REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	Summer 1999	Newsletter Vol. 3 No. 1

4. TITLE AND SUBTITLE
IA Newsletter
The Newsletter for Information Assurance Technology Professionals

5. FUNDING NUMBERS

6. AUTHOR(S)
Information Assurance Technology Analysis Center

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

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

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Defense Technical Information Center
DTIC-IA
8725 John J. Kingman Rd, Suite 944
Ft. Belvoir, VA 22060

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for public release; distribution is unlimited.

12b. DISTRIBUTION CODE

A

13. ABSTRACT ***(Maximum 200 Words)***

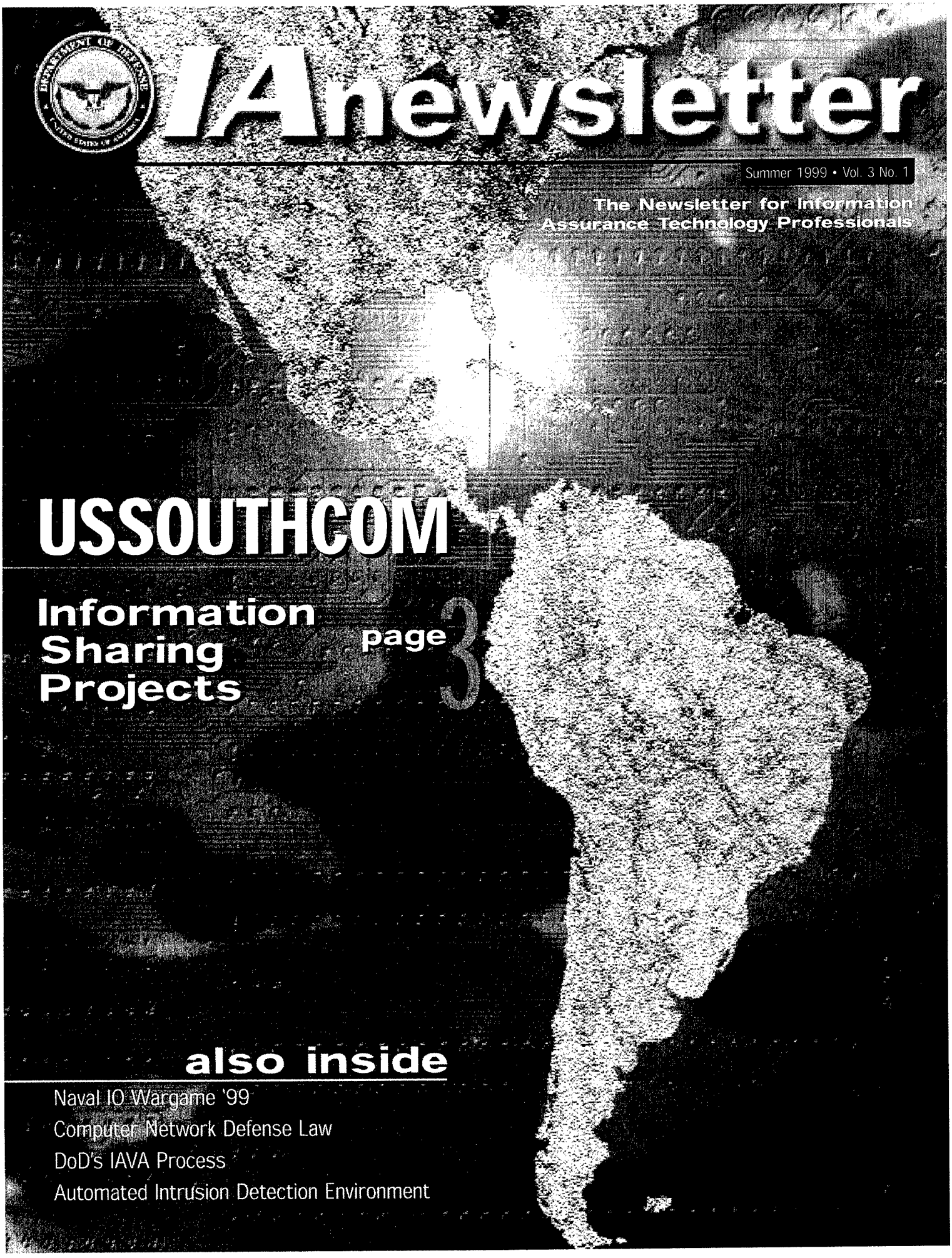
IA Newsletter is published quarterly by the Information Assurance Technology Analysis Center (IATAC). IATAC is a DoD sponsored Information Analysis Center, administratively managed by the Defense Technical Information Center (DTIC), Defense Information Systems Agency (DISA). Featured in the issue:
USSOUTHCOM - Information Sharing Projects
Naval IO Wargame '99
Computer Network Defense Law
DoD's IAVA Process
Automated Intrusion Detection Environment

14. SUBJECT TERMS
Information Security, Information Assurance, Intrusion Detection, Information Operations

15. NUMBER OF PAGES
23

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	None



IAnewsletter

Summer 1999 • Vol. 3 No. 1

The Newsletter for Information Assurance Technology Professionals

USSOUTHCOM Information Sharing Projects

page 3

also inside

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 Weinhold
Information Collection
Alethia A. Tucker
Inquiry Services
Peggy O'Connor
Contributing Editor
Martha Elim

IA Newsletter 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

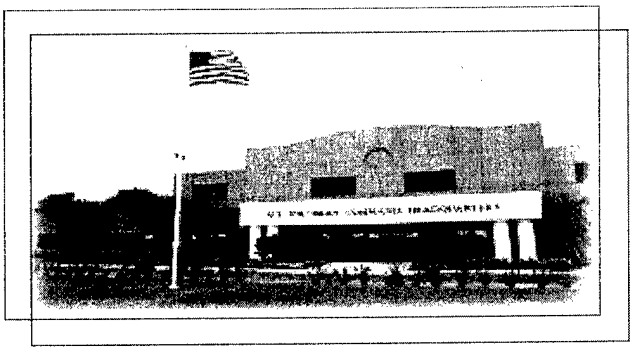
E-mail: iatac@dtic.mil
URL: http://iac.dtic.mil/iatac

Cover and newsletter designed by Christina P. McNemar

United States Southern Command's Information Sharing Projects

Lt Col J. Andrew Pettigrew, III, USAF

The U.S. Southern Command (USSOUTHCOM) pursues a Strategy of Cooperative Regional Peacetime Engagement founded on hemispheric cooperation. The strategy emphasizes the importance of regional, collaborative, multilateral approaches and the value of communications. Essential to this strategy is sharing information with nations in the USSOUTHCOM Area of Responsibility (AOR). Accordingly, USSOUTHCOM is establishing information-sharing networks using the existing theater infrastructures such as the Internet and commercial satellite connectivity as the supporting communications backbone. The Americas' Net (AMNET), modeled after the Partnership for Peace initiative in Europe, is the most mature of the information-sharing networks that support USSOUTHCOM's regional engagement strategy. The Caribbean Information-Sharing Network (CISN) is being developed. Finally, the Southern Command Information Exchange System (SCIES) network, also in development, will support the exchange of releasable classified information with AOR nations.



AMNET consists of an Americas' Net file and E-mail server, a home page, and Internet connectivity for the U.S. Military Groups (USMILGP) and participating nation senior military leadership in the USSOUTHCOM AOR. By automating information-sharing and communications, it creates an environment conducive to regional cooperation in the Americas and the Caribbean. It provides a framework for enhanced political and military cooperation and facilitates interaction for joint multilateral activities, such as humanitarian and civic assistance, nation building, and peacekeeping. The system allows member nations to share lessons learned immediately, participate in planning exchanges directly, coordinate exercise development on-line, and make direct doctrinal comparisons.

AMNET archives its mission by using Internet resources. An array of Web browser-accessible software and user-friendly tools afford participating nations password-protected access to, and exchange of information concerning a variety of subjects, such as security strategies, emergency planning, professional military education, multilateral exercises, doctrine and policies, public affairs, and environmental concerns. Fully operational since May 1997, AMNET has been continually upgraded to meet evolving regional engagement requirements. The Internet Web site was established with Secure Socket Layer (SSL) and password protection. By using Cold Fusion as a back-end Web application server, AMNET manages and delivers information dynamically. The Web site offers extensive links to U.S. military home pages, Latin American Web resources, military schools, countries of interest, briefings, and fact sheets. Additional features include a Web-integrated real-time chat room, a bulletin board with threaded discussion groups and E-mail notification, and a search engine. AMNET also provides E-mail capability. Planned AMNET enhancements include modernizing equipment, bandwidth, and network infrastructure. Password authentication with user access levels for each page in the site is being developed. This feature will add security by enabling users to see only what their access level allows.

USSOUTHCOM headquarters is assisting military forces and law enforcement agencies in the Caribbean Basin of the USSOUTHCOM AOR in establishing an information-sharing network to enhance bilateral and multilateral cooperation in combating transnational threats and

continued on page 4

continued from page 3

addressing issues of common concern. The CISN network will be established in three phases: Phase 1, encrypted E-mail and attachments; Phase 2, Virtual Private Network (VPN) with a central server implementation; Phase 3, VPN with multiple servers.

