs and reduced the size of the staff for running the systems by over 30 persons. While joining two staffs that had been separate forever was not without its growing pains, the final product has been a smaller staff with no decrease in customer service.

The security section of the USSOCOM NOSC was developed in response to DoD's increased emphasis on security issues. USSOCOM is extremely serious about the security, not only of its forces, but also of the information its forces require to carry out USSOCOM missions. In the information assurance arena, USSOCOM is proceeding with its defense-in-depth program on all of its networks. The NOSC is a focal point of this effort. USSOCOM's strategy for security is to defend the outside of these systems as well as the inside.

To defend the outside of USSOCOM's three networks, the command uses a variety of monitoring hardware and software designed to greatly reduce unauthorized users' ability to gain access to system resources. Firewalls, access control lists, monitors, and sensors placed in strategic network locations provide much of USSOCOM's defense against outside attack. The NOSC provides a single, 24-hour watch cell for monitoring this defense strategy.

USSOCOM also realizes that attacks on, and unauthorized access to, computer systems can be caused by people on the inside. To help prevent insider damage to its systems, USSOCOM uses a combination of training and security procedures. For example, password "cracking" is one of the easiest

continued on page 24

Where There's Smoke, There's Fire...

Brian Bottesini, NAVEUR
Brenda Angerhofer, NAVEUR

When we were young, many of us dreamed of becoming doctors, firefighters, at least in a metaphorical sense. This is especially true in the information technology (IT) world, where technology changes every day and IT managers routinely face new challenges and "fires" to put out. Just keeping the network up and running involves putting out daily brush fires to prevent a conflagration.

In the world of information assurance (IA), we have seen a continuing battle between the defenders of our networks and those who intend harm. IA professionals must constantly defend networks from viruses, intrusions, probes, and other harmful activities, whether these are caused by malicious "arsonists" or just someone playing with matches. Effective IA fire prevention and fire fighting involve identifying the threats, applying effective countermeasures, and understanding and accepting the remaining risk to our systems.

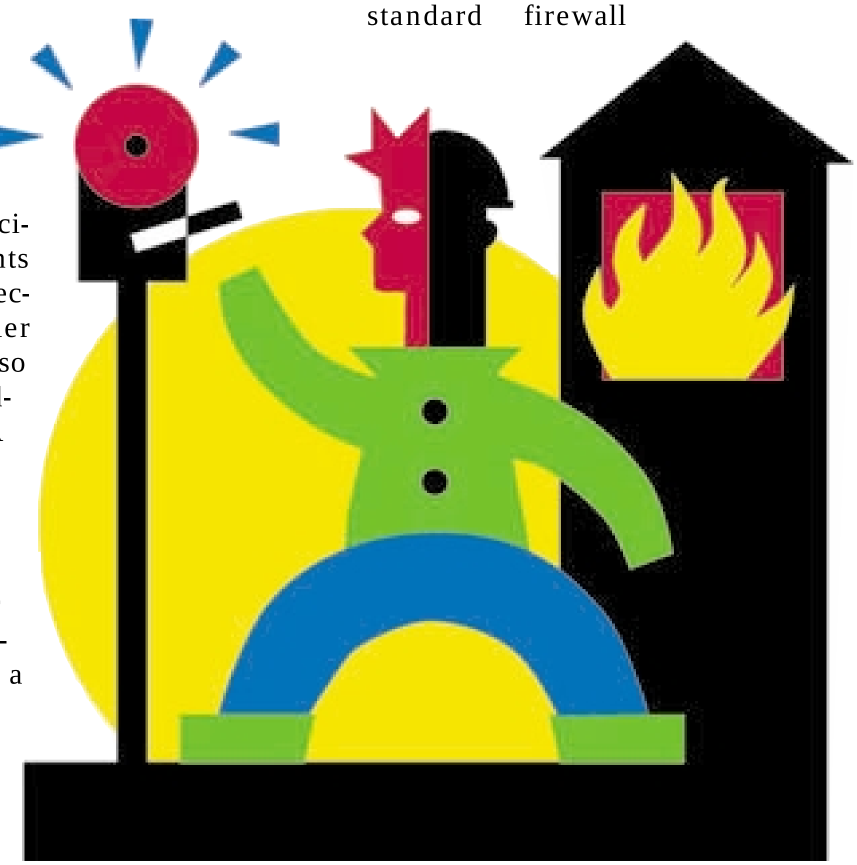
No computer network is completely fireproof. In fact, some say that the only truly safe computer is the stand-alone computer locked in a closet, an arrangement that offers exceptional security but little utility. IA professionals must carefully weigh the needs of their operations against the need for smart security mechanisms. One of the most common IA mechanisms in use today is the firewall. A firewall is a system designed to prevent unauthorized access to or from a private network.

Although the firewall is an excellent security defense mechanism, by itself it is a Maginot Line defense. To be effective, the firewall must be part of a much broader IA architecture that includes several layers of security, including antivirus applications, intrusion detection systems, content filtering, physical and personnel security, and other elements. The U.S. Navy's and Marine Corps' defense-in-depth strategy defines such an overall security architecture with multiple layers of assurance mechanisms.

The Fire Code

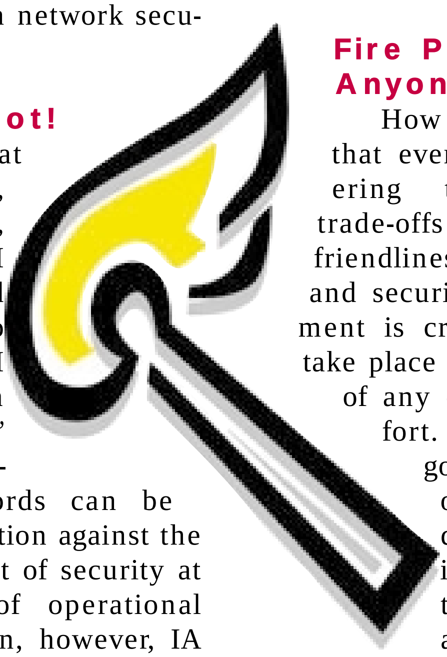
To protect against actual fires, the United States has instituted a standard fire code that specifies requirements for smoke detectors, sprinkler systems, and so on. Why shouldn't we in the IA community have a similar standard for the firewalls defending our networks in cyberspace? Such a standard would address what services are allowed and what are not, how firewalls should be configured when they are connected to the NIPRNET (Sensitive but Unclassified Internet Protocol Router Network) and the SIPRNET (Secret Internet Protocol Router Network), and other critical issues.

We know that a chain is only as strong as its weakest link. Similarly, multiple interconnected networks and firewalls can offer sound protection only if all the firewalls prohibit risky services. Recent events in the news have illustrated the vulnerability of unprotected computers to unauthorized intrusions. Because there was no standard firewall



policy, the U.S. Navy Fleet Commanders in Chief (CINC) implemented a standard fleet firewall policy for all fleet network operations centers, pierside firewalls, and selected shore activities (see http://www.infosec .navy.mil). This policy seeks to standardize the outer layer of computer network defense and is integral to the Navy's and Marine Corps' defense-in-depth network security strategy.

Hot, hot, hot!



The great American poet, Robert Frost, said, "Before I built a wall I'd ask to know/What I was walling in or walling out." In the IA context, these words can be viewed as a caution against the mindless pursuit of security at the expense of operational needs. Too often, however, IA professionals are required to support an application that relies on inherently risky services. Several examples have surfaced recently in which a fully developed software application has shown up on the doorstep of a command, awaiting installation. These "programs of record" are often designed with maximum accessibility in mind and minimum to no security controls. To work properly, these applications require lots of big holes in the firewall. This requirement puts the local Information Systems Security Manager and Designated Approval Authority (DAA) in a difficult position. The local command needs to run the application to do its job, but implementing the application as-is introduces risk to the entire command's information networks behind the firewall. Before such risky programs are implemented, the following questions should be considered: What is the value of opening those holes in the firewall? What is the risk to the rest of the network? Is there a possible compromise?

Fire Prevention Anyone?

How can we ensure that everyone is considering the necessary trade-offs between user friendliness, accessibility, and security? This assessment is critical and must take place at the very start of any development effort. As the saying goes, "It's a heck of a lot easier to design security into an application than it is to add security later on." Although, occasionally, it may be possible to paste on a little security late in the project, all too often doing so is very costly and cumbersome. Thus, information systems must address IA requirements and policies early in development, and before fielding into operational networks.

Recently, more than 20 programs of record were identified that conflicted with the current Fleet firewall policy. Is the policy too restrictive? Are the programs of record poorly designed? Although the answers to these questions are still being debated, one thing is clear: there have been known attacks on information networks when certain services, such as RPC and ActiveX, were permitted to pass unchecked through a firewall.

To mitigate the risks of incorporating these programs into our information networks, we must work closely with the programs' program managers. These program managers must provide the DAA with sufficient documentation to enable him or her to make an informed decision about implementing the new application on the local network. Documentation, such as an accreditation package, system security authorization agreement, risk assessment, and transition plan, will all help in delineating the proposed architecture and assessing the risks. In addition, the local site may require system security engineering before the program of record is integrated into the existing site configuration. Another approach could involve the use of virtual private networks implemented in parallel with existing firewalls, thereby allowing flexibility without compromising security.

As this discussion has shown, there are few easy answers for the IA professional today. As Quintus Horatius Flaccus said about 2000 years ago in his Epistles, "It is your concern when your neighbor's wall is on fire." Thus, for the foreseeable future, IA fire fighting and prevention will require much painstaking work and constant vigilance. In other words, we cannot just ride on the back of the fire engine.

Brian Bottesini is an Information Assurance Advisor to U.S. Naval Forces, Europe. He may be reached at cnen67@naveur.navy.mil

Keys to the Kingdom

Captain Robert West, USN
Deputy Commander, JTF–CND

Not so long ago, the Department of Defense (DoD) was at the forefront of information technology (IT) development. In fact, the Advanced Research Projects Agency Network ARPANET, which later spawned that unruly child the Internet, had its roots in DoD's rich history. When ARPANET was under development, DoD was leading the information IT revolution; however, that is no longer the case. Today, newly emerging information technologies are a part of every viable business enterprise and new technologies affect the lives of all Americans in ways that were unimaginable only a few years ago. The amazing growth in IT over the past several decades coupled with DoD's constantly shrinking budgets, has relegated DoD to the role of an IT consumer. It is simply a fact that we no longer enjoy the technical superiority we once had.

