IAnewsletter

The Newsletter for Information Assurance Technology Professionals

Volume 4 Number 4 • Winter 2001/2002

CYBER TERROR

Potential for Mass Effect

also inside

- DoD IA Acquisition Initiatives
- PACOM TCCC Update
- Building the LE/CI COP
- Biometrics & Smart Card Integration

contents

on the cover

ia initiatives

in each issue

IAnewsletter

Editor
Robert J. Lamb
Creative Director
Christina P. McNemar
Art Director
Ahnie Senft
Illustrations
Maria Candelaria
Information Processing
Abraham T. Usher
Inquiry Services
Peggy O'Connor

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 J. Lamb
Director, IATAC
703.289.5454

Submitting Articles

To submit your related articles, photos, notices, feature programs, or ideas for future issues, please request an author's packet from—

IATAC
Christina P. McNemar
3190 Fairview Park Drive
Falls Church, VA 22042
Phone 703.289.5454
Fax 703.289.5467

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

Article Deadlines

Spring 2002	15 February 02
Summer 2002	17 May 02
Fall 2002	16 Aug 02

Cover design: Maria Candelaria
Original newsletter design: Christina P. McNemar

IATAC chat

by Mr. Robert J. Lamb, IATAC Director

With the tragic events of 9-11, the ensuing anthrax spread, and the war on terrorism DoD and Government are faced with an ever increasing new threat—Cyber Terror. While terrorists' plans have traditionally involved physical attacks, DoD's increasing reliance on a highly interconnected information grid translates into a growing possibility that terrorists could elect to employ computer network attacks. As the Internet has expanded and DoD's reliance on it increased, protests and political activism have entered a new realm. Political activism on the Internet has already generated a wide range of activity, from using E-mail and Web sites to organize, to Web page defacements and denial-of-service attacks. This edition of the *IAnewsletter* features two articles which address this evolving threat.

Exploring Biotechnology

The recent U.S. tragedy and the on-going War on Terrorism has generated increased interest in biotechnology. IATAC, in support of OSD Net Assessment has over the past year researched new biotechnologies and has summarized their findings in the form of a detailed report which OSD has released to the senior leadership throughout DoD, including the Secretary of Defense and the Vice President. Given the events, the interest, and where we are as a nation, IATAC is publishing the report as a Critical Review and Technology Assessment (CR/TA) to provide for its wider exposure. The report, although sensitive, is not classified. We will therefore not post it to our Web site, but requests for hard copies may be made via E-mail.

Recently IATAC assumed responsibility for publishing the IO Calendar. For years Don St. John at DIA did an outstanding job with the calendar. Operational demands and time constraints precluded the upkeep, so IATAC proposed we undertake its management. Published bi-weekly and included in the IA Digest, this calendar summarizes upcoming conferences and training across DoD and Government. If you are interested in either receiving the calendar or posting an upcoming event, please let us know via E-mail at iatac@dtic.mil.

There are a wide variety of interesting articles in this edition of the *IAnewsletter*, which I commend to you, from the DIAP to the LE/CI Center at the Joint Task Force for Computer Network Operations and an update on the PACOM TCCC published a year ago. We continue to receive a diverse set of articles across the spectrum of the IA and IO domains. As always we are interested in continuing to share your thoughts and ideas in this forum. Please visit our Web site to download an author's packet if you are so inclined. ■

Cyber Terror— Potential for Mass Effect

One incident can have a catastrophic ripple effect around the globe

by LTC Ed Sbrocco, Mr. Tom Ward, and Mr. Chris Baden

Terrorist organizations like al Qaeda have indicated the intent to inflict as much physical and psychological damage on their perceived enemies as possible. While terrorists' plans have traditionally involved physical attacks, our increasing reliance on a highly interconnected information grid translates into a growing possibility that terrorists could elect to employ computer network attacks as a means of achieving a mass effect on a targeted population. In the aftermath of the 11 September attacks and in the current dynamic threat environment, there are increasing concerns about predicting, preventing, or mitigating damage from such attacks. This article provides a brief overview of why and how cyber terror might be employed as an act of mass effect. Some key terms are defined, a few real and fictitious scenarios are briefly examined, and some mitigating factors are discussed.

Definitions

There are no universally shared definitions yet for terms like cyber terrorism or weapon of mass effect. As such, the ongoing debate over definitions is beyond the scope of this article. However, for the purposes of discussion this article defines cyber terrorism and weapon of mass effect as follows—

- **Cyber Terrorism:** Under the USA Patriot Act of 2001, Title 18 USC was amended, and the new law allows some computer attackers to be prosecuted as terrorists. Specifically, acts that knowingly cause the transmission of a program, information, code, or command, and intentionally cause unauthorized damage to a protected computer **and** are calculated to influence or affect the conduct of Government by intimidation or coercion, or to retaliate against Government conduct may constitute **cyber terrorism**.
- **Weapon of Mass Effect (WME):** Several types of attacks, including: biological, chemical, nuclear/radiological, conventional explosives, and cyber attacks. Weapons of mass effect may cause large-scale alterations of psychological perceptions, changing and/or influencing both attitudes and behaviors.

Cyber Terror: Potential for Mass Effect

Although it may seem unlikely that a terrorist computer network attack could cause a comparable effect on a population as the 1998 Tokyo subway Sarin gas attacks, consider the following—

- A group calling themselves the Internet Black Tigers took responsibility for attacks in August 1998 on the E-mail systems of Sri Lankan diplomatic posts around the world, including those in the United States.[1]
- Highly visible and publicly accessible Web sites such as http://www.whitehouse.gov provide a ready target for anyone wishing to promote an anti-American position or message. In 1999, electronic intruders, apparently upset over the NATO bombing in Yugoslavia, forced the White House Web page to go offline for over twenty-four hours. While the actual physical damage was unremarkable, the larger damage was the perception by thousands of Americans that the security of the White House

was somehow compromised, albeit electronically.[2]

- The *LoveLetter* virus of May 2000, of which anti-virus vendor Symantec has identified more than 80 variants, infected millions of computers and caused billions of dollars in damage. The original variant of this virus was eventually traced to a lone individual.[3]
- Multiple highly-used Web sites, including eBay, Amazon.com, Yahoo.com, E*Trade.com, and CNN.com suffered near simultaneous denial-of-service attacks in February 2000.[4]
- The *Code Red* series of worms that were launched in July 2001 reportedly infected 250,000 computers in just nine hours, and were labeled "a real and present threat to the Internet" by a group of key INFOSEC agencies including the CERT Coordination Center and the National Infrastructure Protection Center (NIPC).[5] The author of this worm has yet to be identified.

Such attacks by means of the click of a computer mouse have affected larger and wider targets.

Beyond the destruction, corruption, or alteration of data, these examples illustrate another important characteristic of such electronic attacks—the attacker's attempt to erode confidence in the confidentiality, integrity, and availability of vital computer networks (see Figure 1). This is arguably the most significant way cyber terror qualifies as an act capable of mass effect. Such attacks by means of the click of a computer mouse have affected larger and wider audiences. These

documented attacks on computer networks portend potentially more serious attacks.

continued on next page

Figure 1. Beyond the destruction, corruption, or alteration of data, the above illustrates another important characteristic of such electronic attacks—the attackers attempt to erode confidence in the confidentiality, integrity, and availability of vital computer networks.

continued from previous page

In testimony before Congress, National Intelligence Officer for Science and Technology, Lawrence Gershwin cited a recent CIA report that suggests weapons of mass effect, including denial-of-service attacks, are "likely to proliferate in the coming decade."[6] If we accept this as true, then we must consider some even more serious and plausible scenarios including—

- Cyber terrorists conduct a series of major intrusions into international banking networks, resulting in a global loss of confidence in the security of the banking system
- Cyber terrorists use computer network attacks to disrupt trading in all major stock markets, resulting in huge losses in dollars and investor confidence
- Cyber terrorists disrupt air traffic control, raising public alarm about the safety of air travel
- Cyber terrorists launch a denial-of-service attack against vital Government information centers, rendering them unavailable for public use
- Cyber terrorists make subtle, but significant changes to vital online documents or Web pages, which go unnoticed by the victims for days or even weeks
- Cyber terrorists disrupt Internet traffic globally, resulting in a loss of confidence in e-commerce
- In conjunction with physical attacks on key infrastructure, cyber terrorists employ computer network attacks to create a synergistic effect, amplifying physical and psychological damage.

Although the events described in these scenarios may seem unlikely, they are all technically possible and may, in fact, already be within reach for some terrorists. Michael Vatis, director of Dartmouth's Institute for Security Technology Studies, stated that during the current war on terrorism cyber attackers are likely to use Web page defacements, denial-of-service attacks, worms, viruses, and data corruption.[7] One reason attacks like these are likely is that the tools for launching such attacks are commonly shared among hackers via the Internet.

Potential Appeal to Terrorists

In each of the scenarios outlined above, the actual damage to data caused by the cyber attack may be far less significant than the longer-term psychological effects on the targeted population. It is axiomatic that successful computer network attacks undermine trust in systems that rely on those very computers, and this "mass effect" is what could make cyber attacks useful to terrorists. This is not the only characteristic that might attract terrorists. Others include—

- **Asymmetry:** The ability of a lone individual or small group to cause disproportionately massive damage
- **Accessibility:** The possibility of inflicting damage on vital infrastructure that is normally protected by physical means
- **Anonymity:** The ability to remain hidden in the global information network by using commonly available tools like IP address spoofing or by employing multiple, intermediate victim computers and by transiting nations and jurisdictions. Anthony Lake, National Security Advisor to President Clinton, maintains that carrying out a cyber attack presents no immediate physical danger to the perpetrator; a strike can be launched from a remote location, offering greater anonymity; and, the relative simplicity of the equipment and skills involved means an individual can more easily act alone, without recourse to a larger group or government.[8]
- **Range:** The possibility of striking targets around the globe without the need for physical proximity at the scene of the attack. In his recent book *Six Nightmares*, Anthony Lake submits that cyber terror also offers a vast array of targets, as the world becomes ever more wired in the midst of an information explosion.