CISN Phase 1, already operational, enables users to encrypt E-mail and attachments using PGP (Pretty Good Privacy®), a commercial software application from Network Associates, Inc. CISN Phase 2 will implement a VPN and a Collaborative Virtual Workspace (CVW) server. Initial operational capability for Phase 2 is scheduled for October 1999. The VPN will be an encrypted communications link between CISN remote workstations and the CISN intranet that passes through the public Internet. The VPN will use a combination of authentication, data encryption, and tunneling to create a secure channel between users and the CISN network. The VPN will rely on remote access accounts that allow the users to dial in to an Internet service provider (ISP), establish a connection to the Internet, and then identify themselves to the CISN VPN authentication system. The CISN VPN will verify a user's identity on the basis of user name and password. On successful authentication, tunneling or an encrypted session will be set up between the VPN user and the CISN VPN server, thus protecting the privacy and integrity of data exchanged between the remote workstation and the CISN intranet.

USSOUTHCOM is also developing a multilevel security network, SCIES, to share counterdrug planning, intelligence, and operations data with participating nations in the theater. The system will consist of off-the-shelf hardware and software connected to existing local area networks via approved multilevel security devices and firewalls. Specific functions to be accomplished through SCIES include scheduling and approval for diplomatic clearance of overflights and sharing of the releasable portions of counterdrug intelligence data and the Global Command and Control System (GCCS) Common Operating Pic-

continued on page 21

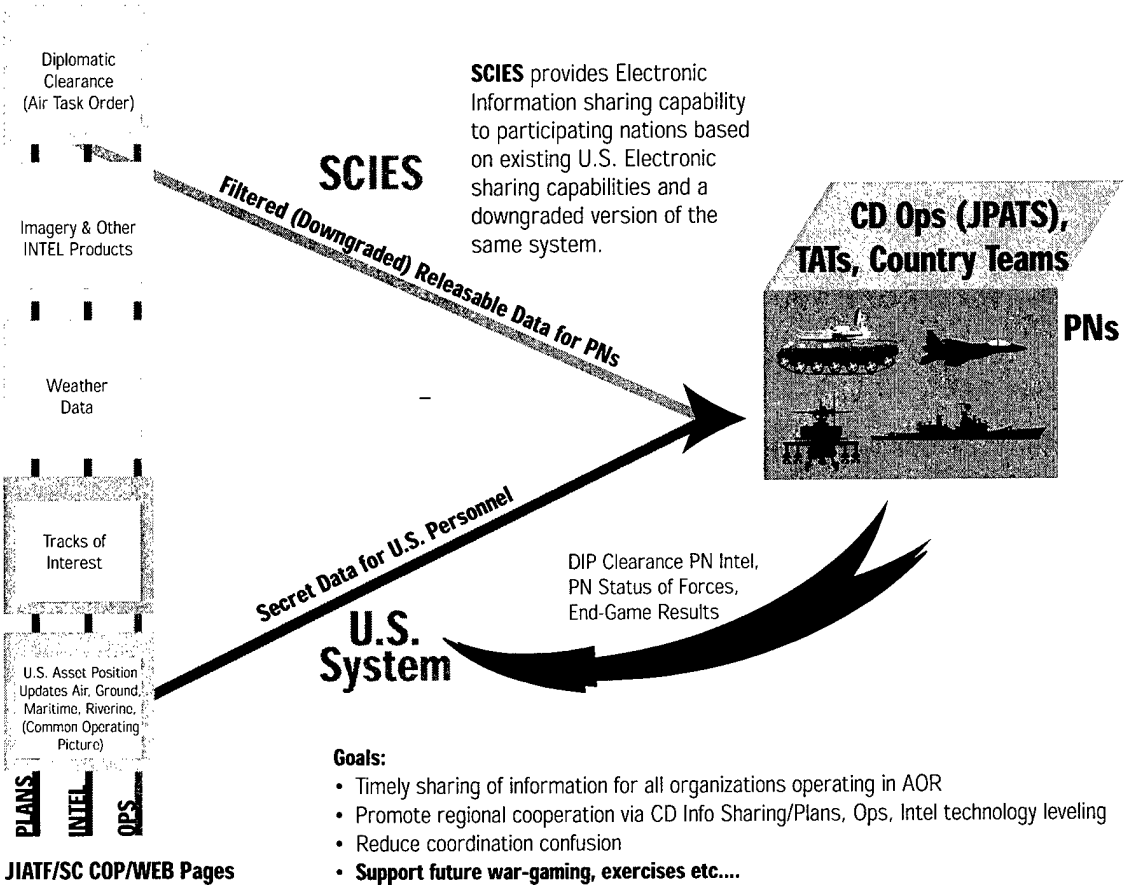


Figure 1. SCIES Goals and Concept of Operations

A Brief Look at the Law of Computer Network Defense

■ Lt Col Charlie Williamson, USAF

You may have heard the rumor: Technology makes computer network defense difficult enough. Then along comes some lawyer saying you can't protect your networks the way you want. Perhaps this article will give you some encouragement. It briefly reviews some of the rules and suggests that the situation might not be as bad as rumor indicates.

Most readers of this newsletter know the threat described in the 1997 report of the President's Commission on Critical Infrastructure Protection. Computer networks can undergo anonymous cyber attacks that can be mounted remotely in minutes with little or no detectable preparation or rehearsal. Over the last few years, the threat has increased. More countries have announced plans to develop information warfare capabilities and the technology used to mount these attacks is more readily available and easier to use than ever before. Likewise, many companies are fielding new technologies that protect online privacy but also make it harder to track hackers. In these circumstances, how do we defend our networks?

We can choose many courses of action. The passive options are easy. We can shut down our networks or divert the attacker, if we know the attacker is coming and how he will attack. Active options are also easy. Arrest him (if he's domestic) or use the full weight of national power (if he's sponsored by a foreign state), if we can find him. The hard choice is to get the right information to the decision makers so they can take the right action. Meeting that challenge can look like transforming the puzzle on the right of Figure 1 to the one on the left.

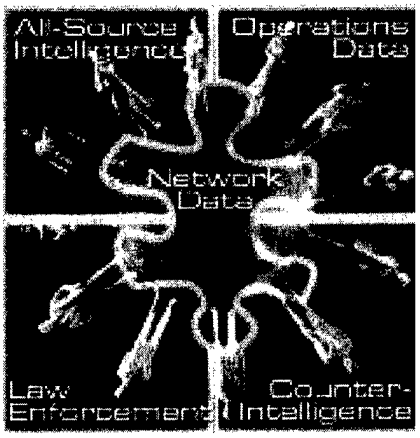


Figure 1. The Law (and culture) as we would like it ▲ and as it appears ➤.

How do we make the puzzle pieces fit? This article looks briefly at some tools that help pull the pieces together: the Computer Fraud and Abuse Act, the Electronic Communications Privacy Act, the fourth amendment to the U.S. Constitution, intelligence oversight rules, counterintelligence guidance, and some international initiatives.

Overview of Domestic Criminal Law

We must start by understanding that computer intrusions are crimes, most of which are governed by the Computer Fraud and Abuse Act (Title 18, United States Code, Section 1030). The law is summarized below, but the details of particular cases can lead to complications, so consult your lawyer. The punishments for each offense vary depending on the seriousness of the intent or outcome.

With this brief definition of what conduct is criminal, we can turn to ways of catching the hacker. The first line of defense is often the Electronic Communications Privacy Act

(ECPA) and its "service provider" exception (Title 18, United States Code, Section 2511). Generally, ECPA makes it illegal to wiretap and provides stiff penalties for violations. However, it sensibly allows electronic communication service providers to protect their rights and property by intercepting successful and attempted hacking. This provision is the legal foundation for deploying intrusion detectors and databases. DoD network operators are then supposed to report suspected intrusions to

continued on page 6

continued from page 5

Service law enforcement agencies.

At this point, the Constitution triggers significant procedural requirements. First, the fourth amendment may require a search warrant if the computer owner is entitled to expect privacy. However, the U.S. Supreme Court has acknowledged a lowered expectation of privacy in certain workplace situations, so a warrant may not be required to search a government computer. Also, certain government employees may consent to network server searches. Check with your lawyer for guidance.

Statutes also impose requirements. Certain statutes address access to subscriber information and communications stored by Internet service providers (ISP). Consult your lawyer for help in these complicated areas. In addition, investigators can use pen register devices and trap-and-trace devices to track source and destination addresses on packets going through computers. If these devices do not yield sufficient information, investigators can deploy full-content wiretaps. However, consent or court orders are required, and the procedures can be complicated. The defense criminal investigating organizations implement these rules by following DoD 0-5505.9-M, Procedures for Wire, Electronic, and Oral Interceptions for Law Enforcement, May 1995. Be sure to consult your lawyer for help in these complicated areas.

Rather than face all these problems, why don't we just have some smart military operators "hack back" at the hacker's computer? First, if the hacker's computer is in the United States, those military operators could be accused of violating the Computer Fraud and Abuse Act. If the ISP is foreign, our military operators will probably need approval from the National Command Authorities, but that discussion is beyond the scope of this article. Second, our operators have to find the target. To trace the hacker attack back to its source, they would normally need to contact some ISPs between themselves and the target. If an ISP does not cooperate, do they hack into the ISP and steal its log data? Obviously, this tactic is a bad idea. It's clearly wrong; it's a crime; and it would take even longer than using the legal process. Finally, suppose our smart military operators succeed in finding the hacker and erasing his hard drive. The hacker immediately reloads his hard drive from a CD-ROM and hacks again minutes later. It may be frustrating from a military viewpoint to work through the law enforcement process, but often this may be the only way to develop enough information to identify and stop the intruder.