As a result of this decline and our increasing dependence on sophisticated high-tech networks for support of operations, we have become increasingly vulnerable to outside influence. For example, DoD, like the rest of the world, has become utterly dependent on the Internet. Whether supporting on-line contract bidding and execution, ensuring robust logistics support worldwide, or maintaining deployed troops with E-mail connectivity to family members back home, the Internet has become vital to how we conduct operations.

With these new dependencies has come an increasing awareness of major information and computer security issues. Let's face it, a system whose primary design feature is the ability for any computer in the world to rapidly and efficiently share information and processes with any other computer on the planet must have inherent security vulnerabilities. And that is the case with the Internet today.

As a major IT consumer, DoD invests heavily in information assurance (IA). The department has instituted a layered-in-depth strategy and is spending millions of dollars each year on sophisticated intrusion detection devices, high-assurance firewalls, symmetric and asymmetric encryption, strong authentication, and any other technologies that show promise.

Additionally, DoD has instituted a department-wide Information Assurance Vulnerability Alert (IAVA) program to patch existing technical vulnerabilities. Since the program's implementation in June 1998, 26 IAVAs have been published. These alerts have addressed a wide range of technical security issues for DoD networks. As a result of this program and other elements in our in-depth strategy, we should be close to achieving a reasonable level of security on our networks.

So why is it that outsiders continue to penetrate DoD networks on a routine basis? A recent statistic developed by the Joint Task Force for Computer Network Defense (JTF-CND) indicates that more than 90 percent of all successful intrusions into the Sensitive but Unclassified Internet Protocol Router Network (NIPRNET) in 1999 were accomplished by exploiting known vulnerabilities. In each case, state-of-the-art security devices were already in place and the exploited vulnerability had been identified and addressed with an IAVA. In fact, implementation of the existing IAVA would have prevented the unauthorized access—if only the patch had been installed at that location. The good news is that DoD's strategy is, in fact, identifying most technical security vulnerabilities. The bad news is that those responsible for implementing IAVA patches have not consistently done so.

Today, this security problem is compounded by the fact that almost all unauthorized accesses are prolonged by the intruders' use of additional exploitation techniques after he or she first gains access to an account. Whether the intruder gains initial access by exploiting an unpatched vulnerability, by gaining physical access to a protected location and stealing the necessary account data, by "sniffing" passwords on-line, or by scanning for never-activated accounts with still-active default passwords, the result is the same. The unauthorized individual achieves user status in the system, and from there generally has no trouble gaining system administrator or root privileges. Tools for gaining such privileges are readily available on the Internet today. Unfortunately, current intrusion detection capabilities have a difficult time distinguishing between authorized users and unauthorized users masquerading as legitimate. The experience of the JTF-CND in the past year supports this perception. With very few exceptions, initial incident detection has come, not from automated devices, but rather from system administrators who have detected unusual account activity at their site through detailed system log analysis or other means. Only after an initial report has been forwarded have we been able to "tune" the intrusion detection devices to help fill in the details about the nature of the abnormal activity and to assess whether there has been a coordinated or systematic effort directed against computers across DoD.

Although we should certainly continue to pursue technical solutions to security concerns, it should be abundantly clear that technical devices alone are inadequate for addressing DoD's ever-increasing security issues. It is time for DoD to shift its corporate focus a bit and begin addressing the most pressing security issue of all, our people. Our system administrators are the ones granting network access in the first place, in the form of user privileges. For this reason, they are the ones best positioned to distinguish between legitimate and illegitimate access. System administrators also are the ones charged with installing IAVA patches when new vulnerabilities are discovered. In short, they own the keys to the kingdom. It is time we recognize just how important this group has become to the success of any operation.

What we need now is a top-down DoD-wide network security policy that brings consistency to system administrator training and certification. Operational commanders at all levels must make network security a top priority. At a minimum, all system administrators should have background checks, SECRET (or higher) clearances, and direct access to a classified environment for incident reporting and coordinated response measures. Additionally, system administrators should receive initial and refresher security awareness training and formal training on IAVA compliance and incident reporting procedures.

We can spend every red cent the congress appropriates on better technology and we are going to be no more secure than we are today, unless—repeat unless—we start spending significant amounts of money on those who are entrusted with maintaining our operational networks in a high state of readiness. After all, our system administrators are the operators of all of this great technology and they are our front line defenders as well. Before we grant that much responsibility to any one group of individuals it only makes sense that those individuals be put through the scrutiny of a background check and that granting of complete access to the inner workings of our networks be coupled with appropriate training and certification. To do otherwise is to ensure that future adversaries will also have access to the keys to our kingdom when it is most imperative for them not to.

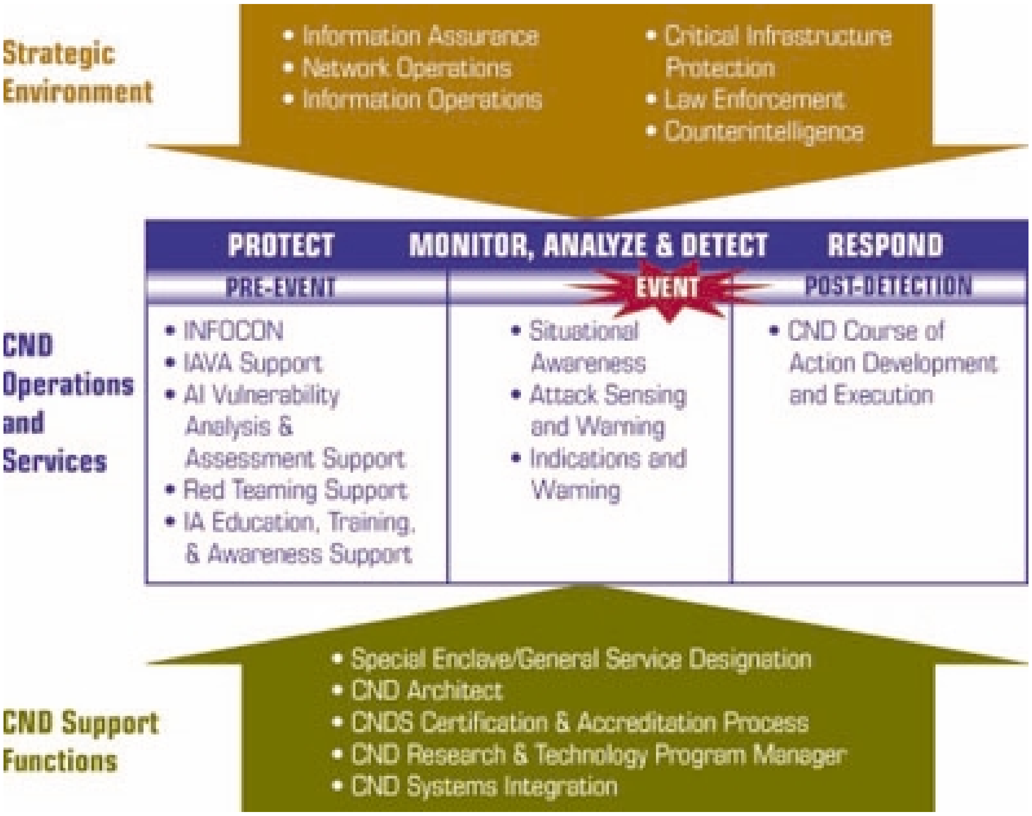
Captain Robert West, USN is the Deputy Commander, Joint Task Force – Computer Network Defense. As such he is responsible for coordinating and directing the defense of DoD computer systems and computer networks. CAPT West earned a B.E. (Electrical Engineering) from Vanderbilt University, an M.S. in Political Science from Auburn University, and a J.D. in General Law from Catholic University of America. He may be reached at westr@jtfcnd.ia.mil.

Law Enforcement and Counterintelligence Support to CND

Special Agent Michael R. Dorsey, DCIO CND Law Enforcement & Counterintelligence Center

Advances in the personal computing industry, the emphasis on information technology, and in particular, the exponential growth of the Internet have dramatically changed the focus, attention, and efforts of law enforcement and counterintelligence (CI) organizations within the United States. In the past 5 years the U.S. law enforcement (LE) community has struggled to keep pace with dramatic changes in this field, since computers are involved in virtually all aspects of criminal investigations. Whether a computer is used as an instrument of a criminal act, is the target of a criminal act, or retains critical evidence of a criminal act, investigators increasingly encounter computers and information technology in their work. Similarly, the U.S. CI community has found that computers are often at the heart of elaborate espionage cases, or are the target of foreign intelligence exploitation through the Internet. Information technology professionals and senior policy experts have publicly warned of the catastrophic consequences that computer network attacks (CNA) could have in the near future. The sheer numbers and complexity of computer network intrusions, probes, and mapping, and the proliferation of viruses and worms have caused considerable alarm in public and private sectors. The most recent round of distributed denial-of-service attacks on a number of well-known e-commerce sites had a direct impact on the value of high-technology stocks and shook the confidence of many e-commerce customers. For these reasons, among others, law enforcement and counterintelligence support must be considered an essential layer in any defense in depth strategy designed to provide a computer network defense (CND). The law enforcement and counterintelligence communities are critical in the efforts to assign attribution to network intrusions, and are the only authorities capable of conducting a detailed forensics analysis of systems to reconstruct evidence of a criminal act.