Mitigating Factors

While the possibility of terrorists using computer network attack as a weapon of mass effect appears to be increasing, it is important to note that there are some factors that serve to mitigate this growing threat. Chief among these are—

- **Technical Challenges Remain:** Causing mass effects using cyber terrorism alone remains a technological challenge, despite the availability of increasingly advanced computer attack technology on the Internet. To successfully create a mass

effect, terrorists would need to cause a major disruption in a critical computer infrastructure. Awareness of the criticality of these infrastructures by organizations like the National Infrastructure Protection Center (NIPC) makes potential terrorist targets less vulnerable.

- **Disruption is Effective:** Aggressive counter-terrorism efforts make planning and executing major attack operations increasingly difficult for terrorists. The more preoccupied terrorists are with operational security, evading law enforcement and intelligence services, and keeping their organizations from being penetrated, the less freedom of movement they have to plan and execute successful cyber terrorist attacks.
- **Strong Information Systems Security Significantly Decreases Vulnerability:** This may be the area where individual users and systems administrators can make the most difference in thwarting a potential cyber terrorism attack. Strict adherence to strong, coordinated security policies makes individual computer networks less vulnerable to cyber terrorists. Furthermore, strong network monitoring, incident handling, and responsive forensics can isolate attacks and keep them from causing a mass effect.

Conclusion

It is likely that some terrorists consider successful cyber attacks against critical infrastructure to be an attractive option for achieving their goals, especially if such attacks hold a high probability of causing a mass effect on a targeted population. Additionally, the availability of cyber attack tools increases the probability that terrorists may successfully achieve a mass effect through cyber terrorism. Aggressive computer network defense, coupled with other traditional counter-terrorist efforts can help mitigate this threat. ■

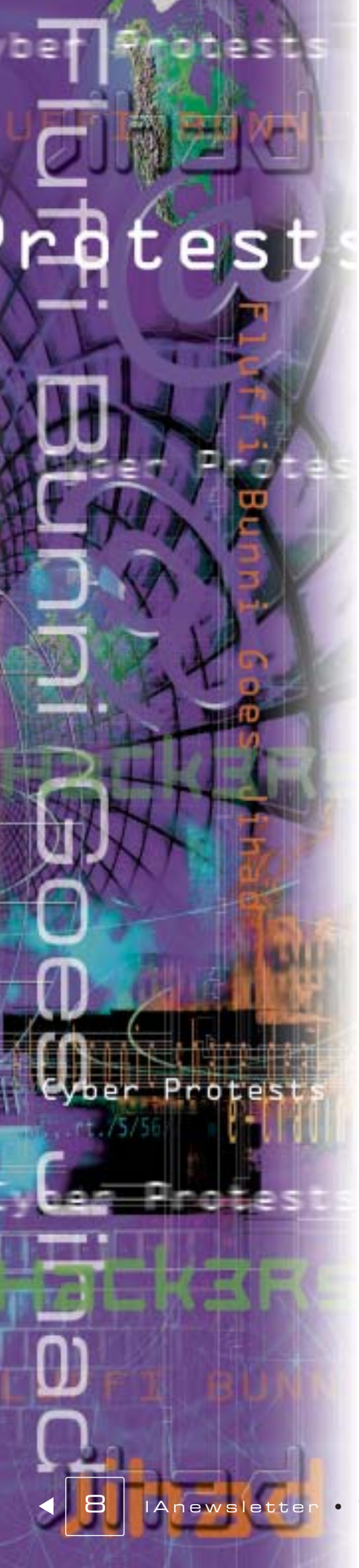
LTC Ed Sbrocco is Deputy Director for Plans, Policy, and Exercises (J5/7), Joint Task Force for Computer Network Operations (JTF–CNO). He is an FA30 officer (information operations) who received his B.S. in 1984 and M.A in 1994 from the United States Military Academy. He has held a variety of command and staff assignments as an Army infantry officer. LTC Sbrocco has been assigned to the JTF since its FOC in July 1999. He may be reached at sbroccoe@jtfcno.ia.mil.

Mr. Tom Ward is a member of IATAC currently supporting the JTF–CNO Director of Intelligence (J2) and the Director of Plans (J5). He holds a B.A. from DePaul University. His M.S. is from Northern Illinois University. Mr. Ward may be reached at wardt@jtfcno.ia.mil.

Mr. Chris Baden is an IATAC member currently supporting the JTF–CNO Director of Intelligence (J2). He holds a B.S. degree from the United States Air Force Academy and an M.S. from the Joint Military Intelligence College. He is currently enrolled in the M.B.A. program at the University of Maryland, Robert H. Smith School of Business. Mr. Baden may be reached at badenc@jtfcno.ia.mil.

Endnotes

1. Serabian, John A., Jr. Information Operations Issue Manager, Central Intelligence Agency, Statement for the Record before the Joint Economic Committee on Cyber Threats and the U.S. Economy. 23 February 2000. Online at http://www.cia.gov/cia/public_affairs/speeches/archives/2000/cyberthreats_022300.html
2. To read more about the White House Web page hack, see http://abcnews.go.com/sections/tech/DailyNews/whhack990511.html
3. To read more about the multitude of LoveLetter variants, see http://securityresponse.symantec.com/avcenter/venc/data/vbs.loveletter.a.html
4. See CNET.com, online at http://news.cnet.com/news/0-1007-200-1545348.html
5. CERT/CC, Joint Alert on the Code Red Worm and mutations. Online at http://www.cert.org/congressional_testimony/CRannounce.html
6. Gershwin, Lawrence K , National Intelligence Officer for Science and Technology, Statement for the Record for the Joint Economic Committee Cyber Threat Trends and US Network Security (as prepared for delivery) 21 June, 2001. Online at: http://www.cia.gov/cia/public_affairs/speeches/gershwin_speech_06222001.html
7. Vatis, Michael A. Cyber Attacks During the War on Terrorism: A Predictive Analysis, Institute for Security Studies at Dartmouth College, Sep. 22 2001. Online at http://www.ists.dartmouth.edu/ISTS/counterterrorism/cyber_attacks.htm
8. Lake, Anthony, *6 Nightmares: Real Threats in a Dangerous World and How America Can Meet Them*, Little, Brown and Company, Boston, 2000.



Cyber Protests—

The Threat to Information Assurance

by Mr. Kris R. Campbell

Since the terrorist attacks on September 11, 2001, the speculation of the potential for cyber attacks has varied—from low-level nuisances to an all out "cyber war." What has been seen thus far is on the low side of the threat spectrum. Both pro-U.S. protesters and anti-U.S. protesters have been active. However, the effects of their actions have not been particularly damaging.

In the last decade, with the expansion of the Internet, protests and political activism have entered a new realm. Political activism on the Internet has already generated a wide range of activity, from using E-mail and Web sites to organize, to Web page defacements and denial-of-service (DoS) attacks. These politically motivated computer-based attacks are usually described as **hacktivism**, a marriage of hacking and political activism.

In addition to the consistent activity of groups devoted to a specific long-term cause, the Internet has also seen short-term periods of intense political activity, which can be referred to as cyber protests. The most common type of cyber protest comes in the form of Web page defacements. In such scenarios, a Web site is compromised through some security deficiency and the hacker is able to alter it, many times placing propaganda, profanity, or pornographic images on it. Mail bombing is a popular form of a DoS attack. Massive amounts of E-mail or Web traffic are directed against a specific site, overloading it and causing it to crash. This can range from being a nuisance and embarrassment for an organization to a major economic loss for an e-commerce business.

Post September 11 Incidents

Pro-U.S. Protests

Beginning on September 11, patriot hackers and hacking groups on Internet Relay Chat (IRC) and newsgroups called for attacks on Pakistani and Afghani Web sites. They promoted active retaliation for the terrorist attacks on the World Trade Center and Pentagon. Some of the first Web sites defaced were those belonging to the Afghan News Network, Afghan Politics, http://www.Taleban.com, and http://www.Talibanonline.com. Some sites were attacked merely because their name sounded vaguely Arabic.

Spam (unwanted mass E-mails) was used to encourage hackers to join together in attacking Web sites of Islamic fundamentalism and those supporting terrorism. The call to hackers to join forces has been successful. A group calling itself the Dispatchers has taken up the task of striking out against Palestinian and Afghani Web sites.

A prominent pro-U.S. hacking group formed in late September. Founded by the

wealthy, German hacker Kim Schmitz, Young Intelligent Hackers Against Terror (YIHAT) has as its stated goal to gather information on terrorists and give that information to the proper U.S. authorities.

Anti-U.S. Protests

Anti-U.S. protesters were quick to respond to the attacks as well. On September 14, a hacker using the name Fluffi Bunni defaced Web sites numbering in the thousands by compromising an ISP domain name server and redirecting those sites to a page created by himself. The message was "Fluffi Bunni Goes Jihad." Also, the LifeStages computer virus was renamed to WTC.txt.vbs in order to infect computer users who were curious about the World Trade Center. The resulting effect on computer systems was minimal.