Section	Prohibits . . .
(a)(1)	Hacking into a government computer to get classified information and then disclosing it
(a)(2)	Hacking into computers to obtain access and information
(a)(3)	Accessing and affecting the use of nonpublic computers of the U.S. Government and government contractors
(a)(5)	Hacking and causing damage (more than a $5,000 loss of data or system availability to one or more victims during any 1-year period); intentionally, recklessly, or simply causing damage; including viruses
(a)(6)	Trafficking in stolen passwords
(b)	Attempting any of the offenses listed above

Table 1. Computer Fraud and Abuse Act Summary

Overview of Intelligence and Counterintelligence Rules

Foreign state threats naturally concern DoD even more than domestic threats because of a state's potential to concentrate resources. At the same time, intelligence operators must be able to gather and analyze data without treading on U.S. citizens' rights. *(This area can become convoluted very quickly, so, again, consult your lawyer.)*

DoD balances these concerns by complying with significant oversight rules that apply to the intelligence community and counterintelligence elements of the U.S. Government. The primary statute is the Foreign Intelligence Surveillance Act (Title 50, United States Code, Sections 1801–1829). It allows high-level administrative approvals for foreign surveillance, but requires court orders for electronic surveillance in counterintelligence opera-

tions against U.S. citizens suspected of espionage. It establishes significant procedural requirements similar to wiretap court orders under ECPA. In addition, the court must conclude there is probable cause that the target is an agent of a foreign power. Probable cause can often be difficult to establish, especially early in a hacking case. In addition, significant guidance on intelligence activities affecting U.S. citizens comes from Executive Order 12333, Dec 1981; DoD Directive 5240.1, Apr 1988; and DoD 5240.1-R, Dec 1982. Because these rules greatly predate the Internet, their use of phrases like "electronic surveillance" and "concealed monitoring" merits cautious analysis. Finally, the intelligence community agencies each have regulations to guide their collection and dissemination actions. The key point is that the mission of the intelligence community is to gather and disseminate intelligence on foreign threats and leave domestic threats to law enforcement and counterintelligence. As a result, DoD decision makers may not get "one-stop shopping" when trying to figure out where a hacker comes from. This area, too, can become convoluted very quickly. Again, consult your lawyer.

International Initiatives

What happens when we do find a foreign hacker? The unpleasant reality is that many countries do not even outlaw hacking. For instance, New Zealand, one of our close allies and a sophisticated country, is outlawing hacking only this year. Many countries that outlaw hacking do not make it an offense that allows extradition to the United States. Furthermore, U.S. punishments may be so mild that extradition may not be worthwhile. All of these factors makes investigation and prosecution either difficult or impossible.

Two initiatives may improve this situation. First, the Group of 8[1] is negotiating a "fast-freeze" agreement that would enable one country to have another order ISPs freeze data while law enforcement seeks evidence across borders. Second, the Council of Europe is negotiating an agreement that may require signatory nations to pass laws making certain computer conduct criminal, providing for extradition for certain offenses, and allowing cross-border access to evidence.

What Can You Do?

Now that you have seen this brief outline, what can you do? First, tell the intelligence community members what products you want. They want to produce useful intelligence, and they need real cases for analysis to see what can and cannot be done. Second, use the ECPA "service provider exception" to widely, but wisely, deploy intrusion detection systems and share databases. Third, commanders and network operators need to seek case status from their law enforcement and counterintelligence agents. This information will lead to security improvements. Finally, commanders and investigators should work closely with their lawyers. Make them write their opinions and alert them they will be working in Information Operations cells. Lawyers need to start working now to come up to speed in this challenging area.

Conclusion

An old Gypsy curse says, "May you live in interesting times." These are interesting times for law as we enter the Information Age. New problems need new thinking and team effort, but the end result—national security—is worth the hard work.

Endnote

1. The Group of 8 (G-8) was established in October 1975 to facilitate economic cooperation among the developed countries (DCs) that participated in the Conference on International Economic Cooperation (CIEC), held in several sessions between December 1975 and June 1977. Membership includes Canada, France, Germany, Great Britain, Italy, Japan, Russia, and the United States.

Lt Col Charlie Williamson is currently the Staff Judge Advocate (SJA) for the Joint Task Force-Computer Network Defense (williamc@jtfcnd.ia.mil). He previously served as the SJA of the 314th Airlift Wing, Little Rock AFB, Arkansas. He had previous JAG assignments at Castle AFB, California, and Minot AFB, North Dakota, along with an assignment as a flight test manager at Hill AFB, Utah. He received his juris doctor from the University of Utah College of Law and his bachelor of science in mechanical engineering from the University of Southern California.

DoD's IAVA Process

Helping Mitigate Network Security Risk to the Defense Information Infrastructure

"Establishing trust in a highly distributed, network-centric computing environment is a fundamental issue today for the Department of Defense and its Defense Information Infrastructure (DII). Widely known and documented vulnerabilities exist throughout the networks and because of our increasing reliance on networks, these vulnerabilities have the capacity to severely degrade our operational readiness and therefore endanger national security. We must shift the current view that information assurance/systems security concerns are secondary considerations to core readiness issues. Everyone—from the highest senior levels of management to the soldiers and office workers—must understand their responsibility as a stakeholder in the vitality and security of our information systems."

—Dr. John Hamre, Deputy Secretary of Defense

Lieutenant Beth A. Evans, USN
DISA D333

The Department of Defense (DoD) Computer Emergency Response Team (CERT), a branch within the Defense Information Systems Agency (DISA), is responsible for providing information assurance procedures and guidance to the DoD community for protection of the Defense Information Infrastructure (DII). Accordingly, the Deputy Secretary of Defense instituted a notification process in 1998 known as the Information Assurance Vulnerability Alert (IAVA) process and designated DISA as its manager. The IAVA process was created because DoD recognized the need for the Commanders-in-Chief (CINC), Services, and Agencies (C/S/A) to have a positive control mechanism to ensure that their system administrators received, acknowledged, and complied with vulnerability alert notifications and to ensure that corrective actions were taken against new and critical vulnerabilities.

IAVA is a Web-based process that incorporates identification and evaluation of new vulnerabilities, disseminates technical responses, and tracks compliance within the DoD community. As the IAVA process manager, DISA is responsible for disseminating the vulnerability notifications to C/S/A points of contact and providing an automated means for the points of contact to report receipt of and compliance with the alerts.

Managing the IAVA Process

DoD CERT has created a three-tiered "vulnerability hierarchy" for notifications. The first-tier notification, an alert or IAVA, is disseminated when DoD CERT documents a new vulnerability that poses an immediate, potentially severe threat to DoD systems. The IAVA requires that C/S/As report both receipt of the alert (after disseminating it to subordinate organizations) and their compliance with the corrective action(s).

The second-tier notification, a bulletin or IAVB, addresses new vulnerabilities that do not pose an immediate threat to DoD systems, but are significant enough that noncompliance with the corrective action could escalate the threat. Like the IAVA, the IAVB requires C/S/As to report receipt of the bulletin, but compliance reporting is not required (compliance requirements and decisions are made by the local commander). However, the IAVB must be disseminated down to the system administrator level within the organization.

The third-tier notification, the technical advisory, is generated when new vulnerabilities exist but are generally cat-

egorized as low risk. Potential escalation of these vulnerabilities is deemed unlikely, but the advisories are issued so that any risk of escalation in the future can be mitigated. Reporting is not required in response to a technical advisory.

The IAVA process allows waivers of the required compliance actions to be granted in response to a specific alert. Waivers are reviewed and granted by a C/S/A's Designated Approval Authority (DAA). The DAA must consider the risks involved, to both the local network and the greater DII, when granting a waiver.

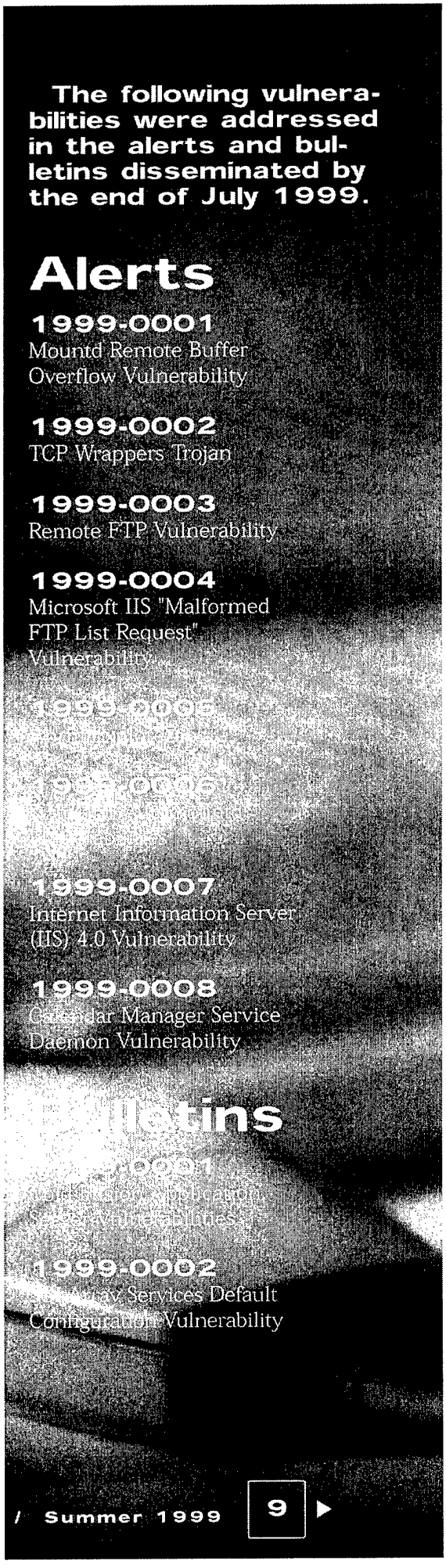
Determining Notification Type

The DoD CERT learns of new vulnerabilities through incidents reported to DoD and civilian CERTs, public Internet resources, and vendor notifications. On notification of a new vulnerability, DoD CERT assesses the threat that the vulnerability poses to the DII using criteria such as the type of operating system and infrastructure affected by the exploit, the access gained by the exploit, the number of exploits reported, and the nature of the exploit's potential end result (denial of service, for example).