Law enforcement and counterintelligence have learned a number of valuable lessons in the wake of significant computer network intrusions such as the *Cuckoo's Egg, Ardita,* and *Solar Sunrise.* Each of these computer intrusion incidents clearly identified weaknesses in law enforcement authorities' processes and ability to respond quickly to CNA. More important, these intrusions have highlighted the wide split between information systems security personnel, who clearly need information to protect their networks from further degradation, and the LE community, which traditionally has held investigative information within its own close circles, drawing a solid "blue line," across which active investigative information does not pass. As a result of these sometimes competing security objectives, senior policy makers have often referred to computer network intrusion incidents as a matter of "national security versus law enforcement." By its very nature, this dichotomy seems to dictate a win-lose scenario. This view has not been of benefit to either the information systems security community or the LE community. Moreover, within the Department of Defense (DoD), this dichotomy has had an injurious effect on the network operations community, which is charged with the ensuring the continuous flow of information over networks to support military operations. The business operations community too has been torn between the needs of its information security personnel and the needs of law enforcement when network intrusions occur. In both cases, critical operational decisions must be made based on the sharing of information among traditionally distinct groups that, in the past, have resisted collaboration and kept information within their own circles.


Strategic Environment
• Information Assurance
• Network Operations
• Information Operations
• Critical Infrastructure Protection
• Law Enforcement
• Counterintelligence
PROTECT
MONITOR, ANALYZE & DETECT
RESPOND
PRE-EVENT
EVENT
POST-DETECTION
CND Operations and Services
• INFOCON
• IAVA Support
• AI Vulnerability Analysis & Assessment Support
• Red Teaming Support
• IA Education, Training, & Awareness Support
• Situational Awareness
• Attack Sensing and Warning
• Indications and Warning
• CND Course of Action Development and Execution
CND Support Functions
• Special Enclave/General Service Designation
• CND Architect
• CNDS Certification & Accreditation Process
• CND Research & Technology Program Manager
• CND Systems Integration

However, this win-lose relationship between national security and law enforcement is now being turned into a win-win philosophy through the establishment of several joint, interagency organizations and a willingness to include the LE and CI personnel as a part of the defense-in-depth strategy of information systems security. After the resolution of the Solar Sunrise intrusions into DoD networks in 1998, President Clinton signed Presidential Decision Directive 63, establishing the National Infrastructure Protection Center (NIPC). Both this directive and the the NIPC were established to formulate a strategy to protect our national information infrastructure (NII) from deliberate attacks. There was a clear recognition that a central information clearinghouse, composed of multiple organizations from the law enforcement, intelligence, and technical security communities, was essential to the protection of the national infrastructure. The development of the NIPC included agencies such as the FBI, the U.S. Secret Service, the Postal Inspections Service, NASA, the Defense Criminal Investigative Organizations (DCIO), the State Department, the CIA, the National Security Agency, the Air Force Intelligence Agency, and various technical security representatives. Additionally, partnerships were developed with the public utilities critical to the NII. It was envisioned that the NIPC would be able to gather information from the public and private sectors and provide ample warning of threats, analyze trends, and collaborate to fight the criminal hackers and foreign intelligence organizations exploiting our information networks. This goal necessitated a change in the traditional thinking of separate, insular organizations that were not accustomed to collaborating with each other, let alone to sharing sensitive information about ongoing events. It has required a degree of trust and the building of partnerships, which has never before been attempted. While much work remains in this process, considerable progress has occurred, and, as a result, significant accomplishments have been realized.

At about the same time that the NIPC was being developed, a similar process was occurring within DoD. The Office of the Secretary of Defense established the Joint Task Force for Computer Network Defense (JTF-CND) to protect the Defense Information Infrastructure (DII). The concept of the JTF-CND was to provide a single organization within DoD that would develop a common operational picture, and situational awareness of computer network attacks against the DII. To accomplish this task, a small cadre of military and civilian personnel with varied professional backgrounds was assembled under one command and co-located with the Defense Information Systems Agency (DISA). The JTF-CND provides joint operational command and control of the military services computer network defense (CND) organizations. As a component of the Commander in Chief, U.S. Space Command, the JTF-

CND works closely with each of its military service components, regional commanders in chief (CINC) and defense agencies. In addition to the military operations and systems security personnel that make up the JTF-CND, the DCIOs have formed a joint law enforcement and counterintelligence center, co-located with the JTF-CND, to provide LE and CI support to CND.

Again, the emerging threats of network attacks and exploitation have resulted in the formation of nontraditional organizational partnerships and necessitated the sharing of information across organizational boundaries to meet and defeat these threats. Within DoD, co-location of diverse expertise and responsibilities from the information security, military operations, LE, and intelligence organizations has resulted in close collaboration concerning the information needed to protect our information infrastructures. However, if this collaboration is to be successful, there must be recognition of the organizational responsibilities and the benefits that the organizational element brings to the problem set. This is especially true for the LE and CI communities. The win-lose perspective of “national security versus law enforcement” significantly hampered coordination and cooperation among traditional military operators, information system security professionals, law enforcement, and counterintelligence organizations. This reluctance to share information on ongoing investigations stems from a concern that the target of the investigation, or the adversary, could be alerted to the investigation and destroy evidence or alter his or her activity to avoid arrest and prevent a successful prosecution. Law enforcement professionals in the computer intrusion environment will have to fight against this understandable reluctance if we are to succeed in our pursuit, and assist in the protection of the national information infrastructure. In addition, technical security professionals and the operations communities of government and business must recognize the benefits and advantages that LE and CI organizations bring to defending computer networks.

During the initial stages of a network intrusion, the systems administrator has the opportunity to gather or capture valuable information from intrusion detection systems or systems logs that will later benefit technical analysis and aid a law enforcement investigation and subsequent forensics analysis of the attacked system. The systems administrator should conduct all actions possible and permissible to him or her under the Electronic Communications Privacy Act (ECPA). ECPA permits network owners to conduct certain activities to protect and defend the health and welfare of their networks. However, network owners and administrators should also recognize that most intrusions are also violations of Federal law. This recognition allows network owners and administrators to avail themselves of the greater authorities and powers granted to law enforcement organizations. LE organizations will typically respond to reports of system intrusions by using criminal investigative authorities. In the event of an attack, the network owner must decide whether to immediately shut down the affected system or network or to allow continued monitoring of the intrusion activity by law enforcement. Continued monitoring of the intrusion activity may present an opportunity to trace the hacker's route and glean valuable intelligence about the tools and techniques being exploited by the hacker. The investigative tools used by law enforcement include official requests for information, criminal subpoena, court orders for records, search warrants, and undercover operations. Additionally, Federal law enforcement maintains close partnerships with counterpart agencies all over the world and will frequently request the assistance of foreign counterparts if an intrusion activity appears to pass through, or originate from, other countries.

This does not mean, however, that a law enforcement investigation is not a matter of national security. Particularly where DoD systems and networks are the victim of root-level intrusions, the DCIOs [Air Force Office of Special Investigations (AFOSI), National Crime Intelligence Service (NCIS), Defense Criminal Investigative Service (DCIS), U.S. Army Criminal Investigation Department (USACID), and U.S. Army Military Intelligence (USAMI)] approach all such activity as a matter of national security because of the potential impact on U.S. military operations and the sensitivity of the information contained in DoD networks. However, current laws and policies require that we first use the investigative tools and authorities of a crimi-

SOCOM NOSC

continued from page 16

ways for unauthorized users to gain access to computer systems. USSOCOM launched a program to ensure that its users' passwords are properly configured to reduce the risk of unauthorized access. In addition, all users are required to receive computer security training before gaining access to any USSOCOM system. USSOCOM then runs periodic programs to attempt to crack users' passwords. If a password is cracked, the user must go through a prescribed process to regain access to USSOCOM systems.

The USSOCOM NOSC provides the command with an organization that can monitor its networks for any type of trouble. If problems occur, the NOSC can determine whether the problem is hardware, software, or security related and contact the proper team to fix the problem. By combining its systems under one section and creating the NOSC, USSOCOM is ready to provide its customers with better and more secure service, making it easier for USSOCOM's forces to carry out their diverse missions.

Major Jordan is the Chief of the Enterprise Systems Branch for USSOCOM. As the branch chief, Major Jordan is responsible for the operations and maintenace of USSOCOM's intelligence, collateral, and unclassified computer systems. He received his B.S. in mathematics with a computer concentration from the University of Notre Dame and a M.S. in Computer Science from the University of Dayton. He may be reached at jordanj@socom.mil.

Law Enforcement

continued from page 23

nal investigation before we use the authorities of the Foreign Intelligence Surveillance Act (FISA) or conduct a counterintelligence investigation. The primary purpose of this requirement is to ensure that our national intelligence agencies, including counterintelligence, do not unlawfully collect sensitive information about U.S. persons, as defined in Executive Order 12333.

For this LE/CI process to work effectively, law enforcement and counterintelligence organizations must be able to provide technically relevant information to the systems security and operations community during an investigation. At the same time, system owners and information security personnel must respect the need of LE and CI organizations to withhold some specific information about the investigation such as the identity of the suspects, confidential source-related information, and information that was derived from a grand jury subpoena or an electronic intercept order. Each component involved in an intrusion incident must recognize the interests of the other components and work in collaboration with them to resolve the incident. The information security community must recognize that the law enforcement investigative process is methodical and somewhat slow by nature to ensure the liberties that we enjoy in our democracy. System owners and operators must recognize the value of deterring further network intrusions through successful investigations and prosecutions of criminal hackers. Where foreign governments, intelligence services, or terrorist organizations are found to be responsible for intrusions and exploitation of networks, CI operations designed to gather information and manipulate the adversary's perceptions may be the most effective method of defending the national information infrastructure.

Our national information infrastructure will continue to be a viable target of criminals, intelligence operatives, terrorists, and nation-sponsored information warfare for the foreseeable future. The DII presents an attractive target for each of these groups for a variety of reasons. To successfully defend the DII, we need to maintain a robust team of technical security professionals, military operators, intelligence officers, and law enforcement and counterintelligence investigators. This team will continue to develop the process by which it shares information across organizational boundaries to protect and defend the DII, and will aggressively pursue those who attempt to illegally penetrate the infrastructure. Law enforcement and counterintelligence support to CND is a matter of force protection and is critical to forming a common operational picture of the threats affecting the security of our military operations.

Supervisory Special Agent Michael R. Dorsey recently completed his duties as the Chief of the DCIO CND Law Enforcement & Counterintelligence Center. He may be reached at his current assignment at MDorsey@ ncis.navy.mil.