Groups of Pakistani hackers have declared cyber jihad on the United States and are calling on all hackers of Muslim faith to participate. GForce Pakistan has taken on a large role in building a coalition to fight the United States as military operations are taking place. Their main targets are U.S. sites but they are also attacking Indian sites and foreign sites supporting the United States. They have stated that they will continue to target military sites and Web sites that support critical infrastructure.

Web servers and other computer systems in foreign nations are vulnerable as well as those in the United States. An incident occurred on October 1, in Hungary, when hackers compromised the Hungarian National Security Office's Web site and defaced a page with anti-U.S. propaganda. This indicates the hackers' willingness to go after those nations not directly involved in the current war on terrorism.

Conclusions

In the week following the terrorist attacks, Web page defacements were well publicized. The cyber protests that have occurred thus far have had little impact on U.S. infrastructure or the defense community as the overall number and sophistication was rather low. Still, they are indicative of cyber protests to date. Generally, the most popularly targeted sites are those belonging to government, educational, commercial, and cultural institutions. However, any site with an exploitable vulnerability will be susceptible to a cyber attack. Political events and emerging international situations will increasingly lead to cyber protests.

As computing technology becomes faster and better, and hacking tools become more advanced and easier to use, cyber protesting and hacktivism will become more significant to U.S. national interests. Cyber protesters are becoming increasingly more organized and their techniques more sophisticated but, most likely, will continue to deface Web sites and perform DoS attacks. There will also be an increase in the number of apparently unrelated hacking groups participating in the cyber protests. National boundaries are not always clearly delineated in attacks on opposing organizations. Because the United States is a multicultural, world-leading nation it will suffer from attacks on culturally related sites and structures in the future. Pro-active network defense and security management is imperative to information assurance. International cooperation and private–public cooperation within the United States are necessary to ensure the ongoing function of the defense and civilian infrastructure.

This product was completed with support from the CRUCIAL PLAYER project. CRUCIAL PLAYER is an interagency project initiated in 1999 by the Deputy Secretary of the Department of Defense (DoD), the Deputy Director of the Federal Bureau of Investigation (FBI), and the Deputy Director of the Central Intelligence Agency, and funded by DoD and FBI. The project is managed by the National Infrastructure Protection Center, Washington D.C. ■

Kris R. Campbell is a Counterintelligence Analyst with Veridian. Mr. Campbell supports the National Infrastructure Protection Center under the CRUCIAL PLAYER project.

DoD Information Assurance Acquisition Initiatives Underway

by Mr. Eustace King

The Defense-Wide Information Assurance Program's (DIAP) mission is to ensure that DoD vital information resources are secured and protected by unifying and integrating Information Assurance (IA) activities to achieve information superiority. As the Department develops solutions to counter the many threats to our information systems and resources, a key element of our strategy will be to incorporate these solutions into the Service/Agency information technology (IT) acquisition processes. The DIAP is leading several initiatives with respect to improving the way the Department is integrating IA products and services into DoD IT acquisition processes.

DoD Wireless Policy Development Efforts

Exploding onto the commercial scene in recent years is a wave of wireless technologies and innovations that offer new business opportunities and convenience features for the public as a whole. These wireless technologies (e.g., local area networks, personal digital assistants, personal electronic devices, cell phones/personal communications systems, mobile satellite systems, and multiple wireless peripherals) also provide tremendous operational capabilities for the Department of Defense that can extend the reach of operational commanders, and are clearly the wave of the future. The uses of wireless technologies within the Global Information Grid (GIG) are rapidly becoming viewed as an operational necessity to facilitate command and control, as well as combat support and business applications.

However, these enhanced capabilities also entail risks that must be managed. To facilitate the implementation of wireless technologies and the management of risk to DoD information, operations, and personnel, the DoD Chief Information Officer (CIO) directed that an overarching DoD policy on the implementation of wireless technologies be developed. To that end, a DoD-wide working group has been charged with developing that policy which will address security, interoperability, spectrum, and technology, to include operational vulnerability assessments. The target completion date for this overarching wireless policy is January 2002.

NSTISSP–11 Deadlines Rapidly Approaching!

The National Security Telecommunications and Information Systems Security Committee (NSTISSC) provides a forum for the discussion of policy issues, sets national policy, and promulgates direction, operational procedures, and guidance for the security of *national security systems* through the NSTISSC Issuance System. NSTISSP No. 11, Subject: *National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology (IT) Products*, was issued in January 2000, and established policy and milestones for incorporating IA into all systems used to enter, process, store, display, or transmit national security information. NSTISSP–11 further states that by July 1, 2002, the acquisition of all commercial-off-the shelf (COTS) IA and IA-enabled IT products to be used on the systems specified above shall be limited only to those which have been evaluated and validated in accordance with one of the following—

- International Common Criteria for Information Technology Security Evaluation [Common Criteria]
- The National Security Agency (NSA)/National

Institute of Standards and Technology (NIST) National Information Assurance Partnership [NIAP] Evaluation and Validation Program
- The NIST Federal Information Processing Standard [FIPS] validation program.

The DIAP continues to publicize this issue and is incorporating appropriate language into the DoD acquisition (5000-series) and IA (8500-series) regulations, as well as DoD's implementation of the Federal Acquisition Regulation (DFAR). In addition, the DIAP is developing a process for reviewing waiver requests, as well as briefing the DoD's Information Assurance Panel (IAP) and CIO Executive Board in January 2002, and and providing briefings at upcoming IA conferences. For more information on NSTISSP–11 and the NIAP processes, refer to http://www.nstissc.gov/ and http://niap.nist.gov/.

Developing an IA Strategy for IT Acquisitions

The National Defense Authorization Act for Fiscal Year 2001 included the requirement to document an "information assurance strategy consistent with the Department's policies, standards, and architecture" before acquiring mission critical and mission essential IT, in addition to complying with other Clinger-Cohen Act (CCA) requirements. Webster's dictionary defines strategy "as the art of devising or employing plans toward a goal." The Department's goal of securing and protecting our information resources can only be achieved through a "cradle-to-grave" approach towards building IA *into* our IT systems, not adding IA onto already established systems.

Formulating a program's IA strategy begins with understanding some key foundation documents: Defense acquisition policies embodied in the DoD 5000-series; DoD Chief Information Officer (CIO) Guidance and Policy Memorandum (G&PM) on Global Information Grid (GIG) Information Assurance; and the DoD Information Technology Security Certification and Accreditation Process (DITSCAP). GIG G&PM 6–8510 and the DITSCAP provide guidance on IA requirements for IT development that must be included in a program's overall requirement document, system design, and proposed operational concepts. IA costs (e.g., technical solutions, personnel, training, physical security, engineering, etc.) must also be de-

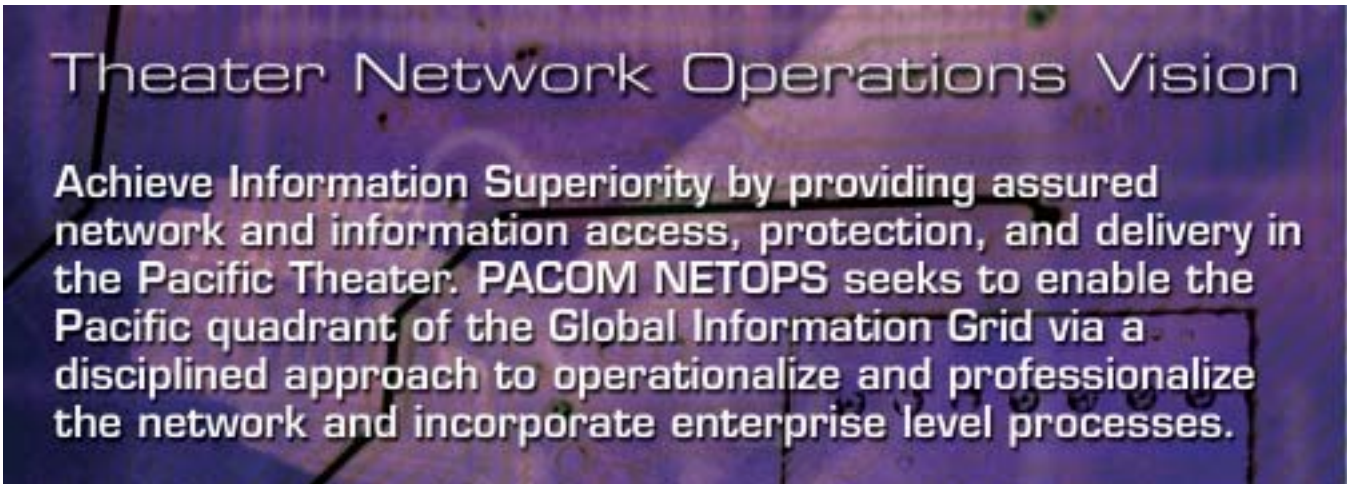
continued on page 25

Figure 1. Although wireless technologies provide tremendous operational capabilities for DoD, they entail risks that must be managed.

Partnership's—

The Key to Success for Pacific Theater Network Operations (NETOPS)

by LTC Timothy M. Petit, USA, Mr. Robert Lietzke, and Mr. Mark Miller



In the spring of 2000, Brigadier General James D. Bryan, then the PACOM J6, authored an article in *IAnewsletter* Vol. 3 No. 4 outlining the vision of the Pacific Theater NETOPS initiative. Since the publish date of that article, the USCINCPAC Theater C4I Coordination Center (TCCC) has made great strides in developing network situational awareness in the Pacific Theater. It became apparent that this initiative is constructed of two distinct components—the technology that makes the vision of the Global Information Grid (GIG) and the NETOPS initiative possible, and the partnerships that make it a reality.

