IAnewsletter

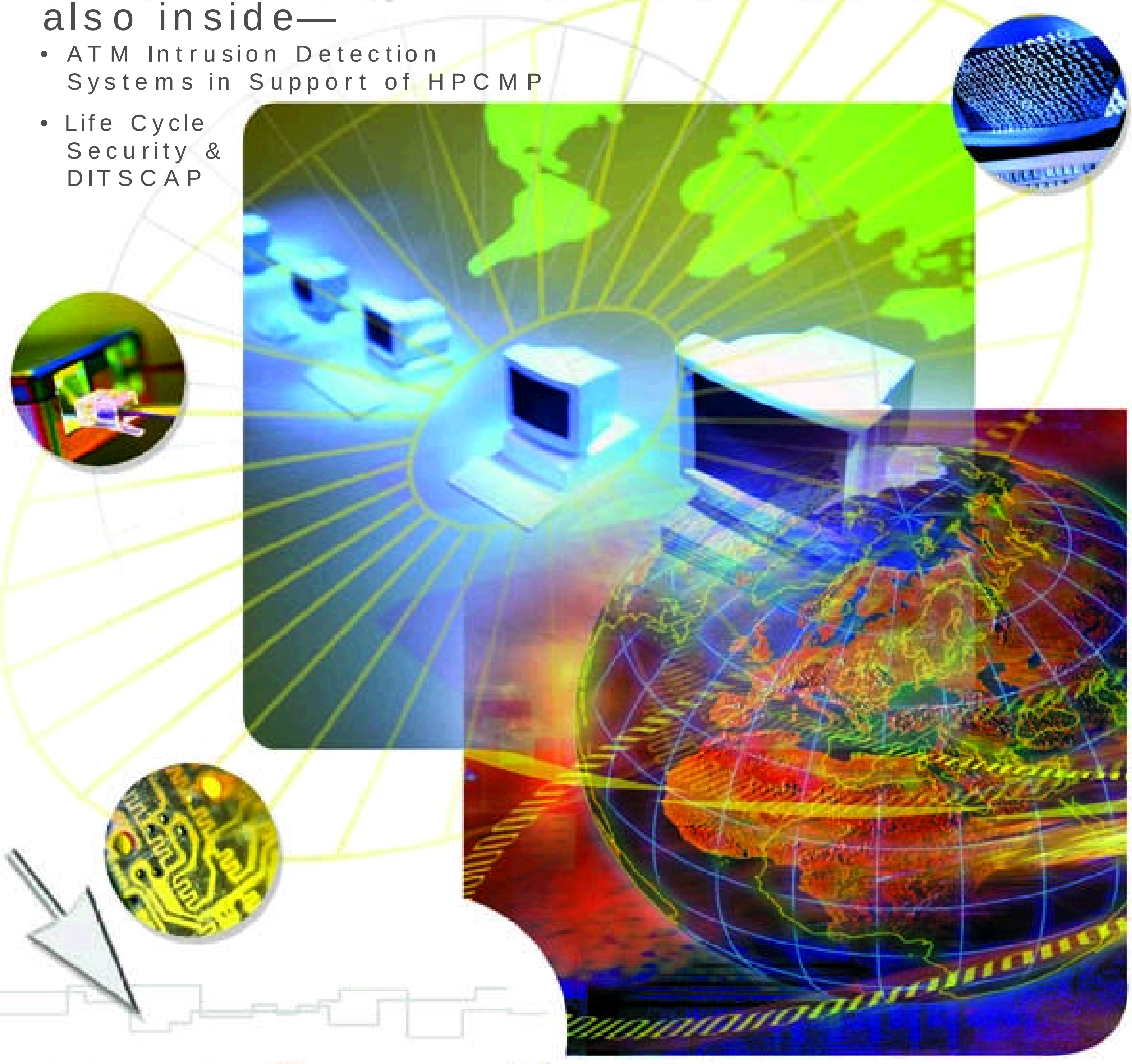
The Newsletter for Information Assurance Technology Professionals

Volume 4 Number 2 • Spring 2001

Modeling & Simulation

also inside—

- ATM Intrusion Detection Systems in Support of HPCMP
- Life Cycle Security & DITSCAP