Information Assurance Training

at the U.S. Army's Computer Science School

Major Mark V. Hoyt, USA
Fort Gordon

Because of the increasing number of information warfare attacks directed against the Department of Defense (DoD), the U.S. Army has issued several directives concerning security training for system administrators (SA) and network managers (NM). The directives, originating from the Army's Director of Information Systems for Command, Control, Communications, and Computers (DISC4), require that all Army military, government, and civilian SAs and NMs be trained in information systems security, depending on their experience and skill levels.

One DISC4 directive states that all Army SAs and NMs will be trained and Phase 1 Information Assurance (IA) certified. All Army SAs and NMs with 3 or more years of experience will be trained to the Phase 2 level and Phase 2 IA certified. The deadline for Phase 1 and Phase 2 IA certification is December 2000.

The U.S. Army's Computer Science School (CSS) at Fort Gordon is conducting computer security training to meet Phase 1 and Phase 2 IA certification requirements. The primary goal of this security training is to increase the ability of Army SAs, NMs, and Information System Security Officers (ISSO) to protect friendly information systems by preserving the confidentiality, integrity, and availability of the systems and the information they contain.

The CSS offers a free Web-based ISSO course requiring approximately 20 to 40 hours to complete. The course, including the test and certificate generation, is completely Web based and is considered equivalent to Phase 1 IA certification by DISC4. Approximately 2,000 persons have taken the ISSO course and passed the ISSO Web-based examination. The course is located on the Web at www.gordon.army.mil/css/css/courses.htm.

The CSS also conducts the majority of Phase 2 IA certification training for the U.S. Army. Phase 2 security certification consists of two 1-week courses, usually conducted in sequence.

SA and NM Level Classification	Training Deadlines	
	Phase 1 Certified by	Phase 2 Certified by
Level 1 SA/NM (Classified System)	31 Jan 1999	Not Required
Level 1 SA/NM (Unclassified System)	31 Dec 2000	Not Required
Level 2/3 SA/NM (Classified System)	31 Jan 1999	31 Dec 2000
Level 2/3 SA/NM (Unclassified System)	31 Dec 2000	31 Dec 2000

The first week of Phase 2 security certification is called the System Administrator's Security (SAS) course. This course focuses on securing the information system platform. The first 4 hours of the course are spent primarily on reviewing army regulations, public law, and access control measures. After the first half day, the course focuses on securing the information system's platform by securing the operating system that runs the system. During the SAS course, 15 hours are spent on hands-on training in securing Windows NT platforms. The final 14 hours of the course are spent on hands-on training in securing UNIX platforms (using Solaris 2.6).

The second week of Phase 2 security certification is called the Network Manager's Security (NMS) course. This course focuses on network security. The first day provides background information on the Army's Computer Emergency Response Team, the Network Security Improvement Program, a briefing by a counterintelligence agent, and an overview of common network and information system threats. The second day focuses first on cryptography and then on how to secure a Web server (an Internet Information Server is used for the hands-on training). The third day focuses on the use of routers to secure networks, with hands-on training conducted on CISCO routers. The fourth day of the

continued on page 34

That's NOT My Final Answer...

Your PKI Help Desk Solution and the Answers You Need.

Ms. Victoria Alkema, DISA Defense Enterprise Computing Center Detachment

The Public Key Infrastructure (PKI) program is a DoD wide team effort. The PKI Program Management Office (PMO) leads the effort, and is supported by the engineers who design and implement the changes. You—our customers—are critical to implementing the PKI technology and the Help Desk stands ready to assist you.

What can I expect?

When you initiate a call to the PKI Help Desk, there is no need to apologize for not understanding the problem or having to contact us. We are quick to dispel these thoughts, for that is contrary to our purpose, which is to assist all DoD personnel in obtaining their PKI certificates. Your PKI Help Desk is located at Defense Enterprise Computing Center (DECC) Detachment Chambersburg and stands ready to assist you.

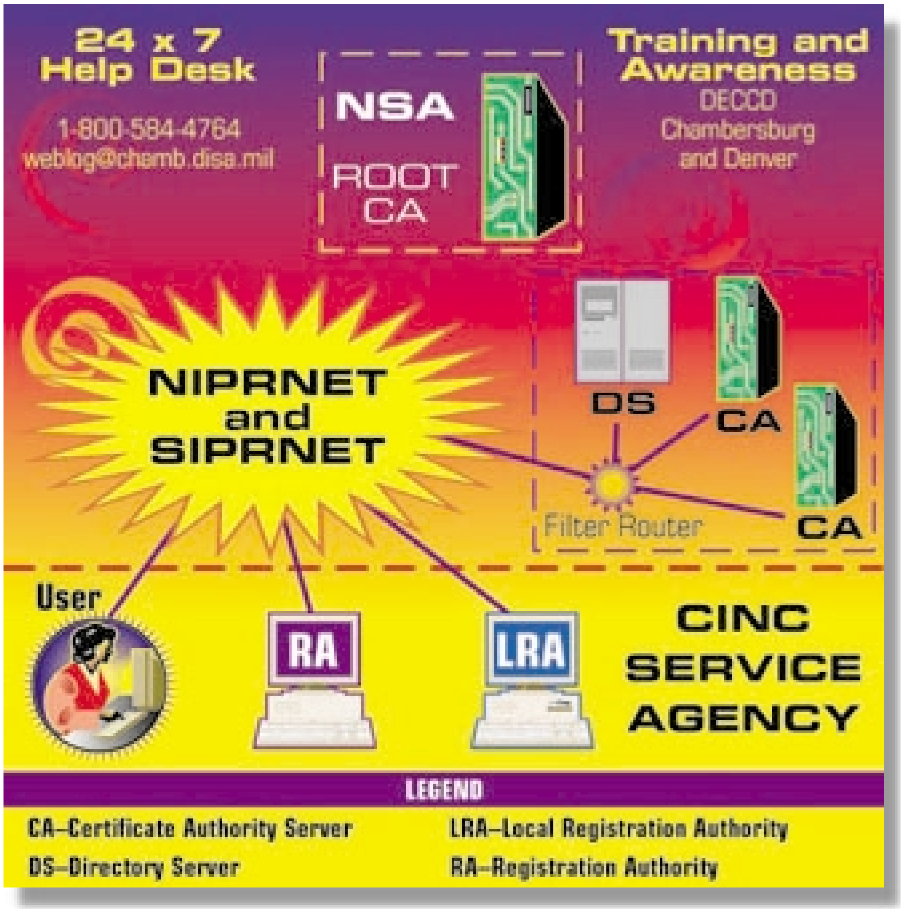
Because of the vastness of potential issues, the Help Desk is limited to assisting in obtaining End User, Local Registration Authority, Registration Authority, and Server Certificates, and will troubleshoot connectivity issues. When you successfully obtain the certificate, the actual implementation and usage will be based on vendor-specific guidance. The Help Desk is not unequivocally responsible for that assistance, but does maintain a knowledge-base of some of the more popular "lessons learned" from others' implementations. That information can be easily recalled from our knowledge-base and, if available, offered to further your investigation.

The PKI Help Desk is staffed by technicians ready to assist 24x7, and may be reached by phone at 1.800.582.4764, commercial 717.267.5690 (DSN 570) or by E-mail at WEBLOG@chamb.disa.mil. When you call, a technician will listen to your situation, ask a few questions, and open a trouble ticket. Should you choose to E-mail the Help Desk, please include your telephone number, IP address, 10 character unique identification number (if known), and a detailed description of the problem. Also include the most convenient time to contact you, and we will attempt to comply. This trouble ticket is important, for it allows the technician to record details of your technical problem, our information, updates, and final resolution.

If the technician is unable to find an existing instance of your problem, you are likely to be connected to a senior technician at that time. The original technician will remain on the line to hear the problem resolution process and obtain the solution. Most often, the situation can be resolved over the phone, but occasionally it requires more in-depth analysis and assistance. However, the resolution will rarely take more than a day. Whatever the case, the ticket remains open until you are satisfied and concur with closure, otherwise the ticket returns to the senior technician to continue the work.

Am I the only one?

The PKI Help Desk staff have been performing these specific services for over two years and have compiled a vast knowledge-base of customer related issues. The questions cover a wide spectrum—from novice users to a system engineers. The PKI hierarchy is the end user will contact the Local Registration Authority (LRA); the LRA would contact his Registration Authority (RA); and ultimately the RA will contact the Help Desk. Since there are less than one hundred RAs and about four hundred LRAs, following the defined hierarchy can better assist the potential 3.2 million DoD end-users. We realize that is not always possible and will respond to all calls accordingly. If you do not know who your LRA or RA is, please contact us and we can assist you.



Class 3 PKI Pilot Architecture

Each CINC/Service/Agency (C/S/A) is assigned an official point of contact (POC) for PKI technical representation. The POC list is maintained by the PKI PMO and is provided to our Help Desk. The Help Desk utilizes a technical representative when an issue arises unique to C/S/A. These representatives are actively participating in the PKI technical groups, representing your interests, and are critical to the Help Desk and you. If the Help Desk cannot arrive at a resolution, the subject is referred to the PKI PMO, who is a constant source of guidance.

The Help Desk offers you the additional benefit of other DoD partners' information during research. As desktop software evolves, we are continually reviewing other knowledge-bases, FAQs, and help sites readily advising callers of information. The PKI PMO is continually posting changes to the PKI Web site http://iase.disa.mil. This is truly a network of knowledge and we are pleased to assist you in finding the answer.

When a situation requires the information be widely disseminated to the DoD PKI users, an E-mail broadcast message is generated from our Help Desk. This is always in compliance of the PKI PMO policy of advising of changes, updating status and/or giving guidance. The PKI PMO and the Help Desk work closely in preparing announcements and responding to customer reported difficulties.

The trouble ticket information you supply is read by the PKI PMO weekly. This information is analyzed by the PKI PMO and engineers and may determine a program change or identify a training weakness. Contacting the PKI Help Desk should never be viewed a weakness, but a contributory strength to the entire DoD PKI team effort. We appreciate you, our customers, and look forward to your call.