After the initial evaluation, a request for comments is sent to a coordination team consisting of the Joint Task Force–Computer Network Defense, Service CERTs, and joint system program managers. This team provides input in determining the type of notification to be generated. After coordination, the notification is disseminated in a variety of ways. Record message traffic (Automatic Digital Network [AUTODIN] and Defense Message System [DMS]) is sent releasing an IAVA or IAVB to the C/S/A points of contact. The message is primarily for notification purposes, as well as assignment of reporting timelines. The message directs recipients to the DoD CERT Web site (http://www.cert.mil) for technical specifics and corrective action(s). An E-mail containing the technical information is also disseminated to all IAVA list serve addressees for the IAVA, IAVB, and technical advisories. List registration can be requested by sending an E-mail to cert@cert.mil. Dissemination is restricted to .mil and .gov domains.

The reporting of receipt, compliance, and waiver information is accomplished via the unclassified or classified IAVA Web site. Normal reporting timelines are 5 days for reporting receipt (IAVA and IAVB) and 30 days for reporting compliance (IAVA). Significant progress is being made in the automation of receipt acknowledgement and compliance reporting, and as of October 1, 1999 C/S/As have access to a greatly improved utility, providing a more robust and effective automated mechanism to report their status information.

LT Beth A. Evans, USN is the Technical Analysis Division Chief for the DoD Computer Emergency Response Team, Defense Information Systems Agency, Arlington, Va. She received her B.S. in Business Administration from the University of California, Berkeley, CA in December 1990. LT Evans is currently pursuing her M.S. in Information Systems from George Mason University, Fairfax, Va. She may be reached at evansb@ncr.disa.mil.



Naval IO Wargame 1999

■ Daniel R. Walters

On June 8–10 the Naval Information Operations Wargame 1999 (NIOW '99) attracted participants from the Fleet Commander in Chief (CINC), Numbered Fleet, Carrier Battle Group (CVBG), Amphibious Ready Group (ARG), and Marine Expeditionary Unit (MEU) staffs. Including observers, more than 85 participants from 29 joint and naval commands took part in the wargame.

Personnel from the Fleet Information Warfare Center (FIWC), together with technical staff from the Information Assurance Technology Analysis Center (IATAC), facilitated this seminar. The game was held at the Shifting Sands Conference Center, located at the Fleet Combat Training Center, Atlantic, Dam Neck, Virginia Beach, Virginia.

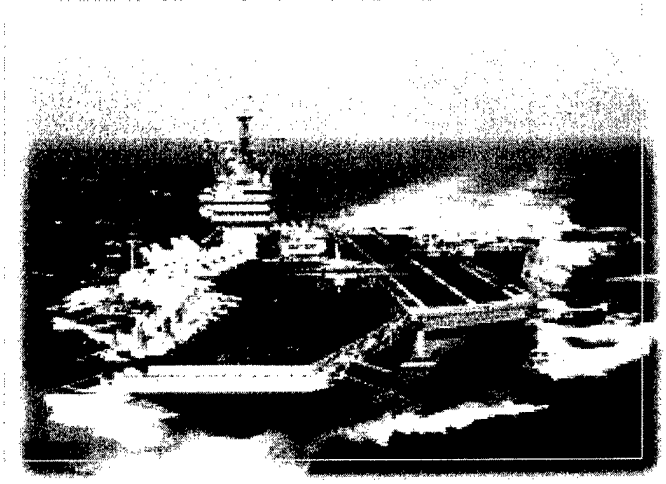
NIOW '99 goals were to examine operational and tactical information operations (IO) planning at the CVBG and ARG/MEU level and to assess Naval IO Mission-Essential Tasks (NMETs). To achieve these goals, the wargame had four objectives:

- To educate participants and provide a professional forum to discuss and evaluate current and future naval IO issues
- To evaluate several IO-related issues resulting from the information warfare (IW) at Sea Conference held at FIWC in March 1999
- To identify and document IO Mission-Essential Tasks (METs) and doctrine issues arising from the game
- To generate and disseminate operational and tactical IW guidance to support IW staffs deployed and ashore, consistent with FIWC's role as the Naval IW Center of Excellence.

The wargame structure included informational briefings, team play, and "hot washups." On June 8, a series of information and background briefings educated the players and prepared them for the game play.

Following briefings on strategic and joint IO policy, naval IW, and FIWC IW initiatives, the players were separated into three teams, one representing a CVBG IW staff, a second representing an ARG/MEU IW staff, and the third representing the IW interests of both Numbered Fleet and Fleet CINC staffs. A fourth team of experienced IO personnel from joint and DoD commands functioned as game play mentors, data collectors, and observers. The principle portion of the wargame occurred on June 9–10 as the players participated in three moves. Each move began with in-depth briefings on the intelligence scenario, the current situation, and the operational or tactical IO mission the players were to plan. In Move 1, the players considered tactical IO planning for routine operations in a Southwest Asia scenario. Move 2 presented the players with operational and tactical IO planning for nonpermissive Noncombatant Evacuation Operation (NEO) operations in a crisis scenario with the CVBG and ARG/MEU acting as a joint task force. Finally, Move 3 involved the players in conducting an evaluation of IO-specific METs as a result of their planning efforts during Moves 1 and 2.

The moves all concluded with debriefings by each team to summarize the team's perspective on IO planning for



USS Theodore Roosevelt (CVN 71) aircraft carrier. U.S. Navy photograph by Photographer's Mate 2nd Class George A. DelMoral.

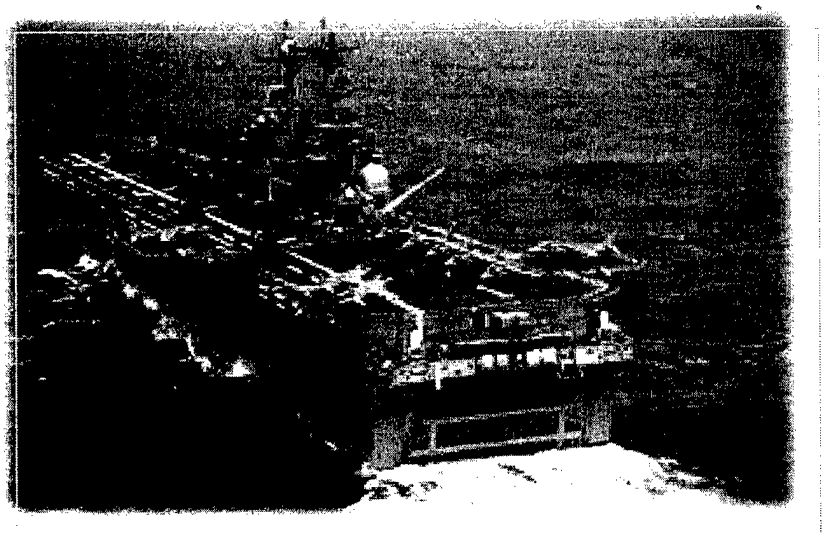
the scenario, evaluate its capability to plan and execute IO at the operational and tactical levels of conflict, and offer feedback on Naval IO METs. The hot wash focused on capturing lessons learned from the game. Participants reached consensus on a number of key points, some of which are summarized as follows:

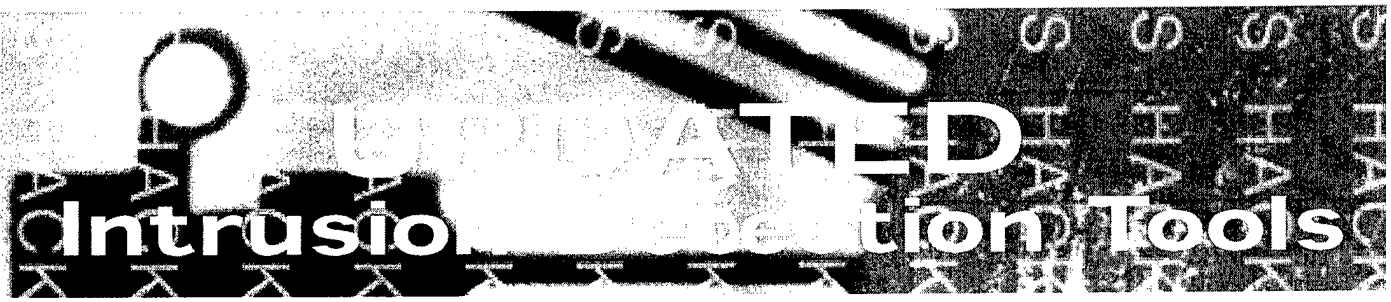
- IO planning is a difficult process, and areas of responsibility for coordination and execution of IO are unclear, especially at the CVBG and ARG/MEU level.
- IO planning for the CVBG and ARG/MEU must start long before operations commence and must be integrated throughout the Inter-Deployment Training Cycle (IDTC).
- The need to integrate IO in all operations is critical. Key to IO integration is development and implementation of significantly improved IO planning tools at the numbered fleet, CVBG, and ARG/MEU level.
- Planning requirements and responsibilities for tactical IO planning and for a joint task force differ significantly.
- Current intelligence production requirements are not focused to support IO requirements.
- Naval personnel need more IO training and education than they now receive.

