Information Assurance Technology newsletter

IATAC is a Department of Defense Sponsored Information Analysis Center. Vol. I, No. 1 • February 1997

Information Assurance: The Road to 2010

by Captain William Gravell, USN
Chief, Information Assurance Division, The Joint Staff (J6K)

I am delighted to have the opportunity to participate in the kickoff of this newsletter associated with the new Information Assurance Technical Analysis Center (IATAC). This initiative is yet another vehicle in support of the common goal of the Joint Staff, services, CINC's, and warfighters everywhere to achieve Information Superiority as described in Joint Vision 2010. The goal is ambitious, and the required techniques and capabilities are largely unprecedented, especially in the scale required to face the security challenges of the next century. For all these reasons, we must embrace every opportunity to share with each other our thinking, as well as our growing understanding of this enormous subject.

We in the Joint Staff Information Assurance Division (J6K) have always recognized the critical importance of training, education and awareness in our IA implementation strategy. In that regard, I look forward to future issues of the Information Assurance Technology Newsletter as a source of information to benefit the broad IA community – policy makers, warfighters, technologists and intelligence specialists. My boss, the Joint Staff Director for Command, Control, Communications, and Computer Systems (C4), also known as the

Continued on page 3

HOTTEST Information Operations Course Around!

by Joan Putman, Program Analyst, DoD IAC Programs in collaboration with Dr. Fred Giessler, *Professor, School of Information Warfare & Strategy, National Defense University*

The Information Warfare & Strategy course taught at the National Defense University (NDU) offers information warriors the inside story on what is happening in the Department of Defense (DoD) in information operations today. This course is one of the '***hottest***' educational opportunities currently being offered on this subject.

Classes are packed with a very diverse cross-section of government and military personnel. In fact, that is one of the strengths of this course. This course is held in a non-attributional forum where briefings and discussions are held a the 'Secret' level, allowing for candid discussions, observations and an open exchange of ideas from this comprehensive audience. Students leave with much to ponder and a true realization of what other government entities are struggling to achieve.

The friendly 'first name' atmosphere promotes networking and career-influencing relationships that may serve to cross over traditional stovepipe attitudes of the past. This very challenging course contains enough material to fill a course twice in length. A vast amount of valuable printed material from past to present is generously supplemented to the continuous flow of seminar-like briefings which the students attend. In addition there are films, strategy sessions and lively discussions. Each attendee has the opportunity to share what their own

Continued on page 2

Information Assurance: A Community-Wide Challenge

by Roger M. Callahan,
Director for Information Assurance, Assistant Secretary of Defense for Command, Control, Communications and Intelligence

The enormous advances within the computer industry and the integration of that information technology within the Department of Defense (DoD) have brought heightened awareness to the challenge of assuring the availability and integrity of the information systems we have grown dependent upon. These concerns have been well founded as we have seen an increase in the number, and the levels of sophistication, of attacks to DoD information systems. The bottom line is that we should not feel secure with our information environment. The threats require action by the Information Assurance Community to promote awareness, build consensus, and provide direction for the defense of our DoD information systems from exploitation.

The Assistant Secretary of Defense for Command, Control, Communications and Intelligence (ASD/C3I) has taken an active role in Information Assurance. These activities include policy development, program oversight (e.g., Major

Continued on page 4.

contents

Information Assurance Technology newsletter

Inaugural Issue

by Ronald E. Hale,
Program Manager,
DoD Information Analysis Centers

On behalf of the Department of Defense (DoD) Information Analysis Center (IAC) Program and the Defense Technical Information Center, I would like to extend a warm welcome to you for the Information Assurance Technology Analysis Center (IATAC) and the inaugural issue of Information Assurance Technology Newsletter. IATAC has been established to provide the Department of Defense (DoD) with a central point of access for information on Information Assurance emerging technologies in system vulnerabilities, research and development, models and analysis to support the development and implementation of effective protection and defense of information and information systems of effective defense against Information Warfare attacks. IATAC support to the Information Assurance community is provided by leveraging the expertise and capabilities of the entire Information Analysis Center (IAC) Program DoD Research, Services lessons learned, other Government Agencies, and the latest Commercial technologies and techniques. Integrated Sponsorship for IATAC is provided by the Director Defense Research and Engineering (ODDR&E), Assistant Secretary of Defense (Command, Control and Communications), Joint Staff, National Security Agency (NSA), and the Defense Information Systems Agency (DISA).