Victoria Alkema is the Defense Information Systems Agency PKI Project Lead, located at Defense Enterprise Computing Center Detachment, in Chambersburg Pennsylvania. She is continually in touch with PKI program management office, training coordinators, and System Engineers to facilitate smooth operations and resolve customer reported outages. A trained team of PKI colleagues and team members make this PKI Help Desk successful.

Marine Corps Active Computer Network Defense

The Changing Face of Warfare

"They will attack us asymmetrically, pitting their strength against our weakness, whether that lies in the military, political, or domestic realm. For example, in future conflicts, data lines of communication may be just as important as sea lines of communication—and our adversaries, whether they are third world nations, transnational actors, or crime syndicates, will attack them."

—General Krulak, 31st Commandant of the Marine Corps

Captain Carl Wright, USMC
Major Ted Steinhauser, USMC (Ret)

Today's enthusiastic and unparalleled consumption of information technology by corporate America and government has created superior enterprise-scale business process capabilities. However, in the rush to exploit the advances in information technology, an evolutionary vulnerability has developed in connection to the interdependencies these systems rely on to function in the global arena. From both the corporate and the DoD perspectives, the enterprise approach to defending the venture capability has become the predominant weapon in the system security arsenal. This article will briefly explore the Active Computer Network Defense (ACND) model in relation to the Marine Corps' success in defending both garrison and deployed tactical environments.

Overview

Significant progress has been made in defining and articulating the effects of information warfare, or cyberwar, on the global information grid (GIG). The majority of these studies concern the information revolution, the changing face of warfare, and DoD's need to develop security procedures that ensure that information is available to commanders when required.

Today's cyber defense efforts indicate that although organizations are striving to enhance their security posture through the use of boundary-level security devices (e.g., firewalls), their focus remains myopically on protecting the "front door" or forward edge of the battle area. Cyber-centric maneuver warfare implies that the adversary will not attempt to effect change or impact via direct frontal assaults on information technology assets, but is far more likely to conduct guerilla-type information warfare, penetrating soft targets while ensuring that the defender's limited security resources are engaged elsewhere. The implication is that the adversary will obtain access to targeted systems by means of well-orchestrated electronic envelopment and distraction drills, eventually achieving penetration regardless of defensive security initiatives. Therefore enclave compartmentalization, distributed defense-in-depth mechanisms, real-time system battle damage assessments, and immediate recovery techniques will become the critical success factor in the new cyber defense model.

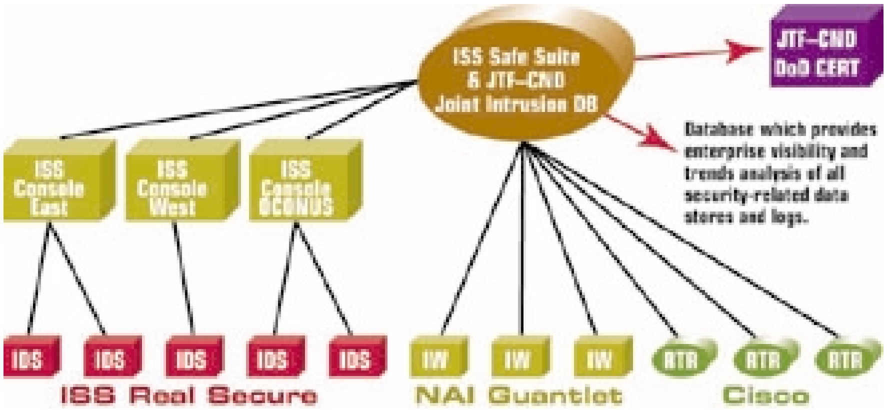
Active Computer Network Defense (ACND) Model

ACND is predicated on the original defense-in-depth model, which is widely used throughout the DoD and the Federal Government. The ACND model capitalizes on the multilayered defensive strategy of defense-in-depth by incorporating enterprise business processes, strong standardization, and configuration control down to the lowest possible point in the organizational information technology infrastructure. The more centralized this control, the more formidable the defense posture the organization responsible for computer network defense (CND) can foster. The ACND model helps answer the "how" of developing, deploying, and sustaining a secure homogeneous enterprise network in a heterogeneous network environment. It is important to understand that ACND does not focus solely on specific security technologies, but is more concerned with enterprise business processes and how they integrate with security technology to address the cyber-centric maneuver warfare threat.

In order to fully understand the Corps' ACND posture, a brief overview of their enterprise network (The Marine cyber battlefield) is necessary. From its inception, the Marine Corps Enterprise Network (MCEN) was built on a foundation of securable technologies, enabling centralized control, sustainment, protection, and, most importantly, the defense of Corps Information Infrastructure. The MCEN ACND process focuses on creating centralized cross-functional information technology support structures resident with the Marine Corps Information Technology & Network Operations Center. By means of 24x7 monitoring of all MCEN access points (see figure below), security-related data and logs are securely transmitted to the centralized data repository for detailed analysis by highly trained Marines supported by government civilians and contractor personnel. Depending on the situation, corrective action may be directed by the Commander (COMMARFOR-CND) after the situation is assessed by the MARFOR-CND staff at which time the defensive response may be enacted at the lowest point in the infrastructure, the user's desktop. In concert with the technological ability to direct defensive response across the enterprise, the ACND response process provides real-time defense to MCEN users no matter where they are or what time of day an incident occurs.

Deployed Security Interdiction Device (DSID)

Technology plays an instrumental part of the Corps ACND methodology. From its initial use in protecting and defending the MCEN environment, the Marine Corps has expanded the ACND model to the Fleet Marine Force (FMF) for use in the deployed tactical environment. The Deployed Security Interdiction Device (DSID) is a tightly integrated package of best-of-breed commercial off-the-shelf technology similar to that of the garrison perspective, that directly supports the Marine Corps' ACND process. DSID gives the deployed tactical commander the same boundary-level security architecture that Marine Corps forces enjoy in the MCEN garrison environment. Its primary function is to provide a layered defense of the boundary-level point-of-presence tactical network. The DSID package integrates routers, advanced access control lists, firewalls, network intrusion detection systems (IDS), host-level IDS, virtual private network technology, and vulnerability assessment software, to provide a comprehensive enterprise network security system. Currently, DSID is an organic asset of the Marine Expeditionary Force Communication Battalion. In the deployed tactical environment, the DSID infrastructure resides between the Defense Information Systems Agency's Strategic Tactical Entry Point (STEP) and the deployed unit's network architecture in the states. DSID provides the deployed commander with the utility of joint information systems in which a deployed unit reaches back to leverage information stores normally resident within the garrison environment. More important, DSID provides this capability to the commander in a robust secure manner.


ISS Safe Suite & JTF-CND Joint Intrusion DB
JTF-CND DoD CERT
Database which provides enterprise visibility and trends analysis of all security-related data stores and logs.
ISS Console East
ISS Console West
ISS Console OCONUS
IDS
IDS
IDS
IDS
IDS
IW
IW
IW
RTR
RTR
RTR
ISS Real Secure
NAI Guantlet
Cisco

Marine Corps Active Computer Network Defense Architecture

In conclusion, the Marine Corps' enterprise ACND approach to integrating technology and security core competencies has laid the foundation for the first deployed tactical CND system business process within DoD. The Marine Corps ACND approach ensures the integrity, availability, and confidentiality of the deployed commander's information regardless of the commander's location, foreign or domestic.

Captain Wright and Mr. Steinhauser have been actively engaged in the defense of the MCEN since the conception and establishment of the Marine Corps' component of the JTF-CND. Captain Wright may be reached at wrightcm @noc.usmc.mil and Mr. Steinhauser may be recached at steinhauserth@ noc.usmc.mil.

Mobile Code

Is It Worth the Risk?

Major Boyles, USAFR

Imagine you are logged onto an NT workstation as a user in the Domain Admin group. You are doing research on mobile code, and your research takes you to a site off the beaten path. Without your knowledge, the registry self-administered maintenance (SAM) file from your workstation is E-mailed to an account at one of the popular free E-mail providers. Several weeks later your network experiences serious problems. The network administrator tracks those problems to a remote access to your network by someone using your account. **Oops.**

Or perhaps while you are surfing the Web, a script called hack.bat is deposited in your Startup menu. The next time you log on to your system the hack.bat script runs and changes the password for every user on your network and the networks of all trusting domains, including the password of the domain administrator. In addition, every NT system on the network has a strategic file removed, preventing each system from booting up after a shutdown. Finally, every NT system on the network is remotely shut down, including yours. **Oops.**

Malicious mobile code can do this. Should you be worried? Yes. You put your system and your network at risk every time you open an E-mail, attachment or not, and every time you browse the Web.

Warning Signs

One of the first demonstrations of our vulnerability to mobile code occurred in January 1997, when three German hackers showed a television audience how a Web page "click-bait" could use an ActiveX control to generate a clandestine electronic transfer of funds using Quicken.

In 1998, users of Microsoft's Hotmail and QUACOMM Inc.'s Eudora were presented with a Trojan horse logon screen generated by a JavaScript embedded in their E-mail. When the users filled out the logon screen, the account information and the Internet Protocol (IP) addresses were E-mailed to the author of the hack.

The recent Guninski Exploit demonstrated how accessing a Web page or opening a hypertext markup language (HTML)–formatted E-mail could allow a malicious mobile code to take control of a user's workstation. This exploit used the "object for constructing type libraries for scriptlets" ActiveX control.

The computer security company Finjan now offers a live demonstration of a harmless Trojan horse called Bill Vote Attack, which demonstrates how mobile code can be used to create a new folder on the Windows desktop filled with files copied from the hard drive.

What is Mobile Code?

Mobile code is any executable or interpreted program, script, or application that is introduced to a local system from a remote location and executed without the user's consent. This broad definition includes the viruses that were once commonplace on floppy disk in the days of stand-alone computers and encompasses viruses, application macros (MS Word, MS Excel, etc.), files executed by applications such as Adobe Acrobat, Postscript files, and some code executed by Web browsers or E-mail applications. Mobile code is sometimes referred to as applets or downloadable code.