For Information Assurance

contents

on the cover

ia initiatives

in each issue

IAnewsletter

Editor
Robert J. Lamb
Creative Director
Christina P. McNemar
Information Processing
Robert F. Scruggs
Inquiry Services
Peggy O'Connor
Conference/Meeting Planning
Alethia Tucker

The 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

Summer 2001	16 June
Fall 2001	16 August
Winter 2001	16 November

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

Cover and newsletter designed by Christina P. McNemar

IATAC chat

by Mr. Robert J. Lamb, IATAC Director

IA M&S SOAR

Our feature article in this edition provides an overview of a jointly sponsored State-of-the-Art Report (SOAR) on Information Assurance Modeling and Simulation. The Modeling & Simulation Information Analysis Center (MSIAC) and IATAC joined forces and expertise to research government and industry efforts in IA related M&S. Page 27 has instructions for ordering the full report.

Prospective Authors

As most of our subscribers are aware, the *IAnewsletter* provides a forum for organizations throughout DoD and government to discuss and present information, which is relevant to the entire IA and IO communities. Many of our subscribers have expressed an interest in submitting articles but were unsure of the procedures to do so. In response, I've asked the staff to include a brief set of instructions on the front, inside cover to get prospective authors started. Typically our articles are 750-1500 words, provided in MSWord format with pictures and charts provided separately. Your organization's Public Affairs Office must approve the submission. If you are interested, please contact us via our E-mail address, iatac@dtic.mil and we will provide you with an authors packet.

PKI Seminar at SpaceComm 2001

As I noted in my last column, IATAC developed and has now presented a one-day Public Key Infrastructure (PKI) Seminar in conjunction with the SpaceComm 2001 Conference.

The seminar kicked-off the conference and exposition, the theme being "Global Leadership in Space and Information Operations" and was divided into 8 sections. It began with an introduction and overview of the technology and applied it to the Defense-in-Depth strategy and an organization's mission. The following sections gave detailed insight into cryptography and how it works and IA security functions of identification, authentication, confidentiality, integrity, and non-repudiation. Following were more details on PKI architectural framework, including PKI selection considerations and PKI component dependencies, and PKI policy, including the DoD directives and deadlines regarding PKI implementation.

The last half of the seminar covered PKI enabled applications and enabling applications for their organizations. Topics covered in this section included an overview of near term candidate applications, the relative effort and cost to enable applications, enabling methodologies, and the issues associated with this process. The final section of the workshop addressed future trends in PKI. Among the topics covered were new PKI milestones, certificate issuance status, current directory and token trends, and challenges. Each seminar section concluded with an open-forum Q&A session. Unsolicited feedback from attendees was consistently positive. Those with no prior PKI knowledge reported coming away from the seminar with new understanding of the technology. Although a small number, those attendees currently working PKI issues, reported finding new insight into the technology.

This PKI Seminar is available to other organizations and can be tailored to meet your specific requirements.

Conference Participation

In addition to the seminar and SpaceComm 2001 conference, IATAC has been on the road during the past several months and will continue to do so during the coming months. We participated in the DISA and NSA sponsored 5th Annual IA Conference and Workshop in early February in Norfolk, Virginia, as well as the AFCEA sponsored West 2001 Conference in San Diego in January, (TechNet Tampa 2001 Conference, 13-14 March, Fiesta Crow 2001 in April). We will continue our travels with attendance and participation at the PACOM IA Conference in May. We highlight our participation in these conferences on the back cover and encourage you to stop by our booth.

Modeling & Simulation for IA

State-of-the-Art Report

by Mr. Gary Waag, Dr. Jerry Feinberg, Ms. Lesley Painchaud, and Mr. Ken Heist

The subject of Information Assurance (IA) has received increased attention over the last several years in the military modeling and simulation (M&S) community and, even more so, in the public domain. In the public domain, organizations are concerned with their ability to ensure the sanctity of their data and associated transactions across networks both public and private. In the military modeling and simulation domain, as our warfare paradigm moves from attrition-based to network-centric, organizations need to ensure that their analytic and training tools adequately reflect how this new environment behaves.