Our rapidly advancing, globally networked societies present many new challenges to our government, military, and private sectors. As part of the world's most technically-advanced and technology-dependent alliance, we are the most susceptible, and, perhaps the most vulnerable, to attacks on our critical information infrastructures. The global dimension of the networks on which we have come to depend further complicate the problem of achieving secure, reliable and timely communications and information sharing across alliance, coalition and bilateral boundaries in times of peacetime, crisis and conflict.

IATAC support is provided via core operations and technical area tasks (TATs). Core operations consists of support to user inquiries, library operations, home page sustainment, and data base operations. Technical area tasks are separately funded efforts (by a sponsoring agency) that fall within the scope of IATAC but are not provided as part of the core operations.

The scope of the global network and its deepening penetration of our nations' military, governmental and commercial sectors draws our attention from several different perspectives: identifying and characterizing critical information dependencies; assessing and understanding the threat; making arrangements for effective and secure information exchange and command; control and communications between partners; and outlining the challenges that we face as cooperating, sovereign nations. The need for emerging technologies information to ensure our mutual security interests is among our highest national priorities. Emerging technologies information is instrumental in protecting critical information resources and will help assure our ability to undertake coordinated military action in defense of our shared interests.

I encourage you to use IATAC to support your Information Assurance needs and requirements and include IATAC in your strategic planning. IATAC has been established to support you, the user, so I invite you to access our web site, data bases, library and inquiry desk. I'd also like to solicit your feedback on how we can best support your Information Assurance Needs. Please send your comments to iatac-alx1@kaman.com, INTELINK-S : http://204.36.65.5/index.html, and for INTELINK- High: http://www.rl.gov./rl/irido/iatac or to me directly at rhale@dtic.mil.

HOTTEST Course

organization is currently doing in Information Operations.

The courseware gets updated with each offering, as briefers bring in the latest word on what is happening at all levels of government from the President's Commission on Infrastructure to the operators in the field. This valuable 5-day course is only offered four times a year, and is generally open to Infowarriors, at the GS-12 through GS-15; civilian level, and Majors through Colonels; military level. Although others that apply, if accepted, may attend. Information presented at the senior level Information Warfare Course is a consolidation of this class, lasting only 2 days and offered only twice a year. Target audience for this course is all Senior Executive Service (SES) civilians and military from 07 to 09 (Flag Officers). The senior level course is usually an exclusive group of about 20 individuals,.

Dr. Fred Giessler, who energetically runs this class is also the Point of Contact. If you are interested in attending you can call (202) 287-9330 ext. 362 / DSN 667 9330 ext. 362 or e-mail giessler@ndu.edu. If accepted, be prepared to be placed on a waiting list, but this course is worth waiting for!