Through its working relationships with DISA, the Service Components, Sub-Unified Commands, JTFs, other CINC TCCC's, and Joint Staff, USCINCPAC continues to strive toward achieving Information Superiority and true enterprise-level processes in the Pacific Theater.

The USCINCPAC TCCC is the pilot program for the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence [ASD/(C3I)] NETOPS concept. Thus, the journey began with development of the architectural framework for the NETOPS initiative. USCINCPAC developed a Concept of Operations (CONOPS) outlining the key players and their roles and responsibilities necessary to develop the NETOPS construct in the Pacific Theater. Standard Operating Procedures were also developed and an effort to develop joint Tactics, Techniques, and Procedures (TT&P) for NETOPS is in progress. The staff also developed an architectural framework linking USCINCPAC Joint Mission Essential Tasks (JMETs) and Information Exchange Requirements (IERs) to the NETOPS mission and daily operations in the TCCC. By linking TCCC operations back to JMETs, leadership is able to more accurately validate both the mission and resource requirements.

To achieve the NETOPS vision, USCINCPAC incorporated a three-phased development model. Phase I focused on gaining essential operational capabilities to obtain situational awareness over the Theater Information Grid (TIG). Currently in Phase II, the focus expanded to include achieving operational capabilities outlined in Joint Vision 2020, Information Transport and Processing; specifically building collaboration throughout the Theater and providing the linkage from systems performance back to current operations. In Phase III, the focus expands again to include creating enterprise-wide processes in order to establish an enterprise operations capability for the TIG. Through the infusion of technology and the evolution of Theater-wide processes the TCCC developed a viable situational awareness and operational impact assessment capability.

Within the NETOPS construct, it is envisioned that ca-

pabilities go beyond the traditional functions associated with Telecommunications Network Management (TNM), Information Assurance (IA) and Information Dissemination Management (IDM) through the synergy of these three functions in an operational environment. USCINCPAC is making significant progress in each of the functional areas as well as in the overarching areas of knowledge management and enterprise operations.

Current Capabilities

Network Management: Network Management is the most mature discipline within the NETOPS concept, with a number of common protocols and methods in use at USCINCPAC. The Integrated Network Management System (INMS) built on AI Metrix NeuralStar technology (INMS V.2) is the Manager of Managers chosen for DISA's long haul circuit and specialized network monitoring responsibilities. The legacy application, World Wide Online System-Replacement or WWOLS–R is now a partner application of INMS V.2, providing specific circuit details such as bandwidth, classification level, circuit designation and basic functionality. These two tools provide a backdrop and substantial near real-time view of the DISN backbone from a "stoplight chart" (red, yellow, green) perspective of tens of thousands of nodes. For the next dimension of visibility the TCCC utilizes DISA's NetHealth application (by Concord®) to provide historical and near real-time statistical reporting of network performance.

Information Assurance: One of the primary goals in this arena is the development of an IA Common Operational Picture (IA COP) for the Theater. The key milestone was the installation of the Automated Intrusion Detection Environment (AIDE). AIDE is an Advanced Concept Technology Demonstration (ACTD) designed to combine raw intrusion data (events) from a wide range of dissimilar vender Intrusion Detection Systems (IDS) products and firewalls. Real time correlation of events from multiple sources provides the basis for a real time IA COP and provides the operator with a predictive analysis capability. Due to the large data warehousing capability, retrospective analysis of large areas of coverage is also possible.

Information Dissemination Management (IDM): IDM endeavors to convert the mass amounts of data available on the GIG into usable knowledge. Made up of a series of Internet/Intranet search engines, the Global Broadcast System (GBS) and a highly configurable information broker concept, IDM promises to ensure delivery of the right information to the right place at the right time. USCINCPAC developed an IDM CONOPS, and is developing a significant GBS capability. As an operational test site for DISA's IDM V3.0 software (scheduled for release later this year), the TCCC is positioned to help shape the implementation strategy for this new capability within the NETOPS arena.

Joint Task Force (JTF) Support

The TCCC recently added Domain Name System (DNS) service to its set of core capabilities. Due to the 24x7 operating schedule, providing DNS service to deployed JTF's from the TCCC improves response time when DNS problems occur or changes are required. It also improves coordination during the planning process and creates a "one-stop" shop for JTFs to work C4 issues.

Creating and Sharing Knowledge

"Data is not information, information is not knowledge, knowledge is not understanding, understanding is not wisdom."

Cliff Stoll & Gary Schubert

The innovations discussed in the previous paragraphs provide the pieces necessary for an overall C4 picture within the Theater. Bringing this information together to create usable knowledge for decision makers is the next step in the creation of a Network/IA Common Operational Picture (NET/IA COP)—a primary focus of the NETOPS concept. To accomplish this the TCCC provides linkage between operational missions and network health through the fusion of NM and IA capabilities. The final step is distributing this knowledge via a vehicle such as IDM.

Further facilitating this transformation of information, developers at USCINCPAC reengineered TCCC processes as well as many Theater-wide processes and tailored a Remedy Knowledge Management System to capture data. The idea is to have all of the information available in one location where it can more effectively be used for metrics and data mining. The latest project in the area of knowledge management and information sharing is the imple-

continued on page 16

Building the Law Enforcement and Counterintelligence Common Operational Picture

by Mr Eric A. White

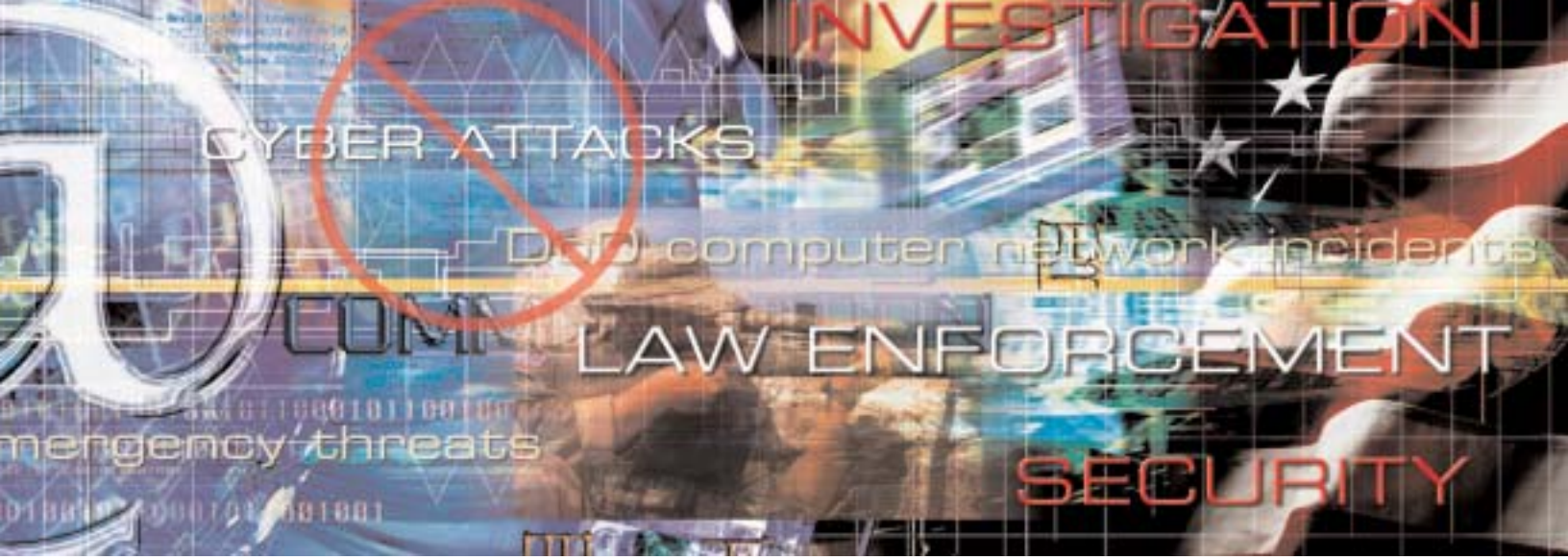
The tragedy of September 11th has shown that terrorist organizations continue to target U.S. critical infrastructures. These events have also shown us "up close," that hostile entities have the resolve, the resources, and an increasing technological capability to carrying out sophisticated attacks. These attacks spotlight an even greater need for information sharing and analysis throughout Government and the U.S. Intelligence Community. The U.S. response to the attacks also emphasizes the need for increased protection of infrastructures supporting DoD and U.S. national security systems.

Because of the inherent vulnerabilities to information systems and the ubiquitous nature of networking, DoD crisis response organizations are re-examining their capabilities for responding to cyber attacks. Capability assessments to support National Military Strategy have also recently taken place to assist in DoD's QDR process. In an effort to support mission assurance, DoD law enforcement (LE) and counterintelligence (CI) organizations have intensified their efforts for responding to cyber attacks against Defense critical infrastructures. The primary DoD agencies involved include the Defense Criminal Investigative Service (DCIS), the Air Force Office of Special Investigations (AFOSI), the Naval Criminal Investigative Service (NCIS), the U.S. Army Criminal Investigation Command (USACIDC), and the U.S. Army Intelligence and Security Command.