Mobile code is not in itself bad. In fact, it is a cornerstone of client/server computing. It enables our applications and allows us to create dynamic programs even if we are not skilled programmers. Its jazzes up our Web pages and E-mail with sound, video, and animation; allows on-line chatting; automates workflow; and enables Web sites to automatically update software such as Windows NT, MS Explorer, and antivirus applications. Mobile code is becoming a requirement for enterprise networking, e-commerce, and data sharing. The problem is security and protecting our computer systems and networks from people with malicious intent. Macro viruses, such as Melissa, are now considered the most widespread malicious mobile code on the Internet.

For the sake of this discussion, let us refine our definition of mobile code to code that is transmitted by a network. If I receive an E-mail message with an executable file—say, a game—attached, I have the choice of executing that program or not. This is not mobile code according to our definition. Although the code moved from somewhere in cyber space to my workstation, I made the choice of executing it, knowingly assuming the risk that the game might contain malicious content. If, on the other hand, I open up an E-mail and inadvertently execute a code written in JavaScript, I have experienced mobile code. Where did this mystery code come from? What did it do? With the Web-enabled E-mail applications available today, previewing E-mail may be all it takes to give away protected information or to crash a workstation or a network. For example, the proof-of-concept worm *BubbleBoy* is activated simply by viewing an affected E-mail in the Preview pane of Microsoft Outlook or Outlook Express. This worm, when activated, performs a mass E-mail a la *Melissa*, then updates the user's registry. *BubbleBoy* is written in Visual Basic Script (VBScript) and uses Microsoft's ActiveX control mobile code.

There are many types of Web-related mobile code. Examples are Microsoft's ActiveX, VBScript and Visual Basic for Applications (VBA), Sun Microsystem's Java Applets and JavaScript, and a whole slew of plug-ins.

Scripted mobile code, such as VBScript, JavaScript, LotusScript, PerectScript, and VBA, arrives in the form of text that must be interpreted at run time. It is possible to discern the scripted text's potential for harm by viewing a Web page or an E-mail source or macro.

For brevity's sake, in our consideration of the compiled class of mobile code, we will limit our discussion to the most popular forms: Java and ActiveX. Java runs in most Web browsers, including Netscape's Communicator and Microsoft's Internet Explorer. It is compiled into an intermediate, architecturally neutral format called byte code. This byte code must be executed within a Java Virtual Machine (JVM) in order to run. JVM is included in most Web browsers. Currently ActiveX is exclusive to Explorer, although it will run with a plug-in on Communicator. This code, known as a control, has been compiled into binary specific 32-bit windows and is essentially the same as the Dynamic Link Library (DLL) files that are common to all Windows-based workstations. ActiveX is the most powerful of the mobile codes and therefore presents the greatest risks. It is native Windows and can do anything Windows can do, depending on the permissions of the user (e.g., read, write, copy, and delete files; run applications and APIs; connect to network resources; send E-mail).

How Mobile Code Works

When you browse a Web page with ActiveX code embedded in it, you are trusting the Web page to do the right thing and not take advantage of you. When you connect to the Web page, code is downloaded from the Web server onto your computer's local environment and executed on your workstation with your privileges and local system resources. This allows you to interact with the Web site, enabling you to fill out information and send it back to the Web server for processing, submit forms, open spreadsheets, execute database queries, and perform other productivity-related functions. The mobile code running on your local workstation can determine information about you—who you are, your permissions, your group membership—and grant you access to data and information without your needing to log in or authenticate. This is most valuable in an intranet environment, where applications are Web enabled and run on the server, but is also valuable for Internet use. Mobile code saves you from having to download and install applications on your local workstation. It also allows applications to manage your file system, create directories and files, update your registry, and prepare your environment for whatever. In addition, mobile code will jazz up your Web experience by creating dynamic images and dialog. Much of what mobile code does can be accomplished by server-side applications with the use of Java servlets, SQL, CGI, gif89s, and many other helpful tools. However, a downside is that server-only Web pages are resource intensive and require users to log in and authenticate. Without authentication all users are treated the same by the server and are considered anonymous, with vastly reduced privileges.

Scripting was developed because plain HTML wasn't enough. VBScript and JavaScript are not nearly as powerful as ActiveX but still put systems at risk. Java Applets present the least threat because they employ a security wrapper called a Sandbox.

Guarding Against Malicious Mobile Code

The risk from mobile code can be mitigated by proper management. What this entails depends on the type of code.

ActiveX has an all-or-nothing approach to security based on digital signatures contained in the ActiveX controls. Your browser can be configured to allow downloading of ActiveX controls from trusted sources only, based on these digital signatures. Nontrusted sources will then cause your browser to prompt you if you want to run an ActiveX control. All ActiveX controls run with the same privileges, regardless of their source. In my experience, only a small percentage of Web sites (1 to 2 percent) actually have ActiveX applications, and choosing not to run ActiveX , in most cases, prevents only a single action from occurring. Therefore, the Web page will continue to function if ActiveX does not run. The area in which ActiveX mobile code is taking off is Web-enabled applications, such as MS Access, running on a server. Even then, preloading ActiveX will prevent it from becoming mobile and being downloaded to your system. A good security practice is to disable ActiveX in your E-mail and to require your browser to prompt you each time it is requested. Then you can decide in each case whether to assume the risk. In the future, expect Department of Defense (DoD) sites to restrict ActiveX at the firewall and to enforce a policy on the browser of "no ActiveX." This practice will still allow you to use ActiveX plug-ins and to have ActiveX associated with installed applications through DLLs, just not mobile code.

JavaScript and VBScript are more popular than ActiveX. It is estimated that more than 80 percent of Web sites contain either JavaScript or VBScript. These active scripts still represent some risk to your private information and system and network integrity. Unlike ActiveX, these scripts do not have associated digital signatures. However, you can restrict "Active Scripting" on most Web browsers, although doing so may severely affect Web access and many Web sites may not perform properly if Active Scripting is disabled.

Java or Java Applets were designed from the ground up with security in mind. Java uses what Sun refers to as a Sandbox. Each applet is wrapped by a set of rules that prevents it from accessing system resources. Java Applets therefore may not interact with file systems. There are only 10 system variables that Java Applets can retrieve. These variables are needed for the Java Applets to perform their job. This still represents an all-or-nothing approach to security, because no distinctions are made based on the level of trust associated with the source of each applet. The biggest risk is associated with Java's complexity and known security breakdowns. Java Applets have been around for a long time. They have reached a mature level and should be considered safe. Unfortunately, the very things that make Java Applets safe limit their usefulness for enterprise computing.

On the Horizon

Sun is extending Java's security to include more ActiveX-like capabilities and is incorporating a digital signature as well. This updated version is referred to as the Java 2 security model. Its major improvement over ActiveX security is the assignment of different permission levels based on local security policy and trust levels assigned to each applet's source. These improvements will make Java Applets more competitive with ActiveX, but incorporates many of the same security risks. Not one to give up the lead, Microsoft is making noises about extending the security model for ActiveX as well.

Other mobile code that puts your systems at risk includes MacroMedia's ShockWave, RealNetworks' RealPlayer, Sun's Save-Tcl, and other plug-ins that you add to your browser. When you connect to a Web page that contains code requiring one of these plug-ins to function properly, the code will be downloaded to your local workstation and activate the associated plug-in. If you have not installed the particular plug-in, your browser will generate an error message. These plug-ins don't offer the same flexibility as ActiveX but nonetheless pose some risk. What is even riskier is the plethora of new plug-ins that are anticipated in the near future as more and more companies try to market to the Internet. And, hold onto your hats, just around the corner is the "mobile agent," mobile code that can jump from one system to another. This prospect will be reserved for a future discussion.

It is likely that over the next 18 months, DoD will be required to replace all mobile code–enabled Web pages on its vast network of over 2,500 primary Web sites with server-only Web pages. This will be a tremendous undertaking but will result in a mobile code–free environment. Achieving this will set the stage from the next step: Forcibly restricting access to mobile code on all DoD networks.

In the meantime, an ever growing number of security products on the market provide some level of protection from malicious mobile code. Some of these products are Finjan's Enterprise Desktop Security, SurfinGate, and SurfinShield; Trend Micro's Interscan, WebProtect, and Web VirusWall; and Computer Associates' Unicenter TNG, SafeGate (Security 7), SafeAgent (Security 7), and SessionWall.

For now, what can and should be done? The following list contains some reasonable precautions:

- Lock down your browser.
- Include only those plug-ins that are required for your job. Entertainment should stay at home.
- Set your browser to a high security setting.
- Prompt for ActiveX and Active Scripting. Refuse to accept the first time around. If you find you need to run the mobile code, think carefully before you try it.
- Never surf as a privileged user (Domain Admin, Account Operator, etc.).
- Use a sanitized machine. Never surf from a server or system containing important data.
- Back up your hard drive often.
- If prompted to open or save a file, always save executables, and run a virus scan on the file before and after execution. Be careful; compressed files may defeat a virus scan.
- Don't assume that a negative scan means you are safe. Virus software will not detect new viruses, Trojan horses, or unique malicious code.
- Network administrators should consider ways of restricting mobile code at the firewall.
- System administrators should consider (1) using third-party software that evaluates mobile code for privileged access or malicious intent and (2) preloading ActiveX code needed to support known Web-based applications.
- Developers should adopt server-only solutions, using development software such as Cold Fusion.
- Security administrators should issue policies and guidelines on the use of mobile code.
- Users should receive training concerning the risk associated with mobile code and how to manage the settings in their browser software to mitigate these risks.

So, Is mobile code worth the risk? Yes. But only if you fully understand what those risks are and take appropriate measures to protect your data, your workstation, and your network.

References

Angel, Jonathan, "Mobile Code Security," NetworkMagazine.com, December 1999, available on-line at: http://NetworkMagazine.com/

Blacharski, Dan, "Mobile Code: Handle with Care," NetworkMagazine.com, December 1999, available on-line at: http://NetworkMagazine.com/

Brown, Doug, & Spangler, Tod, "DoD Weighs JavaScript Ban," *Inter@ctive Week*, November 22, 1999.