Information Assurance: The Road to 2010

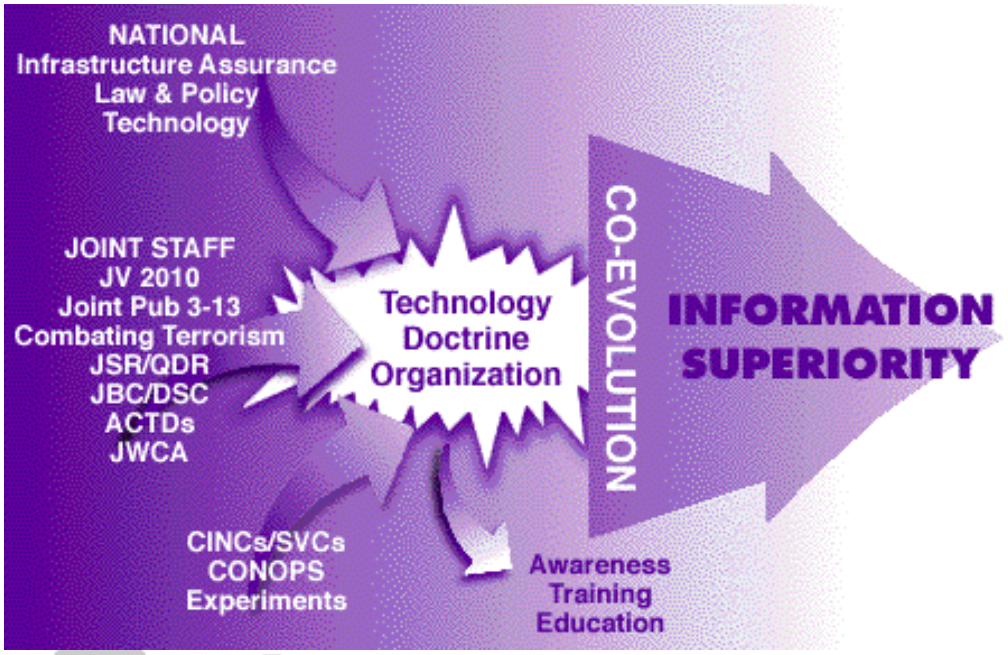
Continued from page 1

J6, is responsible to the Chairman of the Joint Chiefs of Staff (CJCS) for Information Assurance. In this capacity, the J6 provides policy guidance to the CINC's and operating forces; establishes relationships with systems designers, development agencies, and commercial service providers to support the end-users; and, in coordination with other Joint Staff Directors, provides support for joint training, exercise and education initiatives.

Here in J6K, we have been proactive in attempting to develop a broader understanding of, and build consensus regarding, a comprehensive joint approach toward Information Assurance. We have done this by first defining the problem and developing an understanding of what needs to be done; translating those concepts into specific actions; and then bringing that understanding to a broad audience and enshrining that knowledge in policy. In short, we have concentrated on getting everyone onboard the right plan.

The success of our efforts to date is reflected in the status of current initiatives underway within the Joint Staff and throughout the Department of Defense. J6K is the Joint Staff lead in support to the President's Commission on Critical Infrastructure Protection, pursuing a rigorous understanding of the vulnerability of critical information-based infrastructures at the national level. We provide support to CINC exercise and training efforts, and are currently completing the first Joint Doctrine for Information Operations, JP 3-13, in coordination with other Joint Staff offices. In the more technical vein, we are addressing interoperability issues associated with combined-force operations through the Combined Communications Electronics Board (CCEB) and other allied organizations, and J6K is also the coordinating office for the Electronic Key Management System (EKMS), now entering use with US forces, and soon with key Allies as well.

J6K supports the Command and Control (C2) Joint Warfighting Capabilities Assessment (JWCA), which addresses hardware, software, and technology issues related to C4 systems. In our field of Information Assurance, we are focused on developing strategies and technological approaches to long-standing and complex issues such as Multi-Level Security and risk-management. Closely related to that is a recently-initiated Advanced Concept Technology Demonstration (ACTD), entitled Information Assurance Automated Intrusion Detection Environment (IAAIDE). Its objective is to develop an in-depth integrated environment for information defense, using state-of-the-art technologies for intrusion detection, attack detection, and warning. This approach will avoid dependence on a single technology, concentrate on seeking interoperability across organizational and system boundaries, and actively engage almost all CINC's (with CINCSTRATCOM as the designated CINC sponsor), services, defense agencies, and several federal laboratories. We are very excited about this new initiative, and look forward to working with the broad IA community in pursuit of interoperable solutions to our common needs in this area.



In any discussion of the work of J6K, we must acknowledge our extensive and serious participation in several projects focused on understanding, and preparing for, the national security future we all face. Following the CJCS' lead, we are actively working to retain the military effectiveness we will need to prevail against the nontraditional opponents, strategies, and mission scenarios which the next century may bring. In that regard, we are fully involved in larger Joint Staff initiatives such as the Quadrennial Defense Review and efforts to combat terrorism. We hope to bring to those projects our unique perspective on information and information-based technologies, in terms of both their vulnerabilities and the opportunities provided by full use of their capabilities.