In 1998, DoD Components formed a collaborative effort to share information, conduct analysis, and coordinate investigations. This was accomplished through the Defense Components Law Enforcement & Counterintelligence Center co-located within the spaces of the United States Space Command's (USSPACECOM), Joint Task Force for Computer Network Operations (JTF–CNO). Each of these agencies has dedicated representation in the Center.

The LE&CI Center coordinates, de-conflicts, and facilitates law enforcement and CI support and analysis for DoD computer network incidents and relevant criminal counterintelligence investigations and inquiries. These efforts include a comprehensive integrated approach and understanding to support the protection of defense, national, and international infrastructures critical to U.S. national security during times of peace, crises, and war.

To improve upon this capability, the Defense Components have intensified their efforts by forming a "law enforcement and counterintelligence analysis branch" within the LE&CI Center. This newly formed unit will conduct analysis and correlate criminal and CI investigations relevant to computer network intrusions across DoD and military service boundaries to support warfighters and national securi-



ty requirements. The Center's analysts will work to identify trends and support indications and warnings by analyzing fraud, criminal, and counterintelligence cyber investigations and data from multiple agencies and information sources. The LE&CI Center analysis branch will aggregate and distribute information quickly and efficiently to support both the U.S. military LE and CI communities, and the operational needs of the JTF–CNO. Inputs for analysis will come from both classified and unclassified sources to provide an all source view of the current and emerging threats. State-of-the-art information technology, databases, and analytical tools will play a central role in the development of the Center's analysis products. The LE&CI Center analysts will work within DoD by leveraging the analytical efforts of each of the LE&CI Center's parent organizations. External coordination also takes place by leveraging information and capabilities from the security arena, and other Federal, State, and Local law enforcement, and the U.S. Intelligence Community.

The LE&CI Center coordinates, deconflicts, and facilitates law enforcement and CI support and analysis for DoD computer network incidents and relevant criminal counterintelligence investigations and inquiries.

The formation of a multi-agency analysis capability has distinctive advantages for DoD.

- This capability provides the means to integrate multiple agency data and analysis through the production of actionable analytical products.
- It provides agents and analysts with a collaborative environment to bring together the collective experiences and information that has traditionally been stovepiped.
- It provides the ability to aggregate somewhat marginalized data from multiple sources to provide meaningful analysis.
- This effort provides DoD greater insights into the results of law enforcement and counterintelligence investigations that may impact military readiness.

During the Cold War Era, military commanders were mainly concerned with foreign threats to DoD resources and capabilities. Today, the threat has evolved and as we have seen, domestic security is equally vital in managing risks. The integration of DoD investigative analysis with other relevant data increases the commander's view into the law enforcement and counterintelligence common operational picture. ■

Mr. Eric White is a member of IATAC currently supporting the DoD Law Enforcement and Counterintelligence Center (LECIC), co-located with the Joint Task Force for Computer Network Operations (JTF–CNO), Arlington, VA. Mr. White is the lead law enforcement and counterintelligence analyst for the LECIC's Analysis Branch. He holds a B.A. in Criminology from Saint Leo University, and has completed requirements for the M.S. Degree in Information Systems and Telecommunications from Johns Hopkins University, School of Business and Professional Studies. Mr. White is certified as a System Security Practitioner (SSCP). He may be reached at whitee@jtfcno.ia.mil.

continued from page 13

mentation of a Patrol Enterprise Management (PEM). The PEM was installed in the TCCC in September 2001 after being selected as a "Gold Nugget" from last year Joint Warrior Interoperability Demonstration (JWID).

From its inception, developers and operators at the TCCC made sharing visibility a top priority. One of the first initiatives was working with DISA to get INMS and VTC capabilities out to the Service Components and Sub-Unified Commands. Additionally, the aggregate of information collected and analyzed by the TCCC is presented to the J6 in the daily Current Operations Briefing. This information is continually updated and made available to Theater partners through the TCCC SIPRNET Web page. Information is also routinely shared through collaborative means using such tools as VTC, NetMeeting, and Info Workspace. Of note, it was decided early on to pursue technology for implementation only if it had the "joint seal of approval." For this reason, only products that are DISA sponsored, ACTDs, or JWIDs are implemented in the USCINCPAC TCCC.

Partnerships

Technology insertion within the TCCC laid the foundation to achieve the vision of the NETOPS concept for the Pacific Theater. However, the TCCC could not have enjoyed the successes to date without partnering with key players in Theater; specifically, DISA–PAC, the Regional Satellite Support Center Pacific (RSSC–PAC), the Navy Computer and Telecommunications Area Master Station (NCTAMS) Wahiawa, the Service Components, Sub-Unifieds, and JTFs.

The USCINCPAC TCCC has become an operational extension of the USCINCPAC Crisis Action Team (CAT) J6 and provides Theater-wide C4 situational awareness to the J3 and the Joint Operations Center (JOC). The TCCC is able to provide more relevant situational awareness for the CINC's Theater operations.

DISA, as the lead for development of the GIG concept, is not only the most likely candidate to champion its development and enterprise management but is also the only organization with the experience and global reach to execute this concept. The close relationship between the USCINCPAC TCCC and DISA–PAC is one of the keys to success for NETOPS in the Pacific.

The TCCC and the DISA–PAC Regional Network Operations and Security Center (RNOSC) in conjunction with the DISA Field Office, located at USCINCPAC, form the backbone for this very strategic partnership. DISA and USCINCPAC have worked hand in hand throughout development of the NETOPS concept in the Pacific. The DISA–PAC RNOSC serves as the technical arm of the TCCC and the two organizations communicate via a 24x7 active VTC connection creating a virtual "shared workspace." Additionally, DISA and the TCCC have experimented with the CINC NOSC or CNOSC concept, which physically locates DISA personnel in the TCCC. The idea is to facilitate information sharing and provide a robust INMS analysis capability. At USCINCPAC this relationship proved successful with positive results and feedback from recent joint exercises such as ULCHI FOCUS LENS 2001. Permanent, limited hour, CNOSC manning is scheduled to begin in 2nd quarter of Fiscal Year 2002.

Relationships within the theater have also helped accelerate TCCC's achievement of specific IA goals. Developing and refining business processes such as the tracking and reporting Information Assurance Vulnerability Assessments and Bulletins (IAVAs and IAVBs) brought visibility and structure to a process, which is key to ensuring protection of Theater information systems. Evolving relationships between IA organizations such as the Global Network Operations and Security Center (GNOSC), regional Computer Emergency Response Teams (CERTs), Network Operations and Security Centers (NOSCs), and the TCCC greatly improved information sharing and overall visibility of the information warfare threat. USCINCPAC is also working with local intelligence agencies to augment the TCCC with an intelligence analyst in an effort to become more proactive in protecting Theater networks.

The identification and implementation of new technologies to further the NETOPS concept is an on-going effort at TCCC. Critical to this effort are partnerships with the Defense Research Projects Agency (DARPA) and the JBC as well as associations with ACTDs and JWID. These relationships are key to the success of the GIG and serve to accelerate and increase the quality of solutions derived. Collaboration and in-

Artist Rendition of future USCINCPAC TCCC planned for Fall 2003.

volvement of these players has already proven successful with advances such as AIDE and BMC Patrol.

Planners and developers at the TCCC work closely with the USCINCPAC Chief Information Officer (CIO) and his staff in developing the NETOPS concept and TCCC capabilities. The CIO's vision and broad responsibilities form a natural bond for GIG implementation and facilitate a conduit to implement strategic requirements that often cross Service boundaries.

Relationships with individual Services and Sub-Unified Commands continue to mature with great strides being made at the Service level to establish enterprise management capabilities. Programs such as the Navy and Marine Corps Intranet (NMCI) and the Air Force's Network Management System/Base Information Protect (NMS/BIP) provide small examples of and test beds for the global enterprise management concept of the GIG. The key for continued development of the GIG and the NETOPS concept is the massing of these Service initiatives at a Joint level.

Future plans are underway to increase the USCINCPAC TCCC physically and functionally with a move to a larger, state-of-the-art, facility in February 2004. Plans call for the collocation of additional DISA–PAC and USCINCPAC functions to further capitalize on this successful partnership.

Conclusions

"Those who capture this computing power and the corresponding speed of the information flow are going to have a tremendous advantage. I don't care where you look in the spectrum of warfare. Throughout history, soldiers, sailors, Marines and airmen have learned one valuable lesson: If you can analyze, act and assess faster than your opponent, you will win!"[1]

Gen Ronald R. Fogleman

Through technical integration and evolving Theater partnerships the USCINCPAC TCCC is forging the way for NETOPS in the Pacific Theater. Developers are working with the Joint Staff and DISA to help shape the GIG and NETOPS initiatives in order to provide situational awareness of Theater networks and the critical link back to Theater operations. This operational linkage provides the mass of force necessary for more accurate and timely decision-making for Theater warfighters and is the foundation for information superiority in the Pacific Theater. ■

Lieutenant Colonel Timothy M. Petit is Chief, C4 Current Operations Branch, J6 USCINCPAC, Camp H.M. Smith, Hawaii. He graduated from the United States Military Academy with a B.S. in Computer Science. He also holds a Masters of Science Degree in Operations Research from Georgia Tech University and an M.A. in National Security and Strategic Studies from the Naval War College.

Robert Lietzke is a Program Manager supporting the Pacific Network Operations initiative at Camp Smith, Hawaii. He graduated with a B.S. in General Engineering from the United States Air Force Academy and holds an M.S. in Human Resource Management and Development from Chapman University.