Analysis of participant feedback indicated that NIOW '99 was educational and productive, providing an outstanding forum for evaluating the naval IO planning process and METs. Most participants said that the game was an effective overview of naval IO planning and that they left with an increased appreciation and understanding of CVBG and ARG/MEU IO coordination issues. Because of the success of the first naval IO wargame, FIWC plans to conduct games on an annual basis to explore various aspects of naval IO.

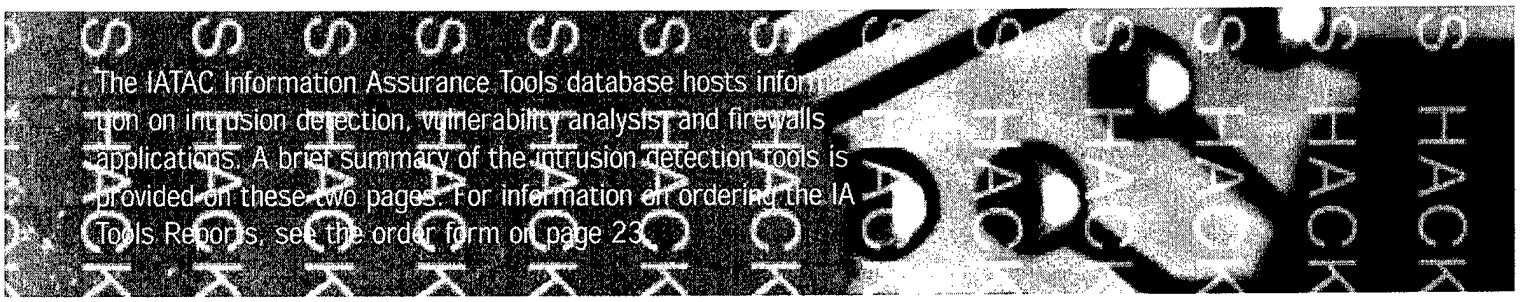
All wargame material, including a list of game participants, all briefings, team debriefings, the wrap-up message, and post wargame slide presentation, are available on the FIWC Secret Internet Protocol Router Network (SIPRNET) Web site (www.fiwc.navy.smil.mil). Questions and comments are welcomed and encouraged.

Daniel R. Walters is Technical Director, Fleet Information Warfare Center Norfolk, VA. He is also serves as Captain, U.S. Navy Reserve Crisis Response Planner for the Office of Secretary of Defense, Personnel and Readiness, Readiness and Training Plans and Policy Division. He received his B.S. in Chemistry from Wilkes University in 1972 and graduated from the Naval War College in 1997. He may be reached at td@fiwc.navy.mil.





TITLE	COMPANY	URL
AAFID	Purdue University	http://www.cs.purdue.edu
ACME	Intermidia	http://www.intermidia.icmc.sc.usp.br
AID	Brandenburg University	http://www-rnks.informatik.tu-cottbus.de
ALVA	GE Corporate R&D	http://www.crd.ge.com
Alert-Plus	Computer Security Products	http://www.compsec.com
Argus	Carnegie Mellon University	ftp://ftp.sei.cmu.edu/pub/argus/argus-1.7.beta.1e/
ARMD	George Mason University	http://www.isse.gmu.edu/~jllin/system
ARPMon	University of Illinois	http://www-commeng.cso.uiuc.edu/docs/jacques/software/arpmon.html
ASAX	University of Namu	http://www.info.fundp.ac.be/~cri/DOCS/asax.html
ASIM	U.S. Air Force	http://www.afiwc.aia.af.mil/
Black Ice	Network ICE	http://www.networkice.com/products/blackice
Bro	Lawrence Berkely Laboratory	http://www.aciri.org/vern/bro-info.html
Centrax	CyberSafe Corporation	http://www.centrax.net/products.html
CMDS	SAIC/ODS Networks Inc.	http://www.cmds.net
CyberCop	Network Associates	http://www.nai.com/asp_set/products/tns/cybercop_intrusion.asp
Dragon	Network Security Wizards	http://www.network-defense.com/dragon.html
EMERALD	SRI International	http://www.csl.sri.com/emerald/index.html
Flight Jacket	Anzen Computing	http://www.anzen.com/afj/
Gabriel	Los Altos Technologies	http://www.lat.com/gabe.htm
GrIDS	University of CA—Davis	http://olympus.cs.ucdavis.edu/arpa/grids/welcome.html
Hummer	University of Idaho	http://www.csds.uidaho.edu/~hummer/
Ifstatus	IBM	http://www.ers.ibm.com/~davy/software/ifstatus.html
INTOUCH INSA	Touch Technologies, Inc.	http://www.ttisms.com/tti/nsa_www.html



TITLE	COMPANY	URL
IST	Internet Security Systems	http://www.iss.net/prod/isb.php3
ITA	AXENT Technologies, Inc.	http://www.axent.com/product/smsbu/ITA/default.htm
JiNao	MCNC/NCSU	http://www.anr.mcnc.org/JiNao.html
KSM	RSA Security, Inc.	http://www.rsasecurity.com/products/intrusion/
NADIR	Los Alamos National Lab	http://wwwc3.lanl.gov:80/cic3/home/projects.html
Net Stat	University of CA—Santa Barbara	http://www.cs.ucsb.edu/~kemm/netstat.html/
NetRanger	Cisco Systems, Inc.	http://www.cisco.com/warp/public/cc/cisco/mkt/security/
NFR	Network Flight Recorder, Inc.	http://www.nfr.net
NID	Lawrence Livermore Lab	http://ciac.llnl.gov/cstc/nid/nid.html
NIDES	SRI International	http://www.sdl.sri.com/nides/
NOCOL	Marquette University	http://www.mscs.mu.edu/contact.html
POLYCENTER	Compaq Computer Corp	http://www.digital.com/info/security/id.htm
PreCis	PRC Inc.	http://www.bellevue.prc.com/precis/index.htm
RealSecure	Internet Security Systems	http://www.iss.net/prod/rs.html
SecureNet PRO	MimeStar, Inc.	http://www.mimestar.com
Session Wall-3	Computer Associates	http://www.abirnet.com/sw3intro.html
Snort	Stanford Telecommunications, Inc.	http://www.clark.net/~roesch
Stake Out	Harris Corporation	http://www.stakeout.harris.com/
Swatch	Stanford University	http://www.stanford.edu/~atkins/swatch
Tripwire	Tripware Security Systems	http://www.tripwiresecurity.com
T-sight	En Garde Systems, Inc.	http://www.engarde.com/software/t-sight/index.html
UNICORN	En Garde Systems, Inc.	http://www.EnGarde.com/~mcn/unicorn.html
USTAT	University of CA—Santa Barbara	http://www.cs.ucsb.edu/TRs/TRCS93-26.html

Automated Intrusion Detection Environment

■ Brian T. Spink
Brad Jobe

Increased reliance on information systems requires maximum system integrity. Although absolute system integrity is not achievable, it is possible to warn commanders of attempted system attacks in real time. This warning has limited utility if it concerns only the local level. Effective defensive information operations (DIO) entails a comprehensive understanding of system operations on a global level. A critical DIO component is the ability to warn of suspicious activities across various command levels. The objective is to secure local networks, detect coordinated attacks at designated regional levels, and enhance the global picture of real-time threats to DOD-wide systems. The Automated Intrusion Detection Environment (AIDE) is designed to address the challenge of determining whether the information grid is under attack.

AIDE's goal is to reduce false positive reporting and create a tactical warning capability across the warfighters' information grid. To this end AIDE will create a multitiered integration environment, incorporating stand-alone sensors and correlating sensor information at different command echelons. AIDE leverages existing commercial off-the-shelf (COTS) and government off-the-shelf (GOTS) technologies that include intrusion detection, enterprise management, object-oriented design, process visualization, and knowledge engineering.