Information Assurance is critical to the success of our current and future warfighting efforts. The "Road to 2010" will be not be paved by a single organization or guided by the production of any single plan or policy. The most casual examination of the distributed ownership and equities associated with Information Assurance will convince anyone that is not the model. The journey begins with a broad awareness that everyone has a stake, and as such, we will achieve the required capability through cooperative efforts from the entire engaged community. We in the Joint Staff Information Assurance Division look forward to meeting you as fellow travelers along that road, and in the pages of future issues of the Information Assurance Technology Newsletter.

INFO ASSURANCE

A Community-Wide Challenge

Automated Information Systems Review Committee or MAISRC), and the establishment of standards and practices. An example of some recent policy initiatives is the release of DoD Directive 3600.1 "Information Operations" which provides a definition of Information Assurance. Information Assurance are those information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for the restoration of information systems by incorporating protection, detection, and reaction capabilities.

ASD/C3I has established a working group, called the Information Assurance Group (IAG), to function as a Steering Group for Information Assurance (IA). The membership of the IAG is comprised of the Services, Joint Staff, Intelligence Community, and Defense Agencies. Within the IAG, several working groups have been formed to address critical IA issues. These groups include Policy, Computer Emergency Response Team (CERT) Operations, Education ,Training, Awareness, and Professionalization, Tools, and Multi-Level Security..

Training and education are funda-

Information Assurance Defined

"Information Operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for the restoration of information systems by incorporating protection, detection, and reaction capabilities."

- DoD Directive 3600.1 "Information Operations" December 9, 1996

Conferences & Symposia

Information Warfare
March 13 - 14, 1997
Crystal City Marriott,
Arlington, VA
Information: (310) 534-3922

Southeast C4I Biennial Conference and Exposition, "Global Information Society, The Warfighters Perspective" (sponsored by AFCEA Tampa-St. Petersburg Chapter)
March 18 - 20, 1997
Tampa Convention Center, Tampa, FL; POC: J. Spargo & Associates, Inc. (703) 631-6200

Dixie Crow Symposium — Theme: "Information and Electronic Warfare Their Impact Upon Battlefield Technology As we Pass Into the 21st Century"
March 24 - 27, 1997
Warner Robins Air Force Base Museum of Aviation, Warner Robins, GA; POC: Mike Salis (912) 923-4266

1997 Sea-Air-Space Systems & Technology Exhibition
March 24 - 27, 1997
Sheraton Washington Hotel, Washington DC; POC: (703) 318-0300

AFCEA Spring Intelligence Symposium
April 9 - 10, 1997
Washington, D.C.
POC: AFCEA Intelligence Department (703) 631-6238 or (800) 336-4583, ext. 6238

Fiesta Crow '97 Symposium and Exhibits - Theme: "Military Operations in the Information Age"
April 20 - 23, 1997
Henry B. Gonzalez Convention Center, San Antonio, TX
POC: Milton Driggers
(210) 522-8207

6th UNIX Systems Administration, Networking, and Security Conference
April 21 - 26, 1997
Baltimore, MD; For Information Call: (714) 588-8649

Joint C4ISR Symposium, "INFORMATION DOMINANCE FOR THE FORWARD DEPLOYED WARRIOR"
April 22 - 24, 1997
San Diego, CA
POC: Dr. Bob Kolb (619) 553-3010 or Jan Renninger (619) 592-3709

mental and an essential ingredient for all Information Assurance efforts. An adversary only has to find a single vulnerability that he or she exploits, whereas, those defending the system must defend against all the vulnerabilities, and know how to react and recognize attacks.. On-Line Survey (OLS) testing and vulnerability assessment results highlight these vulnerabilities, they're known and the solutions to those vulnerabilities are known, yet they continue to reappear. It's a training and education issue that needs to be addressed and ASD/C3I has initiated a department-wide assessment for IA training and education.

The DoD lacks a consistent or uniform practice for Information Assurance. This is somewhat of a cultural issue that will need the commitment of everyone within an organization to address. The leadership must recognize the importance of the organization's information systems and provide the resources, both in personnel and funding, to assure the availability and integrity of those systems.