Mark Miller is a Senior Information Assurance Engineer supporting the Pacific Network Operations initiative at Camp Smith, Hawaii. He graduated from Troy State University with a B.S. in Computer Science and holds an M.S. in Computer Science from Boston University.

Endnote

1. "Information Operations: The Fifth Dimension of Warfare" Remarks as delivered by Gen Ronald R. Fogleman, Air Force Chief of Staff, to the Armed Forces Communications-Electronics Association, Washington, April 25, 1995.

Fundamental IA—

JITF Gets Back to Basics With Code Review

by Mr. Louis Scheiderich and Mr. James C. Cable

Those charged with providing computer and network security are faced with a dizzying array of defense strategies, hardware solutions, software tools, and policies all aiming to provide some element of information assurance. As is the case with any security, it can be difficult to know when things are working properly and that security efforts are on the right track. Considering the rate of technological development, the challenges easily appear insurmountable. As with any lofty undertaking, every now and again what is needed is to get back to basics. In recent months, the Joint Integration and Test Facility (JITF) at the Air Force Research Laboratories, Rome Research Site has been exercising the fundamentals of Information Assurance (IA) and getting back to basics with source code reviews.

Code reviews are critically important to IA. If there are any doubts about the necessity of such reviews, consider that an extremely high percentage of our collective approach to IA and Information Operations (IO) relies directly on software and its ability to function reliably. Aside from the obvious computers, software runs our switches, routers, hubs, and other networking hardware. It comprises the very tools we use for computer and network defense. Conventional software testing may demonstrate that the software is generally stable, but IA requires answers to additional questions. Did the software come from a trusted source? Did it even come from within this country? How many hands were involved in the creation of our software? Do we care to speculate whether it is opening holes in our defense, possibly exposing invisible weaknesses? With these questions in mind, reviewing source code for security is clearly a wise investment of our efforts.

The mission of the Rome Research Site's Joint Integration and Test Facility is to evaluate the installation and integration of Department of Defense Intelligence Information System (DODIIS) Intelligence Mission Application (IMA) software and other information technology assets. The chief objective of the JITF is to establish that IMAs integrated into a combined site system will not negatively interact with other IMAs and will not lower the ability of the user to perform his job. This role gives the JITF a unique purview of IA requirements and the negative impacts of bad software, making the JITF particularly qualified to perform source code reviews.

Traditionally, code reviews are performed during the development cycle by the development staff. They take the form of a non-critical peer review aiming to create a higher quality product by enforcing coding standards, employing more efficient algorithms, and eliminating bulky, needless code. Often,

the development phase is the best place for this sort of review due to its potentially large impact on the final product and lower implementation costs due to early intervention.

However, the JITF is in a unique position to perform a different type of code review, effectively reinforcing those done during development. The JITF staff includes experienced engineers who have a greater collective view of the operational environment than might be available to a developer. Moreover, because they are not associated with any development staff or program office, they offer objectivity that is essential for candid reviews. This impartiality in testing allows JITF engineers to perform review of source code at possibly the most critical juncture—before it is deployed at user sites and after the majority of the development work has been done.

Methods used by the JITF range from traditional low-tech approaches (this typically means visually scanning the source code) to innovative automated approaches.

The visual scan is time consuming and places rather hefty demands on reviewers. Having a good grasp of the software's intended capabilities and deployed architecture before the start of the review is frequently helpful. From that point, the review is helped along by a limited number of automated tools (such as ITS4 or RATS)[1] to speed up the process, but ultimately it will resort to reading and reporting on every part of the code. Such was the case in a recent scan of 70,000 lines of Java code for a Department of Defense client.

Not all code reviews are conducted to hunt out computer security holes. Sometimes code review is necessary in order to release raw source code to a foreign government or prepare it to be recompiled in such a way that will not reveal sensitive comments or phrases. For example, when releasing it to trusted third parties or subcontracted developers. The JITF has recently made headway in this area with the development of a specialized code scanning utility.

The JITF engineers were faced with reviewing the source code of a large product without any software tools to identify changes that must be made before the software could be released to coalition partners. As a result, they created the "Source Code Review" (SCR) tool kit. In its current version, SCR performs dynamic searches on source code and identifies any words or phrases that might be objectionable. The entire code base can be examined at the same time, cataloguing original source along with recommended necessary changes for historical reference.

SCR also accelerates the progress of any review of associated images, which might include emblems, banners and icons. While it does not yet examine each image for hidden markings, SCR does organize all images as expandable thumbnails, permitting the reviewer to select suspicious images for closer examination and eliminate them from the baseline if necessary.

If much of this sounds analogous to good configuration management practices, this is not coincidental. The philosophies are quite similar, after all. In fact, good coding practices, configuration management and judicious use of strict compilation rules will eliminate the great majority of weaknesses in most software. However, in those special cases of high sensitivity calling for extra precaution, there is nothing like being able to reach back to fundamentals and being able to assure software users that the code itself is safe. This is the practice of the JITF. ■

Mr. Louis Scheiderich, GM–14, Supervisory Computer Engineer is the Program Manager for the Joint Integration Test Facility. He manages the activities of approximately 22 government and contractor personnel with a primary mission of enhancing the integration and interoperability of intelligence systems during development and while operational. The JITF performs testing and evaluation, and provides engineering and consulting support to intelligence system developers and operational sites. He received his Associates Degree in Engineering Science from Mohawk Valley Community College in 1968. In 1970 he received his B.S. in Aerospace Engineering from the University of Buffalo and in 1982 his M.S. in Systems Management from the University of Southern California.

Endnote

1. ITS4 can be downloaded from http://www.cigital.com/its4/ at no cost (certain conditions apply) and RATS is available from http://www.securesw.com/rats under the GNU public license version 2.

Biometrics & Smart Card Integration

Achieving Functionality and Enterprise Solutions

by Mr. Tom Castellano

Converging Technologies

In FY98 the General Services Administration (GSA) Smart Card Initiatives Team announced an initiative to explore the framework to integrate biometrics and smart card technologies and to develop guidance for Government-wide smart card interoperability. Part of the initiative included the formation of a biometrics/smart card integration effort and the publication of a comprehensive biometric/smart card integration guide.

The Defense Department's Smart Card Senior Coordinating Group (SCSCG) recently chartered the Department of Defense (DoD) Biometrics Management Office (BMO) to form a working group to explore the combination of biometrics and smart card technologies. The DoD smart card, commonly referred to as Common Access Card (CAC), is similar in size to a credit card and contains an embedded integrated circuit chip (ICC).

The new working group, referred to as the CAC–BWG, will evaluate biometrics alternatives and recommend enterprise solutions for biometrics with the CAC. DoD started the review of smart card technology after the National Defense Authorization Act of FY00 required the establishment of a smart card senior coordinating group (SCSCG) chaired by the Department of the Navy (DON). Furthermore, DoD established the Electronic Business Board of Directors (EB BOD) to oversee the operations of the SCSCG in their development and implementation of department-wide interoperability standards for use of smart card technology.

The SCSCG chartered the CAC–BWG to—

- Evaluate biometric alternatives and recommend an enterprise solution for biometrics with the CAC
- Make recommendations to the SCSCG concerning CAC related biometric, hardware, software, policy, and legal issues
- Assist Functional Community Panels (FCPs) and CINC/Services/Agencies in biometrics/CAC integration
- Coordinate and analyze requirements for CAC-biometrics
- Seek commonality in applications and software/hardware interoperability

CAC–BWG Membership—The CAC–BWG is chaired by the DoD BMO and membership is open to representatives from each Functional Community Panel (FCP), CINC, Service, and Agency.

Technology

Technological advances in Integrated Circuit Chip (ICC) capabilities, smart card readers, and card configuration provide multi-purpose applications to authenticate, identify, and verify users in logical and physical domains. These applications not only provide enhanced information assurance and access control but can also streamline organizational processes and procedures. Several enhancements in smart card capabilities include increased 64-Kilobyte EEPROM (electrically erasable programmable read-only memory), 32-Bit Controllers, up to 135-Kilobyte ROM, 5-Kilobyte RAM, and enhanced data crypto accelerator/engine. In essence, these mini computers enable smart cards to hold more data, increase data encryption speeds, and increase processing capabilities.

Other emerging technologies include the use of contactless smart cards using radio frequency identification (RFID) technology. This technology enables smart cards to transmit a signal to a receiver device embedded in either the smart card reader or access control device. Combination smart cards

(combi-cards) include both contact and contactless applications depending on the operational environment, such as tighter security environments.

Multi-Applications

Biometrics combined with smart cards offer unique identification and authentication applications. These applications, coupled with the correct blend of support and training, provide the end-user access to logical or physical systems. Possible applications include access to portals, extranets, intranets, Web-enabled resources, internet e-commerce applications, medical data, DoD controlled facilities, and potentially future weapon systems. Depending on environmental and operational constraints, multiple biometric identification applications can be layered into one suite to enable multi-factor authentication.

Recently, the Air Force conducted a CAC/Public Key Infrastructure (PKI) beta test to evaluate the issuance and use of CACs with PKI certificates. The evaluation focused on interoperability of CAC software, middleware, and hardware configurations. The evaluation resulted in collection of empirical interoperability data and identified issues with end-user education and training.

Future applications of biometric-enabled smart cards depend on the widespread acceptance of both technologies and the operational utility to the end-user. Studying possible variations and alternatives of combining these technologies may lead to viable solutions in an operational setting.