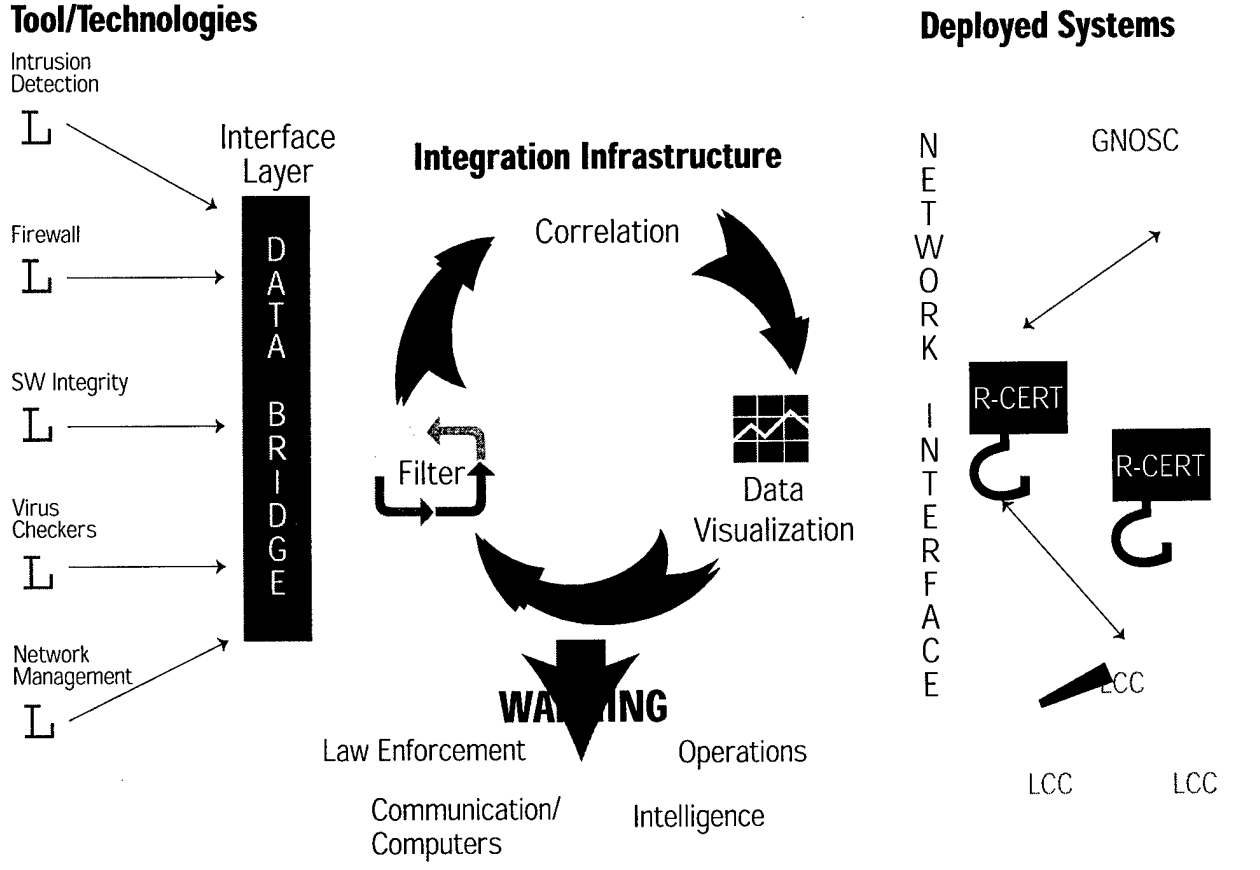


Figure 1. Architecture of the AIDE System

AIDE Architecture

The AIDE architecture shown in Figure 1 is composed of sensors, sensor interfaces, normalization, integration environment, data storage, and the communication topology. An AIDE goal is to incorporate whatever sensors are in place at an installation, rather than prescribing certain sensors. To determine the desired baseline of intrusion detection, network management, and firewall products, an AIDE team surveys installation sites. Once it identifies the sensors, the sensor interfaces to send data to the AIDE integration environment are developed.

Gensym's G2 intelligent enterprise management software creates the basic integration infrastructure. This software applies real-time rule-based reasoning to network management data, activity sensor data, and intrusion detection information derived from distributed sources in real time.

Raw sensor data and correlated event information are stored in an Oracle database. Users from local, regional, and global sites can gain access to detailed data from the Web server installed on the system. This feature allows the system to push small amounts of information, while allowing users at all levels to pull the supporting data they need to the appropriate level.

The communication topology requires secure hierarchical and lateral reporting. The overall AIDE concept calls for three-tier reporting: local control centers (LCC) report to regional computer emergency response teams (R-CERT), which report to a global network operations and security center (GNOSC). Figure 2 depicts the hierarchical reporting structure. Systems at each level can also report laterally (LCC to LCC, or R-CERT to R-CERT).

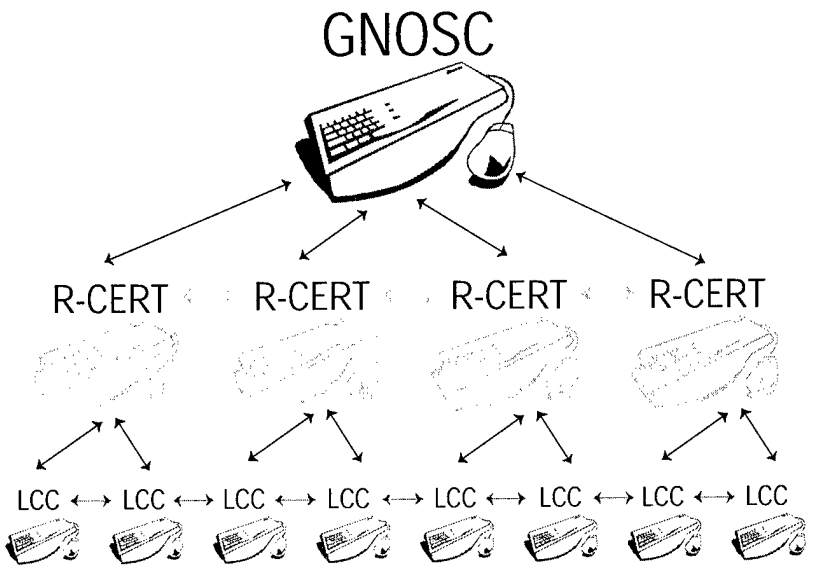


Figure 2. Hierarchical Reporting Structure

Each node in the system can be dynamically configured to send its alerts to any or all of the other nodes in the network. A node receives all alerts sent to it (that is, the configuration specifies only outbound constraints). This capability allows AIDE to be customized to conform to each site's reporting policy.

Improving Network-wide Detection

Network connectivity significantly improves the ability to detect network-wide, coordinated attacks. Individual sites can detect local intrusions in isolation, but regional centers can correlate intrusions reported by multiple local sites. This function is actually the major purpose of an R-CERT. When more than one local site reporting to the same R-CERT reports intrusive behavior, the R-CERT AIDE operator can immediately compare the behaviors and draw conclusions about the nature of the attack. This capability allows the R-CERT to alert its other LCCs that an attack may be forthcoming and provide a consolidated report to the GNOSC.

The GNOSC can serve the same function, correlating events at local sites that report to different R-CERTs. The GNOSC provides a single perspective on the state of the entire network covered by the AIDE system. It can alert sites to intrusions as they are happening, so administrators can take immediate action to limit any damage and reduce the attack's effectiveness.

Brian Spink is an electronic engineer with the Air Force Research Laboratory in Rome, NY. He received his B.S. ECE from Clarkson University and his M.S. ECE from Syracuse University. He may be reached at spinkb@rl.af.mil.

Brad Jobe is a senior program analyst for Litton PRC in Rome, NY. He received his B.S. from South Dakota State University and his M.B.A. from Colorado State University. He may be reached at jobeb@rl.af.mil.

NEW infosec training products

The Information Assurance Program Management Office (IPMO) at the Defense Information Systems Agency (DISA) now offers the training and awareness CD-ROMs and videos listed in this article. Use form to order ➤

CD-ROMs

CyberProtect—An interactive computer network defensive exercise that looks and feels like a video game. It is intended to familiarize players with information security (INFOSEC) terminology, concepts, and policy. Players learn about defensive security tools and seek to deploy them judiciously on a simulated network. They face a spectrum of security threats and must make practical decisions about allocating resources (in quarterly increments) using risk analysis and risk management considerations. Play is divided into four sessions, simulating a fiscal year. After each session, players receive feedback on how well they are doing. At the end of the last session, players are given a report summarizing their cumulative operational readiness rating. The report also details every attack by type, origin, and effectiveness of defensive tools.

System Administrator Incident Preparation and Response for Windows NT—is an interactive multimedia training CD-ROM. It provides a virtual hands-on experience, taking the student through the steps necessary to configure networks to collect and protect event information that may be useful for investigating suspected unauthorized activity. The user learns what techniques are often used to commit computer crimes, what information to collect before an incident, how to prepare systems for possible incidents, how to implement policies, how to log and recognize unauthorized activity, and how to respond to suspected unauthorized activity. Other topics covered include policies and procedures to simplify a computer emergency investigation, audit strategy, audit implementation, recognition of unauthorized activity, and security incident notification and response strategies. A glossary of terms and links to service and agency computer emergency response teams are provided for reference. This CD-ROM is a product of the DoD Computer Investigations Training Program (DCITP).