The Assistant Secretary of Defense for Command, Control, Communications and Intelligence is committed to Information Assurance. That commitment has been demonstrated by it's sponsorship (along with the Joint Staff, Director J6) of the Defense Science Board Report on Information Warfare - Defense, the creation of the Information Assurance Group (IAG) and subgroups, and the allocation of resources to address this critical requirement. Information Assurance is a community-wide problem. It will require a community-wide and comprehensive approach, if we want to assure the availability and integrity of our critical information systems and networks.. To this end, ASD/C3I is working closely with the Information Assurance Community to build consensus, promote awareness, develop new policy, and improve IA training and education.

IATAC BASIC SERVICES

The **Information Assurance Technology Analysis Center** (IATAC) provides a variety of services as a part of core operations. These services include support for user inquiries, analysis, operation of the Information Assurance (IA) library, the development of IA data bases, and the generation of products and services (e.g., Newsletter, Technical Reports). For more information on available services, please contact the IATAC staff (contact information provided on back cover).

An overview of the available IATAC data bases is provided below.

Bibliographic

The Bibliographic data base contains information on holdings resident in the Information Assurance library. In addition, the Bibliographic data base maintains citations to Information Assurance-related articles available in the open media.

Vendor

The Vendor data base maintains corporate information on companies that serve the Information Assurance Community. This data base is oriented toward product information (e.g., firewalls, anti-virus tools) available to the community. The type of information maintained includes name of company, address, point-of-contact, telephone number, production name, version, and hardware and software platforms..

Security Alerts

The Security Alerts data base contains virus and system vulnerabilities for computer operating systems. Information stored in the Security Alerts data base includes system platform, type of vulnerability or virus, and recovery patch. A copy of the complete announce is contained in the data base as well as keywords for search capability.

Web Sites

The Web Sites data base maintains URL addresses for pertinent web sites germane to Information Assurance technology. The data base lists the URL address and a description of the site. The purpose of the data base is to provide users with a quick reference for Information Assurance-related sites.

Training & Conferences

The Training & Conferences data base provides detailed information on Information Assurance training courses and conferences. This data base can be searched according to location or date..

Information Assurance Technology Newsletter, Vol. 1 No. 1

IATAC, a DoD Sponsored Information Analysis Center (IAC), is administratively managed by the Defense Technical Information Center (DTIC) under the DoD IAC Program. Inquiries about IATAC capabilities, products and services, or comments regarding this publication may be addressed to:

Robert P. Thompson
Director, IATAC
2560 Huntington Avenue
Alexandria, VA 22303-1403
Com: (703) 329-7337
Fax: (703) 329-7197
E-mail: iatac-alx1@kaman.com
URL: http://www.iatac.dtic.mil

Contacting Us

Telephone:	(703) 329-7337
Facsimile:	(703) 329-7197
STU-III:	(703) 329-3940
STU-III Facsimile:	(703) 329-7106
e-mail:	iatac-alx1@kaman.com
www:	http://www.iatac.dtic.mil
Intelink-S:	http://204.36.65.5/index.html
Intelink:	http://www.rl.gov./rl/irido/iatac

Distribution & Information

☐ CHANGE ME (as noted below) ☐ ADD ME

☐ SEND IATAC TECHNICAL AREA TASK INFO (Government)

Name_____

Title _____

Company/Organization _____

Address _____

_____

City/State/Zip_____

Country _____

Phone _____ Fax _____

DSN_____ E-mail _____

SERVICE: ☐ Contractor ☐ USAF ☐ USN ☐ USA ☐ USMC ☐ OSD

CLIP & SEND TO:

Information Assurance Technology Analysis Center
ATTN: Christina Wright
2560 Huntington Avenue,
Alexandria, VA 22303-1403

FAX (703) 329-7197

e-mail: iatac-alx1-kaman.com

Your Input Is Welcome...

The Information Assurance Technology Newsletter welcomes input from our readers on a wide variety of levels. To submit photographs, related articles, notices, feature programs or ideas for future issues, please use address, fax or e-mail as noted.

Information Assurance Technology newsletter

2560 Huntington Ave., Alexandria, VA 22303-1403