The statements in this article describe work in progress within the DoD BMO and the USAF Biometrics Office, and do not necessarily represent the official policy of the Biometrics Management Office or the USAF Biometrics Program Manager. ■

Mr. Tom Castellano is a member of IATAC and supports the U.S. Air Force (USAF) biometrics office at HQ's, USAF Communications and Information, Directorate of IT Enterprise Operations, Network Systems, Infrastructure Branch. He was recently mobilized to support Operation Noble Eagle at the U.S. Army Land Information Warfare Activity (LIWA) and can be reached via E-mail at tjcaste@liwa.belvoir.army.mil.

Sample of a Smart Card

References

CardTech/SecurTech Web site and conference proceedings CDROM, available at: http://ctst.com.

Department of Commerce, National Institute of Science & Technology (NIST) Biometrics Consortium, available at: http://www.biometrics.org/.

Department of the Navy CIO available at: http://www.doncio.navy.mil/focusareas/smartcard/index.html.

Department of the Navy (DON) Information Management and Information Technology (IM/IT) online resource site, available at http://www.don-imit.navy.mil/.

DoD Biometrics Management Office (BMO), available at http://www.c3i.osd.mil/biometrics/.

Peck, Michael, Smart Cards for Smart Soldiers, Card Technology—Tracking the Future of Card Systems and Applications, May 2001.

U.S. General Services Administration (GSA) Smart Card Office, available at http://www.smartcard.gov.

DISA IA
Education, Training, and Awareness Products

A series of Information Assurance distributive training products, which provide baseline training for CINCs, Services, agencies and other DoD organizations and can be integrated into specific IA training programs, is currently being disseminated by the Defense Information Systems Agency. These computer-based/Web-based training products serve organizations and individuals throughout the Department of Defense, as well as other federal departments and agencies, state and local governments, and educational institutions.

Many DoD organizations use these training products in their certification programs for System Administrators (SAs), Information System Security Officers and Managers (ISSOs and ISSMs), and other IA personnel. They are also used to satisfy the requirements of the Computer Security Act of 1987 for end users. Four of the CBT products, Introduction to the Defense Information Technology Security Certification & Accreditation Process (DITSCAP), Operational Information Systems Security, CyberProtect, an interactive computer network defensive exercise, and DoD Information Assurance Awareness, are currently required by DISA for level one certification of its System Administrators. Although these products are created primarily for the DoD, with input from the Defense-wide IA Program (DIAP) office and service IA training representatives, they are also used in support of national-level IA Education, Training, and Awareness outreach programs. Several of the products, including CyberProtect, have a nationwide as well as a federal-wide audience. Many public and private universities, as well as Service and agency schoolhouses, have incorporated the series into their IT courses. Furthermore, some of the products have been customized by non-DoD organizations and agencies to create training materials designed for their specific training needs.

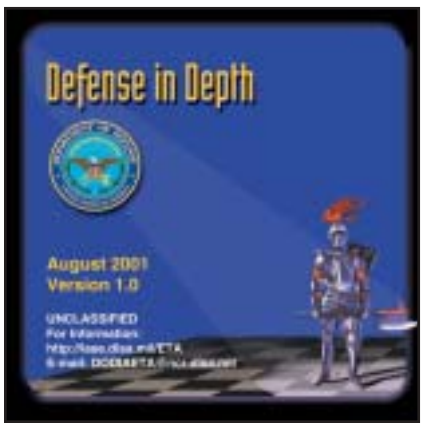
Information Age Technology

Many new training products have recently become available. Updates of Information Age Technology, now Information Age Technology V.2.1, and DoD INFOSEC Awareness, now DoD Information Assurance (IA) Awareness, are additions to the IA series. Intended for those who are not information technology professionals but need to understand the terms and operations of the communications infrastructure, Information Age Technology V.2.1 describes critical infrastructures and their relationship to the Internet. DoD Information Assurance Awareness explains the components of Information Assurance, as well as the laws and policies designed to ensure it. In addition, DoD IA Awareness includes expanded sections to reflect the ever-changing world of information technology: descriptions of internal and external threats to information systems, new information about technology specific vulnerabilities, and an additional focus on the Internet, including detailed discussions of E-mail, macro viruses, hoaxes, and Distributed Denial of Service (DDOS) attacks.

IA in Defense in Depth

Information Assurance in Defense in Depth is another recently released Web based training product. Based on the Joint Vision 2020 concept of Information Superiority, and intended for military and civilian personnel responsible for the defense of DoD computers and computer networks, this course explains the concept of "Defense in Depth." Using the multi-dimensional defenses of a mediaeval castle as a model, it demonstrates the importance of a layered defense, which integrates the capabilities of people, operations, and technology. The user will learn how to detect, defuse, and react to a wide range of threats to networks, enclave boundaries, local computing environments, infrastructure support, and emerging technology.

These CBT/WBT products are additions to a growing selection of Web based training products, including IO Fundamentals, an overview of Information Operations in the Joint context, and Secret and Below Interoperability (SABI), an explanation of the network-centric process that incorporates risk management into all decisions for Secret and Below connectivity.



Unix Security for System Administrators

Additional Web based training products include Unix Security for System Administrators, designed to help the beginning to intermediate level systems administrator understand what makes up a secure UNIX system, and Windows NT Security, which details the steps necessary to safeguard system resources in a stand-alone or networked Windows NT operating environment.

Introduction to Computer Incident Response Team (CIRT) Management

Introduction to Computer Incident Response Team (CIRT) Management has also been recently released for distribution. Introduction to CIRT Management is an interactive CD–ROM intended for those whose responsibilities include setting up and managing a CIRT team. Procedures for hiring CIRT personnel, tools for preventing and dealing with incidents, and CIRT reporting requirements, including an explanation of IAVAs (Information Assurance Vulnerability Alerts) and INFOCONs (Information Operations Conditions), are among the topics covered. This training product, which includes review exercises that highlight customer service, different types of network attacks, and incident priority, can be delivered to the desktop via CD–ROM or installed on a network.

Other CD–ROMs available include DAA Basics, which highlights the duties and responsibilities of the Designated Approving Authority and Public Key Infrastructure, which explains PKI and the security services it provides. Information Assurance for Auditors and Evaluators examines IA threats and countermeasures, risk management, and the advantages and disadvantages of networked systems, as well as the DITSCAP process, data testing, reporting on evidence, and assessing reliability, in the context of detailed examples of computer crime. System Administrator Incident Preparation & Response (SAIPR) for Windows NT provides a virtual hands-on experience, taking the student through the steps necessary to protect information that may be useful in an investigation of suspected unauthorized activity.

Nineteen video presentations are also currently available. Sixteen of these are distributed in a compilation format. Compilation 1 includes titles such as "Protect your AIS," which is about Information Security in the workplace and "The Scarlet V," which discusses virus-scanning software. Compilation 2 includes presentations such as "Just the Fax Sir," in which Officers Joe January and Frank Jones investigate the security risks associated with the use of fax machines, and "Sherman on My Mind," which examines the issue of spending time on personal projects at work. Two additional videos, Solar Sunrise, about the computer hackers who gained access to DoD computers during the 1998 Iraqi weapons inspection crisis and Understanding PKI, an explanation of how PKI can be used to ensure the security and privacy of cyber-based transactions, may be ordered separately.

All IA CBT/WBT products and videos (with the exception of Solar Sunrise, which is available only to US military and government personnel) are available upon request and free of charge. For more information or to order IA Education, Training and Awareness products please go to the Web site at http://iase.disa.mil. There, you can also sign up for the "IA Product News" E-mailing list, to get updates on new products, as they become available. Please direct any questions or comments (including ideas or requests for new training products) to the products and distribution E-mail address: DODIAETA@ncr.disa.mil. ■

***Note:** These products are Web-deliverable, using html and Flash technology. They can be loaded on Web servers for delivery via the Internet or intranet. As with our traditional products, they also run on a LAN or from a CD-ROM drive.*