VIDEOS

Protect Your AIS: The Sequel—This U.S. Government video dramatizes INFOSEC-related concerns in the workplace. The scenes demonstrate the need for password protection, virus prevention, data safeguards, user identification (ID) security, and controlled access to computer equipment. (30 minutes)

Dr. D. Stroye—This U.S. Government video discusses correct methods for magnetic media destruction, while providing humorous examples of how not to destroy data safely. (8 minutes)

The Scarlet V—This U.S. Government video discusses the need to use virus-scanning software on a regular basis to prevent file infection. It comically depicts the life of an individual who inadvertently introduces a virus into a networked system. (8 minutes)

Safe Data: It's Your Job—This Department of Labor video is relevant to DoD because it focuses on the need to safeguard sensitive but unclassified data, such as medical records and personnel files. It discusses ways to secure data to prevent sensitive information from getting into the wrong hands and emphasizes the role of the end user in computer and network security. It also offers tips for preventing data from being compromised by hackers and unauthorized users, such as good password management, virus protection, and physical security. (19 minutes)

Think Before You Respond—This NRO video deals with Internet security, stressing the need for viewers to be careful about the information they share. It encourages caution when discussing topics in live chat sessions or responding to requests for information. (3 minutes)

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)

To register for the IA Newsletter, visit http://www.iatac.dtic.mil/products.htm

rev. 23 Sept 99

SilentRunner™

Thomas Hudson
Michael Maloney

SilentRunner™ is a network security tool kit recently released by Raytheon. It is a passive, multifunctional network discovery, visualization, and analysis (DVA) system that provides real-time auditing and monitoring. The analytical engine replicates network activity and provides a wide variety of two- and three-dimensional (2D, 3D) views to enhance users' understanding of complex networks.

Operationally, SilentRunner™ maps topology and displays network data for analysis. It shows network activity and links information concerning each terminal. It also shows both physical and virtual relationships, who contacts whom, communication paths, and traffic flow and density. SilentRunner™ can play back recorded data sequences for detailed network analysis and can integrate other types of data to provide a complete picture of the activity under investigation. For example, SilentRunner™ may receive external sensor data inputs and present the inputs in a common view with the network data. External sensor data such as physical security logs, private branch exchange (pbx) logs, and intrusion detection probe data have successfully been assimilated, displayed, and analyzed. SilentRunner™ can be used for post-intrusion analysis, complementing administrative network security efforts. As described below, the DVA modules use both data and meta-data to perform context analysis on reconstructed information.

SilentRunner's software tool kit has four patent applications pending. The system is composed of six discrete software modules and is available in two versions (laptop computer and enhanced workstation). The software modules are the collector module (CM), knowledge base (KB) data parsing, analytical engine (AE), display, man-machine interface (MMI), and external sensor (ES). The enhanced workstation provides more analytical capability than the deployable laptop and includes 3D-display visualization, recorded data playback, and context analysis.

CM is the application's front end. It contains a family of autonomous, passive, local-area-network (LAN)-monitoring data acquisition tools. Additional tools for wide-area-network (WAN), computer code, and network heuristics are under development. The CM LAN tool collects data, presents 2D displays, and stores the formatted data for the subsequent modules. This very robust module updates the 2D displays and databases in real time while providing packet decoding for up to 2,500 simultaneously active terminals without interfering with the host network (Figure 1). SilentRunner™ dynamically graphs the network topology, reconstructs sessions for seven standard protocols, and identifies and labels unknown packets. It incorporates operator-definable Boolean queries for alerts and displays network activity levels statistically for individual protocols and terminals on the network.

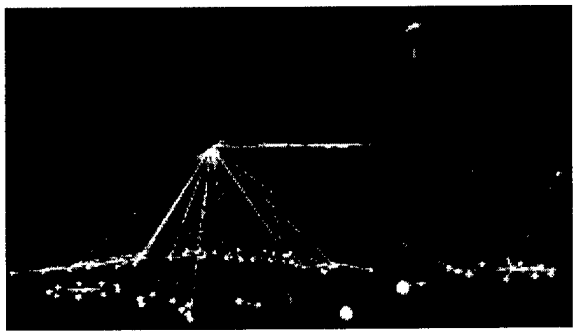


Figure 1. SilentRunner' network view shown in 2-D.

The KB data parsing module uses a family of algorithms to transform the data stored in CM into formatted categories that the analytical engine modules require. The module currently consists of eight independent selectable functions, with each function having many selectable sub-functions. Major parsing modules are parse, E-mail, join, Web tool, graphics, summing, file tool, and column. Parse formats traffic data into 15 selectable options. For example, parse can sort data by domain, host, Internet Protocol (IP) address, MAC address, and other fields. The join, Web tool, graphics, summing, file tool, and column parsing modules have similar sorting capabilities.

AE is the dynamic graphic module that accepts data from the KB data-parsing module and presents an array of relational data sets in a 2D display. The module's basic function is to render large (hundreds of megabytes) data files into visual representations that convey meaningful information about the data. This module consists of two distinct sub-modules that run on different platforms. On the laptop, AE operates in a Microsoft Windows NT environment, whereas the enhanced workstation is a Unix platform. Compared with the laptop, the enhanced workstation has a higher central processing unit (CPU) speed, giving it greater analytical power and additional analytical features such as network traffic playback, context analysis of text, and graphics.

The 3D display module acquires data from the enhanced AE or KB data parsing modules. The analyst specifies a third axis for display purposes. This module can capture and display in 3D a variety of complex relational data sets that would be obscured by traditional 2D display methods. The module can display a large number of nodes, up to 10,000 simultaneously. The node diagrams are produced by using node implode and explode techniques. The imploded diagram maintains full functionality with respect to every node in the original diagram. Animation of the nodal diagram, a unique feature, permits different types of network traffic to be shown as colored icons as the traffic moves between nodes while the operator rotates the entire node diagram to any position.

MMI and ES are the last two modules in the SilentRunner™ architecture. The MMI software provides the operator with a user-friendly interface. This module also controls equipment configuration, data collection, data storage, visualization, and analysis. ES integrates external data for DVA purposes.

SilentRunner™ should complete the National Security Agency (NSA) Security Proof-of-Concept Keystone (SPOCK) verification by mid-November 1999. SPOCK verification is conducted by an NSA-sponsored consortium of government system integrators and commercial information security (INFOSEC) solution developers that meet regularly to discuss emerging solutions and enabling technologies. When unique tools like SilentRunner™ are introduced, the consortium forms a team to verify vendor claims. The final SPOCK report on SilentRunner™ should be published before year-end. The Raytheon Lithicum office is responsible for developing and sustaining SilentRunner™.

Tom Hudson is the Director of Integrated Information Systems with Raytheon Systems Company. A retired Army Intelligence Officer, he received a Masters in Computer Science and Civil Engineering from West Virginia University. He was the Deputy Director of the Army Land Information Warfare Activity (LIWA), 1994/98. He may be reached at thudson@re-ro.com

Mike Maloney is the inventor and lead IR&D program manager for this project at Raytheon Systems Company. Prior to joining Raytheon, Mike was a Technical Director at the National Security Agency (NSA). While at NSA he was involved in the design and development of all types of collection and processing systems. In 1978 he received his M.S. in Engineering from George Washington University and has an B.S. in Electronic Engineering from the University of Detroit. He may be reached at m5m@hrb.com.

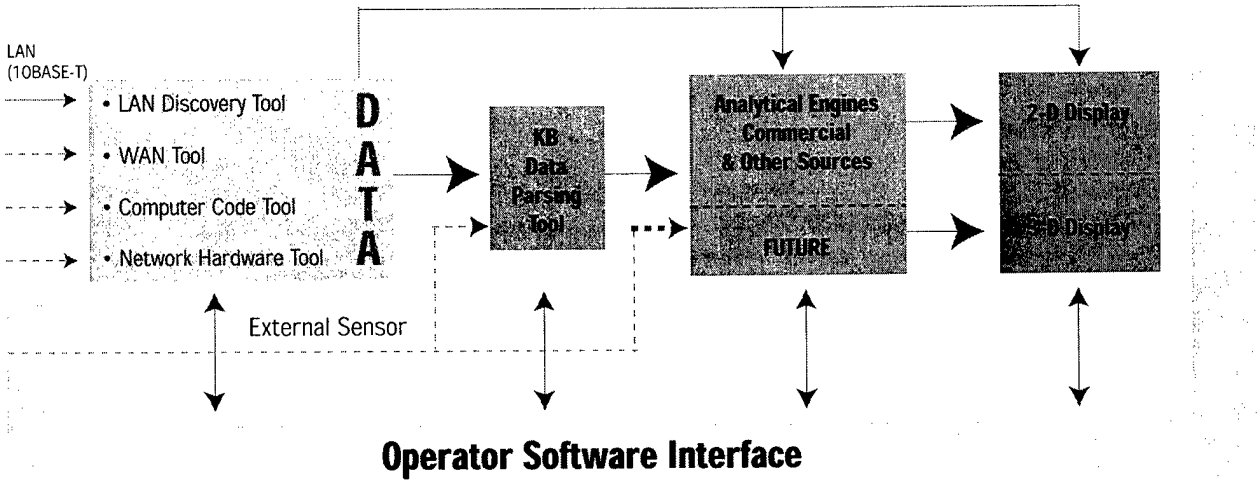
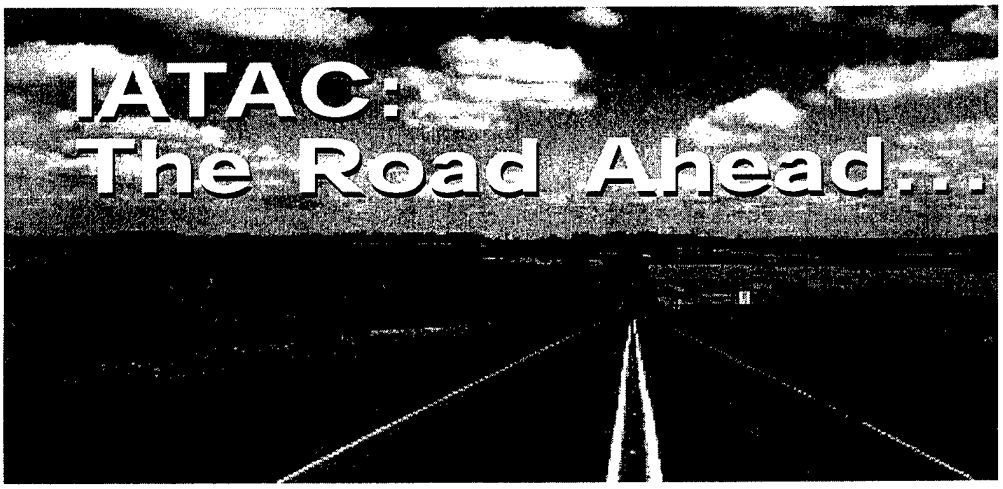


Figure 4. SilentRunner' network DVA Tool.