Clark, Elizabeth, "Mobile Code Safety," NetworkMagazine.com, December 1999, available on-line at: http://NetworkMagazine.com/

Ferris, Nancy, "DoD Weighs Ban on Advanced Web Technology," GovExec.com, October 7, 1999, available on-line at: http://gov.exec.com/.

"Frequently Asked Questions—Java Security," Java Web site, available on-line at: Java.sun.com, accessed July 22, 1998.

Karve,Anita, "Securing Java and ActiveX," NetworkMagazine.com, December 1998, available on-line at: http://NetworkMagazine.com/

McGraw, Gary, & Felten, Ed, *Securing JAVA: Getting Down to Business with Mobile Code*, John Wiley & Sons, Inc., January 1999.

Mendel, Brett, "Mail Hacks Affirm Mobile Code Fear," LanTimes September 14, 1998.

Nelson, Matthew, "*BubbleBoy* Worm Infects without Opening File," InfoWord Services, November 10, 1999, available on-line at: http://infoword.com/.

Richardson, Robert, "Taking a Flying Leap," NetworkMagazine.com, December 1999, available on-line at: http://NetworkMagazine.com/.

IA Training

continued from page 25

course focuses on firewalls, with hands-on training on the Raptor-Eagle firewall. The final day includes an introduction to intrusion detection systems (IDS), with hands-on training on the Real Secure IDS. The primary aim of the router, firewall, and IDS training is to give the SAs and NMs hands-on training with these network security tools so that students know the tools' capabilities, although not necessarily how to use a specific tool or application.

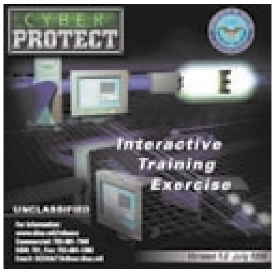
The main goal of the SAS and the NMS courses is to educate and train SAs and NMs in how to secure their information system platforms and networks. A secondary goal is to give students additional resources and reference material to help them secure their information systems at their duty stations. To support this secondary goal, in addition to the 2 weeks of training, each student is given handouts, including an NT security checklist and a UNIX security checklist, along with a CD that includes all class material and additional references and sources. The CSS has trained more than 1,000 personnel to the Phase 2 IA security certification level.

All three of the courses described above are continually changing because of the rapid changes occurring in operating systems, security tools, and regulations. The CSS remains committed to providing these courses; keeping them up to date; and helping ISSOs, SAs, and NMs win the IA battle.

Major Mark V. Hoyt may be reached at hoytm@gordon.army.mil.

DISA IPMO Products Promote Information Assurance Worldwide

Edward Smith



CyberProtect

The Defense Information Systems Agency (DISA) Information Assurance Program Management Office (IPMO) produces award-winning, interactive CD-ROMS and videos for use by information assurance (IA) professionals throughout the Department of Defense (DoD) and the Federal Government. With titles like Operational Information Systems Security (OISS), CyberProtect, and Federal INFOSEC Awareness, these CD-ROMs seek to enhance computer security awareness across all levels of every government agency, at no cost to the user. More than 175,000 of these products have been disseminated since July 1997.

Several IPMO products have been nominated for industry awards. CyberProtect was a big winner, taking two of *NewMedia* magazine's 1999 Gold Invision Awards (Best Overall Design and Technical Training) and the 1999 Cinema in Industry (CINDY) Competition Silver Award. CyberProtect also received a favorable review in *Federal Computer Week* in December 1999.

DISA and other defense organizations use a combination of OISS, DoD INFOSEC Awareness, and CyberProtect in the Level 1 certification of their system administrators. In fact, these products have been so successful in reaching and educating the end user that several Federal agencies have tailored IPMO CD-ROMs for use in their organizations.

New products are in the works, including Secret and Below Interoperability (SABI) and UNIX Security for System Administrators. These new courses will be Web delivered, cutting down on distribution costs and giving users instant Internet access to the information and to product updates.

Finally, the IPMO has developed an on-line, automated product order form that will allow paperless receipt and distribution of products. To order, the user simply fills out the form at our Web site and submits the order electronically to our shipping department. In most cases, the order will be sent out within a few hours. Best of all, the user can track the progress of the shipment using his or her order number or E-mail address.

To order CD-ROMs and videos at no charge, or to obtain a complete list of product descriptions, visit our new Web site at http://iase.disa.mil:88/ProductOrder.html or use the order form on the next page.

DOD INFOSEC Training and Awareness Products

Order Form

INFOSEC Program Management Office
5113 Leesburg Pike, Suite 110
Falls Church VA 22041-3204
Attn: Product Distribution

Commercial: 703-681-7944/3476 *DSN:* 761
Fax: 703-681-1386
E-mail: DODIAETA@ncr.disa.mil
Homepage: http://www.disa.mil/infosec

How did you hear about our products?

○ World Wide Web ○ Word of Mouth
○ *Conference ○ *Class ○ *Other

*Specify ____

Customer Information

Name ______________________________________ Title ____________________ Date __________

Command/Org/Agency ____________________________ Dept/Mail Code ____ Phone: (_____)____________ DSN ____

Address ____ Fax: (_____)____________________

City _________________________ State ____ Zip+4 ____________________ E-Mail ___________________________

NOTE: If you have ordered IPMO Products before and your address has changed, mark here ○

Mark appropriate organization:

○ OSD ○ Joint Staff ○ CINC (specify)_______________ ○ Army ○ Navy ○ Marines ○ Air Force ○ Coast Guard
○ Defense Agency (name)____
○ Non-Defense Agency (name)____
○ Government Contractor (Agency contracting with)___________________________
○ Other____

Order Form

Products are unclassified and available at no cost. Videos may be reproduced (for government use only) without further permission.

Multimedia CD-ROMs

○ DOD or... ○ Federal INFOSEC Awareness, V.1
(Select One)

○ Operational Information Systems Security
(OISS), Vols. 1 and 2, V.1.2 (Set of two)

○ Fortezza Installers Course for Windows NT 4.0, V.1

○ Introduction to the DITSCAP, V.1.1

○ Information Age Technology, V.1.03

○ IA for Auditors and Evaluators, V.1.04

○ Designated Approving Authority (DAA) Basics, V.1

○ CyberProtect, V.1 **New!**

○ System Administrator Incident Preparation & Response
(SAIPR) for Windows NT, V.1.1 **(for System Administrators) New!**

Videos

○ Understanding PKI (DOD) *(13 min)*

○ Networks at Risk (NCS) *(10 min)*
Information Front Line (IW) (IC) *(10 min)*
Bringing Down the House (IW)(NSA) *(11 min)*

○ Computer Security 101 (DOJ) *(11 min)*
Computer Security - The Executive Role (DOJ) *(9 min)*
Safe Data: It's Your Job (DOL) *(19 min)*
Think Before You Respond (US Gov) *(3 min)*

○ Protect Your AIS (US Gov) *(6 vignettes)*
Protect Your AIS, The Sequel (US Gov) *(30 min)*
Dr. D Stroye (US Gov) *(8 min)*
The Scarlet V (US Gov) *(7 min)*

○ Exploring MISSI (DISA/NSA) *(10 min)*

Upcoming Products

Information Operation Fundamentals - *Winter 99*
(Multimedia CD-ROM)

iatac chat

Leveraging the Institution

- What kind of documents do you collect?
- How do I find out about inquiries you've processed?
- What scientific and technical information (STI) has been developed through the TAT program?

Mr. Robert P. Thompson
Director, IATAC

These questions have been generated by our users as they seek answers to their Information Assurance (IA) requirements. To support our users demand for additional IA information, IATAC has introduced two new products to promote current awareness of IATAC products and services: Collection Acquisitions CD-ROM and the Quarterly Bulletin.

INFORMATION ASSURANCE
COLLECTION ACQUISITIONS
JUNE 2000
IATAC
E-mail: iatac@dtic.mil URL: http://iac.dtic.mil/iatac SIPRNET: http://iac.dtic.smil.mil
3190 Fairview Park Drive, Falls Church, VA 22042
DISTRIBUTION STATEMENT B

IATAC is chartered to collect IA-related STI. Our collection activities are focused on an established set of resources from the research and development (R&D), policy, acquisition, and operational communities that have traditionally produced IA-related STI. In an effort to transfer that knowledge to the IA community, IATAC has generated a CD-ROM of new acquisitions to the IA collection. Produced on a bi-annual basis, the initial Collection Acquisitions CD-ROM includes—

- Joint Vision 2020
- Kosovo After-Action Report
- Information Assurance Legal, Regulatory, Policy and Organizational Considerations
- Joint Staff Defense in Depth Brochure
- Defending America's Cyberspace National Plan for Information Systems
- And More....

To obtain a copy of the IA Collection Acquisitions CD-ROM, simply complete the IATAC order form (page 39) and fax it to us or download and complete the product form on the IATAC home page (http://iac.dtic.mil/iatac).

Information Analysis Centers (IACs) are structured such that other DoD organizations can leverage the results of previously acquired STI resulting from the inquiry process and the technical area task (TAT) program. The STI developed in response to technical inquiries are entered into the acquisition holdings for further access and use by other organizations with similar technical questions. In addition, the products developed through the TAT program are entered into the acquisition holdings and can be leveraged by other DoD users to address their IA requirements. Secondary distribution of TAT products are processed in accordance with distribution statements. To further disseminate information developed through the inquiry and TAT programs, IATAC is producing the Quarterly Bulletin that provides a summary of inquiries and identifies new STI developed through the TAT program. Contact IATAC via E-mail at iatac@dtic.mil to be added to the distribution list for the Quarterly Bulletin.

The IATAC Collection Acquisition CD-ROM and the Quarterly Bulletin are a result of IATAC's continuing examination of ways to better support the DoD IA Community and our continuing resolve to Support the Warfighter!