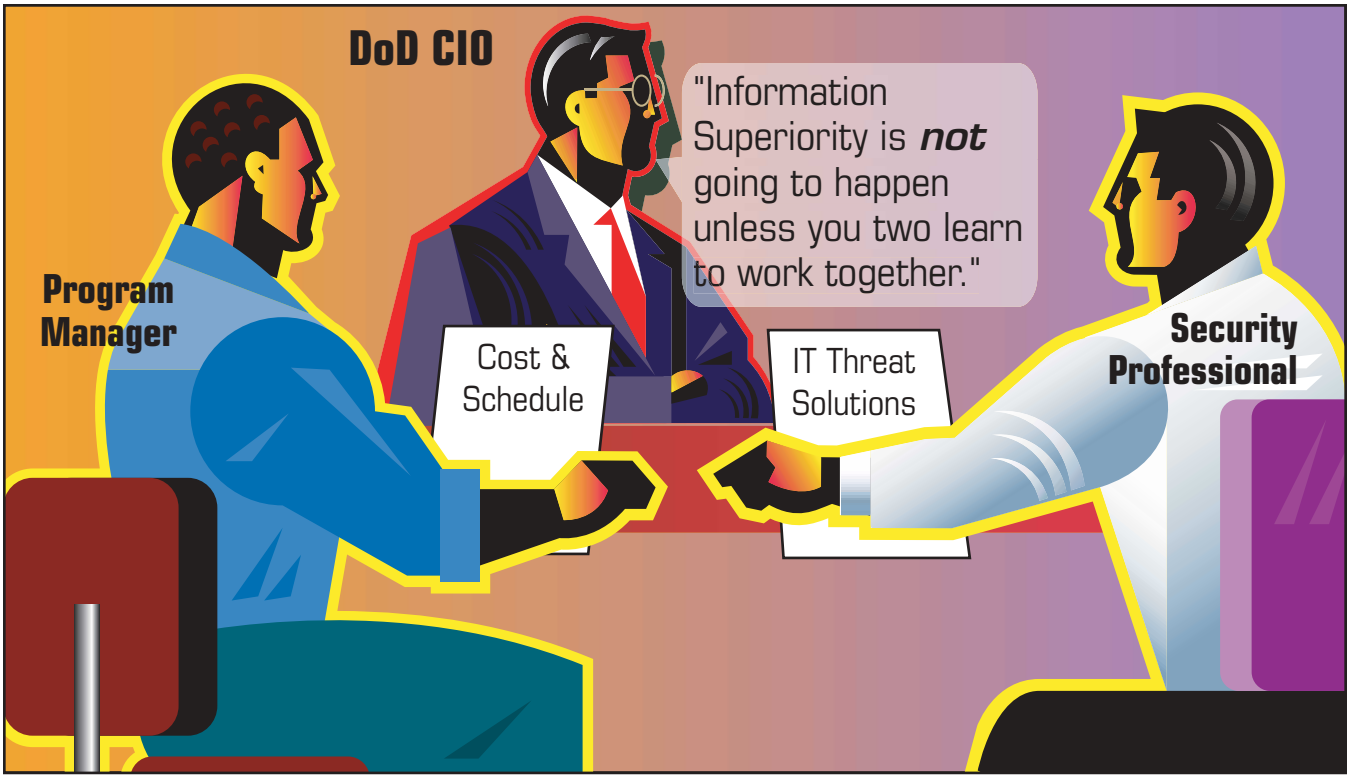


Figure 2. Services/Agencies must enlist the services of security professionals or organizations to assist program managers as they incorporate sound IA practices into every IT system development.

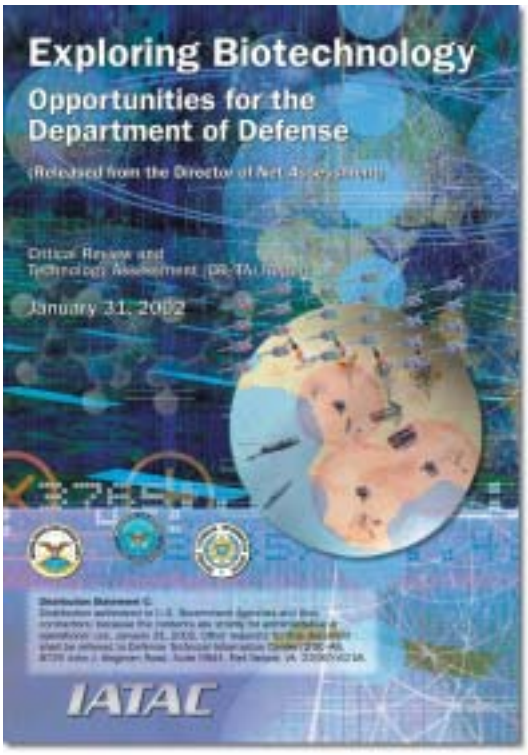
continued from page 11

veloped as part of the IA strategy, and considered during analysis of alternatives, life cycle cost estimates, testing plans, and development of the Acquisition Program Baseline (APB).

Services/Agencies must enlist the services of security professionals or organizations to assist program managers as they incorporate sound IA practices into every IT system development (see Figure 2). Information assurance reference materials and strategy development examples are available on the Defense Acquisition Deskbook Web site [http://www.deskbook.osd.mil/default.asp] and the DIAP Web site [http://www.c3i.osd.mil/org/sio/ia/diap/]. DoD Instruction 8580.1, "Integrating Information Assurance into the Acquisition Process," is under development and should be published by April, 2002.

Mr. Eustace King is a Civil Service GS-15 employed by the National Security Agency (NSA), detailed to the Defense-Wide Information Assurance Program (DIAP), Office of the Assistant Secretary of Defense, Command, Control, Communications & Intelligence (OASD[C3I]). Mr. King is the Technology and Capabilities Development Team leader and is responsible for acquisition oversight, research and technology development, security management infrastructure, and IA architecture/requirements. Mr. King is a 1975 graduate of Brooklyn College (City University of New York) and earned an M.B.A. from Gonzaga University in 1982. The DIAP is located in 1215 Jefferson Davis Highway, Crystal Gateway 3, Suite 1101, Arlington, VA 22202. Mr. King can be reached at 703.602.9969 or E-mail Eustace.King@osd.mil.

What's New



Exploring Biotechnology—Opportunities for DoD

Critical Review and Technology Assessment (CR/TA)

Biotechnology has revolutionary potential for a broad range of U.S. military capabilities. Further, because of the United State's unparalleled lead in research and development, biotechnology presents the opportunity to recast the framework of military operations and create a long term U.S. advantage in the global strategic environment.

Biotechnology applications range from enhancing human performance by making warfighters resistant to the elements, to hardware systems design, such as creating advanced missile defense systems with biomimetic Unmanned Aerial Vehicle (UAV) swarms. If biotechnology's strategic importance is realized, it could provide the U.S. with a significant advantage for the next two to three decades.

Although the broad military potential of biotechnology is exceptionally promising, capturing it for defense purposes is not being realized. Biotechnology requires different skill sets and expertise than DoD currently recruits and retains. In addition, there is little guiding policy or legal documents to establish the ethical "playing field" for DoD to take advantage of emerging commercial applications and advances. This framework must be established to support and facilitate biotechnology research and development. Finally, even if DoD were to identify and prototype a biotechnology appliqué for the war-fighter, it does not have the military industrial complex to mass-produce the products. DoD needs to establish firm business ties to the commercial biotechnology community to develop the industrial base required for military capability production.

These issues and others must be addressed by the highest level of DoD leadership in order to ensure biotechnology's potential is captured and fully exploited.

The purpose of this report was to determine if the explosion of discovery and advances in biotechnology held the same potential for advances in military affairs as the Information Revolution. The approach undertaken focused on three converging areas—

1. Legal and Policy
2. Development of Exemplars
3. Provide Recommendations on the DoD Infrastructure.

Biotechnology holds the promise of revolutionary military advances for DoD in a broad range of applications. Given our unique lead in this fundamental science, these advances may provide a significant strategic advantage to the United States for the next several decades. However, DoD is poorly disposed to recognize, much less take action to realize this potential. A process of education, action, and the involvement of senior DoD leaders is needed to move forward on the opportunities being presented. This report may be ordered on our Web site or by completing the order form on page 27 and faxing it to IATAC. ■

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 (unless you are DoD or Government personnel). TO REGISTER ON-LINE: http://www.dtic.mil/dtic/regprocess.html.

Name _____ **DTIC User Code** _____

Organization _____ Ofc. Symbol _____

Address _____ Phone _____

_____ E-mail _____

_____ Fax _____

LIMITED DISTRIBUTION

IA Collection Acquisitions CD–ROM

❑ Fall 2001edition

Critical Review and Technology Assessment (CR/TA) Reports

❑ Biometrics ❑ Computer Forensics* ❑ Defense in Depth ❑ Data Mining
❑ IA Metrics ❑ Configuration Management ❑ Exploring Biotechnology

IA Tools Report

❑ Firewalls (3rd Ed.) ❑ Intrusion Detection (3rd Ed.) ❑ Vulnerability Analysis (2nd Ed.)

State-of-the-Art Reports (SOARs)

❑ Data Embedding for IA ❑ IO/IA Visualization Technologies ❑ Modeling & Simulation for IA
❑ Malicious Software (Release due Summer 2002)

*** You MUST supply your DTIC user code before these reports will be shipped to you.**

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

Feb 4-7

6th Annual IA Workshop "Transforming the Force"
Norfolk, VA
Come see us at Booth #3
http://www.iaevents.com/IAWorkshop/IAWNewInfo.html

4-8

Managing Information Security in a Networked Environment (SEC)
IRM College of the National Defense University
POC: Dr. John Saunders, DSN 325-2078 or IRM College Registrar at DSN 325-6300 or (202) 685-6300,
http://www.ndu.edu/irmc

4-8

Information Warfare Seminar (IWS)
IRM College of the National Defense University
POC: Dr. Giessler, DSN 325-2258 or IRM College Registrar at DSN 325-6300 or (202) 685-6300,
http://www.ndu.edu/irmc

5-6

National Regional Threat Symposium
DOE, North Las Vegas, NV
POC: Systematic Solutions, Inc. (SSI) at (410) 691-7581,
http://www.iaevents.com

19-21

SpaceComm 2002
Come see us at Booth #16
http://www.rockymtn-afcea.org/2002/2002home.htm

20-22

Phoenix Challenge "Information Operations Concepts and Solutions Exploration" Conference
The Air Force Information Warfare Center (AFIWC) at New Mexico State University (NMSU), Las Cruces, NM

Mar 1

IATFF Information Assurance Technical Framework Forum "Securing Web servers/Web sites"
John Hopkins Applied Physics Laboratory, Laurel, MD
IATFF Chairperson (410) 854-7302, webmaster@iatf.net,
http://www.iatf.net

13-17

National Operations Security Conference & Exhibition
Salt Lake City, UT.
http://www.iaevents.com/NATOPSEC2002/NOSC&ENewInfo.html

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