IATAC: The Road Ahead...



Mr. Robert P. Thompson
Director, IATAC

The IATAC Steering Committee recently convened to review ongoing activities and provide technical guidance and direction for future IATAC operations. In addition, the steering committee also provides a forum to discuss critical issues, facilitate the exchange of ideas, and build upon the expanding knowledge-base for information assurance and defensive information operations. Committee members represent the broad DoD Information Assurance community to include operations, policy, research and development, and soon to include acquisition elements. As a result of the meeting, IATAC has undertaken several new initiatives to enhance operations and respond to emerging warfighter needs. These initiatives include the following:

Information Assurance (IA) Newsletter

IATAC will transition to electronic distribution of the IA Newsletter. Hard copies of the newsletter will be available upon request and at conferences and symposia.

Collection Activities: Insider Threat

IATAC has increased its collection activities on the "insider threat." Collection activities focus on the technology aspect of the insider threat and not necessarily on social engineering or the human element. Specifically, what tools, technologies, or research and development activities are available that can be applied to respond to the insider threat problem.

IA Tools Reports

The scope of the IA Tools Reports (e.g., Intrusion Detection, Vulnerability Analysis, Firewalls) will change from its current format of providing descriptions of tools to an improved format that focuses on the evaluation of individual tools. IATAC will provide short descriptions of the tool, reference evaluations conducted by other DoD entities and possibly commercial reviews, and provide an assessment of state-of-the-art for that particular technology.

Technical Report: Visualization

Warfighters are inundated with massive amounts of data related to network monitoring and intrusion detection. This data must be fused and cross-referenced with intelligence data as well as technical intrusion data. To address this data fusion problem, IATAC will conduct a survey and develop a state-of-the-art report (SOAR) on visualization technologies and its application to information operations and information assurance.

Technical Report: Defense-In-Depth

Security architecture associated with Defense-In-Depth requires further definition. IATAC will develop a technical report that focuses on emerging technologies that support a Defense-In-Depth strategy (e.g., at User, System Administrator, Enclave, and Network levels).

Technical Report: What is Good Enough Security?

IATAC will develop a report that examines information assurance metrics and security architectures that answer the question—how do you know your security is any good?

For more information on IATAC initiatives, contact Bob Thompson at 703.289.5454 or via e-mail at iatac@dtic.mil.

The IAnewsletter Hits Cyberspace

The IAnewsletter will be available for electronic distribution (pdf format) beginning with the Fall 1999 issue. Please take a moment and either E-mail (iatac@dtic.mil) or fax (703.289.5467) your format preference for receiving future issues of the newsletter, including the following information:

Full Name: _____

Mailing Address: _____

_____

E-mail Address: _____

I would like to receive: ❑ Electronic ❑ Hard copy

USSOUTHCOM

continued from page 4

ture. The system will initially be bilateral between the United States and participating nations (PNs) but can later be expanded to multilateral if all participants agree.

Like all the USSOUTHCOM information-sharing networks, SCIES is intended primarily to expedite event coordination, promote data sharing between United States and participating nations, encourage bilateral and multilateral data sharing, increase the effectiveness of U.S. support to participating nations' operations, and, most importantly, promote regional cooperation. These networks provide a cost-effective approach to achieving these objectives through the use of information technology to share information and disseminate it to participating nations.

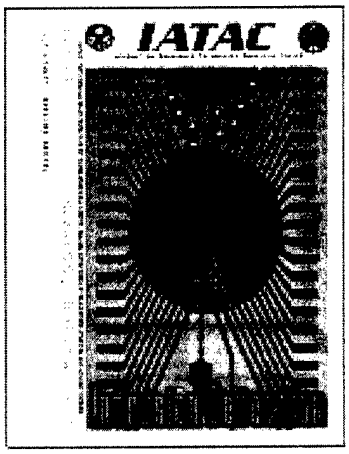
IATAC readers may access AMNET by visiting the Americas' Net home page at http://www.reddelasamericas.net. The following identifier and password will allow readers access: user name, iatacguest; password, 67Pm3Rp8.

Lt Col Pettigrew is the Chief, Information Assurance Division, Directorate of Command, Control Communications Computers and Intelligence (C4I), USSOUTHCOM. He received his B.S. from King College in Bristol, TN and his M.S./M.I.S. in 1987 from the University of Arizona, Tucson. Lt Col Pettigrew may be reached at pettigrj@reddelasamericas.net.

products

Intrusion Detection Tools Report

This newly updated report provides an index of intrusion detection tool descriptions contained in the IA Tools Database. Research for this report identified 47 intrusion detection tools currently employed and available.



Data Embedding for Information Assurance SOAR

Provides an assessment of the state-of-the-art in data embedding technology and its application to information assurance. 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 those desiring 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

The primary focus of this report is a comparative analysis of currently available software tools that are used in computer forensic examinations. For readers who are unfamiliar with computer forensics, this report provides a useful introduction to this specific area of science, and offers practical high-level guidance on how to respond to computer system intrusions. For all readers, however, this report provides a useful analysis of specific products, including their respective capabilities, unique features, cost, and associated vendors.

Firewall Tools Report

This report provides users with a brief description of available firewall tools and contact information. Currently the IA tools database contains 46 firewall tools that are available in the commercial marketplace.

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.

Modeling & Simulation Technical Report

This report, released December 1997, describes the models, simulations and tools being used or developed by organizations within DoD. Data collection efforts focused on the definitions of Information Operations, Information Warfare, and IA as described in DoD Directives S-3600.1 and 6510.1 As well as the definitions prescribed by DMSO for model and simulation.

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 those individuals who are responsible for effectively integrating fingerprint identification products into their network environments to support the existing security policies of their respective organizations.

Vulnerability Analysis Tools Report

This report summarizes pertinent information, providing users with a brief description of available tools and contact information. Currently the IA Tools database contains descriptions of 35 tools that can be used to support vulnerability and risk assessment.

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 _____

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 _____

Technical Reports
❑ Biometrics ❑ Computer Forensics ❑ Modeling & Simulation

IA Tools Report
❑ Firewalls ❑ Intrusion Detection ❑ Vulnerability Analysis

State-of-the-Art Reports
❑ Data Embedding for Information Assurance

❑ 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

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

October

19- 20

Visit us at booth #903

Information Systems Security Expo (ISSE) '99
Arlington, VA
Call J. Spargo & Associates
703.631.6200

20- 29

TechNet Europe '99
Renaissance London
Heathrow Hotel
http://afcea.org/tne99/default.htm

26

ShadowCon
NSWC Dahlgren, VA
Call 877.921.0612
www.TechnologyForums.com

October 31- November 3

Visit us at booth #412

MILCOM 1999
Into the Next Millennium-
Evolution of Data Into Knowledge
Atlantic City, NJ
www.milcom1999.com

9

Fort Lewis/DISC4 Information Assurance Workshop & Accreditation Program
Tacoma, WA
Call 877.921.0612
www.TechnologyForums.com

15- 17

26th Annual Computer Security Conference & Exposition
Washington, DC
Marriott Wardman Park
www.gocsi.com

16- 18

TechNet Asia-Pacific '99
Honolulu, HI
Call J. Spargo & Associates
703.631.6200

December

1- 2

Space & Missile Systems Center Information Assurance Technology Forum
San Pedro, CA
Call 877.9210612
www.TechnologyForums.com

8- 9

The Colorado Springs Military Information Assurance Technology Forum
Colorado Springs, CO
Dec. 8th - Schriever AFB
Dec. 9th - Peterson AFB
Call 877.9210612
www.TechnologyForums.com

February

8- 10

DISA 4th Annual IA Workshop
Holiday Inn Hampton Hotel
Hampton, VA

9- 11

AFCEA West 2000
San Diego Convention Center
San Diego, CA

22- 25

Come See Our Booth

SPACECOM 2000
Space Communications- Key to Information Operations
Colorado Springs, CO
Call Michael J. Varner
719.590.1051

April

3-5

InfoSec World Conf & Expo
Orlando, FL
Call 508.879.7999
www.misti.com

25- 27

Come See Our Booth

Fiesta Informacion 2000
San Antonio, TX
Call J. Spargo & Associates
703.631.6200

IATAC

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