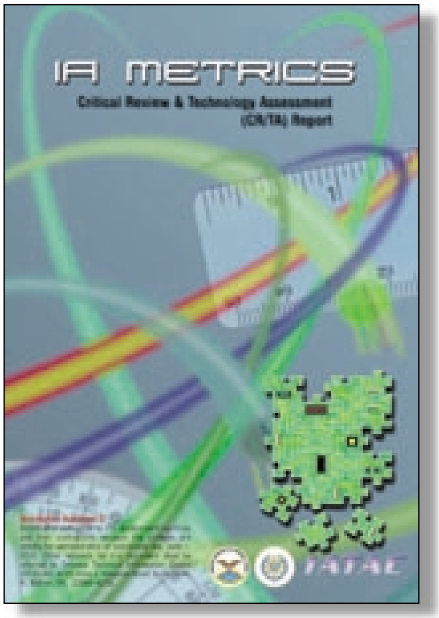
IO/IA Visualization Technologies

State of the Art (SOAR) Report

This report provides a synopsis of the information visualization industry, the industry's associated technologies, and visualization methodologies. It is written for a broad audience, principally for those unfamiliar with this technology, new to the industry, or seeking visualization capabilities for the first time. This report is written for system users. Visualization is, by nature, user-centric. Visualization technologies, for example, allow users to interact with information systems. Therefore, users must first understand what visualization is, what its capabilities and restrictions are, and what ideas factor into its use.

This SOAR should help readers decide whether visualization is appropriate to their needs, determine what types of visualization technologies are available and relevant, and formulate possible strategies for implementing a visualization solution. To order this report and our other products, complete the form on page 39.

IO/IA Visualization Technologies
State-of-the-Art Report (SOAR)
May 11, 2000
IATAC



IA Metrics CR/TA

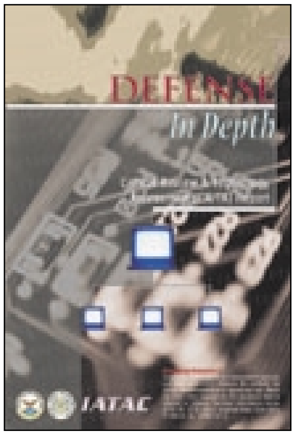
This report establishes the fundamentals of metrics development methodology and metrics program establishment. It answers the following questions:

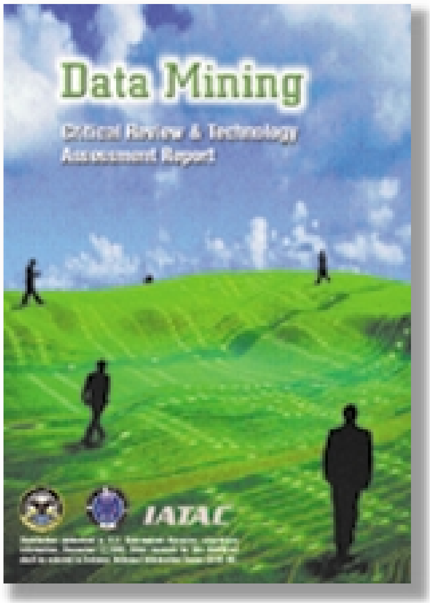
- What are IA metrics?
- Why do organizations need them?
- How can they be used?
- What is the process for developing IA metrics?
- What are some of the IA metrics already and what are their strengths/weaknesses?
- What is the future direction for IA metrics?

This report is intended to further facilitate the IA metrics discussion within the IA community, assist organizations in developing IA metrics, and provide guidance to organizations about how to establish their IA metrics programs. It provides examples of specific metrics that can be derived using the proposed methodology. The report also describes several ongoing metrics development, collection, and application efforts. A database of metrics, collected from multiple sources, is available from IATAC.

Defense in Depth CR/TA

This report describes the impact of evolving technology on the defense in depth strategy. The execution of the strategy requires a significant number of different security and networking technologies. This report focuses on examining the trends and giving an overview of the relevant technologies. It reviews the strategy and discusses its implementation in the Defense Information Infrastructure (DII). Key elements of the strategy and current implementation of the strategy are discussed.





Data Mining CR/TA

This report provides an overview of data mining techniques, applications, and COTS data mining software products. Data mining is used to discover previously unknown and meaningful relationships by sifting through large amounts of stored data. Data mining has applications in marketing, information assurance, risk management, and fraud management. To help users select a product that best meets their objectives, data mining tool evaluation criteria are provided. A table summarizing the features of available products is also provided.

Data Embedding for IA SOAR

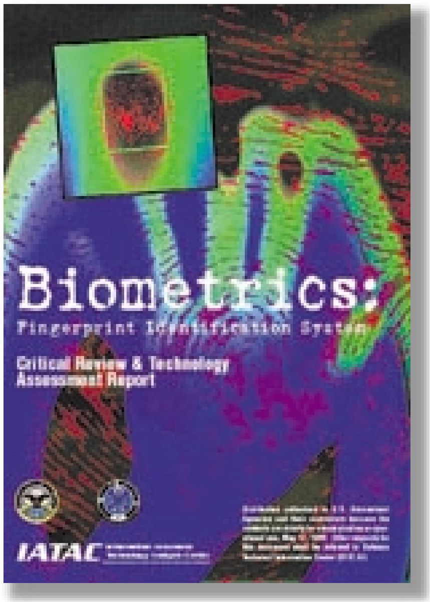
Provides an assessment of the state-of-the-art in data embedding technology and its application to IA. It is particularly relevant to: information "providers" concerned about intellectual property protection and access control; information "consumers" who are concerned about the security and validation of critical information; and law enforcement, military, and corporate organizations concerned about efforts to communicate covertly. The report has been specifically designed for readers who are not experts in data embedding. For more in-depth information, the bibliography provides an extensive list of authoritative sources from which the reader can obtain additional technical detail.

Computer Forensics—Tools and Methodology

This report provides a comparative analysis of currently available software tools used in computer forensic examinations. It provides a useful introduction to this specific area of science, and offers practical high-level guidance on how to respond to computer system intrusions. This report provides a useful analysis of specific products, including their respective capabilities, unique features, cost, and associated vendors.

Malicious Code Detection SOAR

This report includes is a taxonomy for malicious software providing a better understanding of commercial malicious software. An overview of the state-of-the-art commercial products and initiatives, as well as future trends is presented. The report presents observations and assertions to support the DoD as it grapples with this problem entering the 21st century. This report is classified and has a limited release.


Biometrics:
Fingerprint Identification System
Critical Review & Technology Assessment Report
IATAC

Biometrics: Fingerprint Identification Systems

Focuses on fingerprint biometric systems used in the verification mode. Such systems, often used to control physical access to secure areas, also allow system administrators access control to computer resources and applications. Information provided in this document is of value to anyone desiring to learn about biometric systems. The contents are primarily intended to assist individuals responsible for effectively integrating fingerprint identification products into their network environments to support the existing security policies of their respective organizations.

Order Form on Page 39

order form

IMPORTANT NOTE: All IATAC Products are distributed through DTIC. If you are NOT a registered DTIC user, you must do so PRIOR to ordering any IATAC products. TO REGISTER ON-LINE: http://www.dtic.mil/dtic/regprocess.html.

Name ______________________________ DTIC User Code ______________

Organization ______________________________ Ofc. Symbol ______________

Address ______________________________ Phone ______________________

______________________________ E-mail ______________________

______________________________ Fax ______________________

DoD Organization? □ YES □ NO If NO, complete **LIMITED DISTRIBUTION** section below.

LIMITED DISTRIBUTION

In order for Non-DoD organizations to obtain LIMITED DISTRIBUTION products, a formal written request must be sent to IAC Program Office, ATTN: Sherry Davis, 8725 John Kingman Road, Suite 0944, Ft. Belvoir, VA 22060-6218

Contract No. ______________________________

For contractors to obtain reports, request must support a program & be verified with COTR

COTR ______________________ Phone ______________________

IA Collection Acquisitions CD-ROM

□ June 2000

Critical Review and Technology Assessment (CR/TA) Reports

□ Biometrics □ Computer Forensics □ Defense in Depth □ Data Mining

□ IA Metrics □ Modeling & Simulation

IA Tools Report

□ Firewalls □ Intrusion Detection (2nd Ed.) □ Vulnerability Analysis (2nd Ed.)

State-of-the-Art Reports (SOARs)

□ Data Embedding for Information Assurance □ IO/IA Visualization Technologies

□ Malicious Code Detection [□ TOP SECRET □ SECRET]

Security POC Security Phone

UNLIMITED DISTRIBUTION

Newsletters *(Limited number of back issues available)*

□ Vol. 1, No. 1 □ Vol. 1, No. 2 □ Vol. 1, No. 3

□ Vol. 2, No. 1 □ Vol. 2, No. 2 (soft copy only) □ Vol. 2, No. 3 □ Vol. 2, No. 4

□ Vol. 3, No. 1 □ Vol. 3, No. 2 □ Vol. 3, No. 3 □ Vol. 3, No. 4

Please list the Government Program(s)/Project(s) that the product(s) will be used to support: ______________________

____

____

Once completed, fax to IATAC at 703.289.5467

calendar

September

13–14

Biometric Consortium 2000 Conference
Gaithersburg, MD.
http://www.nist.gov/pblic_affairs/confpage/000913.htm

25–28

e-Gov 2000
Alexandria, VA
www.e-gov.com

27–28

Second Annual Commonwealth of Virginia Information Technology Symposium
Lexington, VA. Held at the Virginia Military Institute.
http://csrc.ncsl.nist.gov/events/

October

3–5

AFIWC Information User's Conference
San Antonio, TX
POC: SSgt Kari Garcia
210.977.2870, DSN: 969

11–12

The Hacker Phenomenon: Tools and Penetration Techniques
Atlanta, GA
http://www.infowar.com/conf/00/conf_080700a_j.shtml

17–19

DoD Security Managers' Conference
Williamsburg, VA
http://www.sctymgrconf.com

24–26

Third Information Survivability Workshop
Boston, MA. Sponsored by IEEE Computer Society and the US State Department.
http://www.cert.org/research/isw.html

November

8–9

Army IA Industry Days 2000
Hilton Hotel, Crystal City, VA
at Reagan National Airport
POC: Mr. Zadil Ansari
703.604.6865, DSN: 664

12–13

DoD PKI Users Forum
Las Vegas, NV
http://www.iaevents.com

IATAC

Information Assurance Technology Analysis Center
3190 Fairview Park Drive
Falls Church, VA 22042