To help understand the current state of the art in the M&S of IA, IATAC and the U.S. DoD Modeling and Simulation Information Analysis Center (MSIAC) co-sponsored the development of a report that makes such an assessment. Over the last quarter of calendar year 2000, a survey was conducted of U.S. Government, public and private organizations to collect information that describes tools, data and other research activities that support M&S of IA for purposes as diverse as—

- penetration testing
- network performance analysis
- course of action planning and analysis
- warfighter training and exercise support
- mission rehearsal

Responses have been incorporated in a State-of-the-Art Report (SOAR) on Modeling and Simulation for Information Assurance that is available in its entirety from both the IATAC and MSIAC. This report assesses the degree to which a robust set of tools and associated databases and research now exist to support the various IA M&S application areas described above. The report concludes by summarizing needed areas of further investment and research. This article provides a synopsis of the report.

Dovetailing with the development of the IA M&S taxonomy, definitions of what constitutes an “IA M&S” tool were developed. This clarified the distinction between real-world operational IA tools (that actually ride on information infrastructures and provide some form of information protection), and tools that “simulate” some aspect of IA in support of one or more different functional applications. A list and associated definitions of uses or functions of M&S tools in which representation of IA is essential were developed.

It was noted early on that although the initial focus of this effort was to assess the state of the art of IA M&S, that it would be necessary to expand the scope to include the wider spectrum of Information Operations (IO) M&S as well.

Information Operations (IO) are defined in Joint Vision (JV) 2020 as, “*those actions taken to* *affect an adversary's information and information systems while defending one's own information and information systems. Information operations also include actions taken in a noncombatant or ambiguous situation to protect one's own information and information systems as well as those taken to influence target information and information systems.*" [1]

U.S. DoD instructions define IA as "*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.*" [2]

The rationale for expanding the scope of this assessment was that any simulation tool that attempted to represent the defensive aspects of some IA techniques to protect an infrastructure must also represent some form of offensive attack against this infrastructure. That is to say, assessing the quality of a defense without a worthy offense provides little insight. Accordingly, it was necessary to expand the scope of this assessment to address both IA and IO M&S tools.

Lastly, the above described taxonomy and set of definitions supported the development of a survey form that would be used as the principal means to collect detailed information on existing IA/IO M&S research activities and simulation tools. Survey responses were supplemented with information culled from open literature sources, though open literature rarely provides the same level of insight as a completed survey form.

Five primary functions were developed and used to categorize the user community for each tool, as described below—

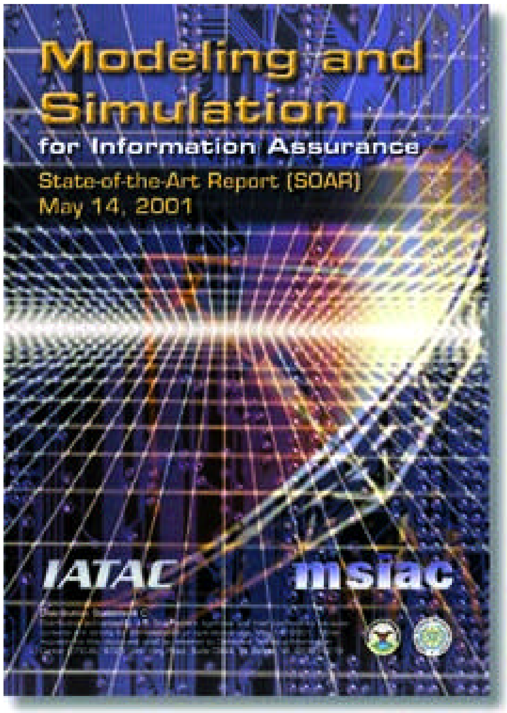
- Course of Action Planning and Analysis
- Infrastructure Protection (e.g., Penetration Testing, Network Performance Analysis)
- General Communications Systems Performance Analysis
- Test & Evaluation
- Warfighter Training and Exercise Support

Recognizing that users of the assessment may look at the field of IA M&S from different perspectives, several other dimensions of this taxonomy were developed to further categorize IA M&S tools. These categories included the following—

- Sponsor organization
- IA functions represented
- Resolution
- Scope
- Analytic techniques employed

Several different methods were used to circulate the survey, including the following—

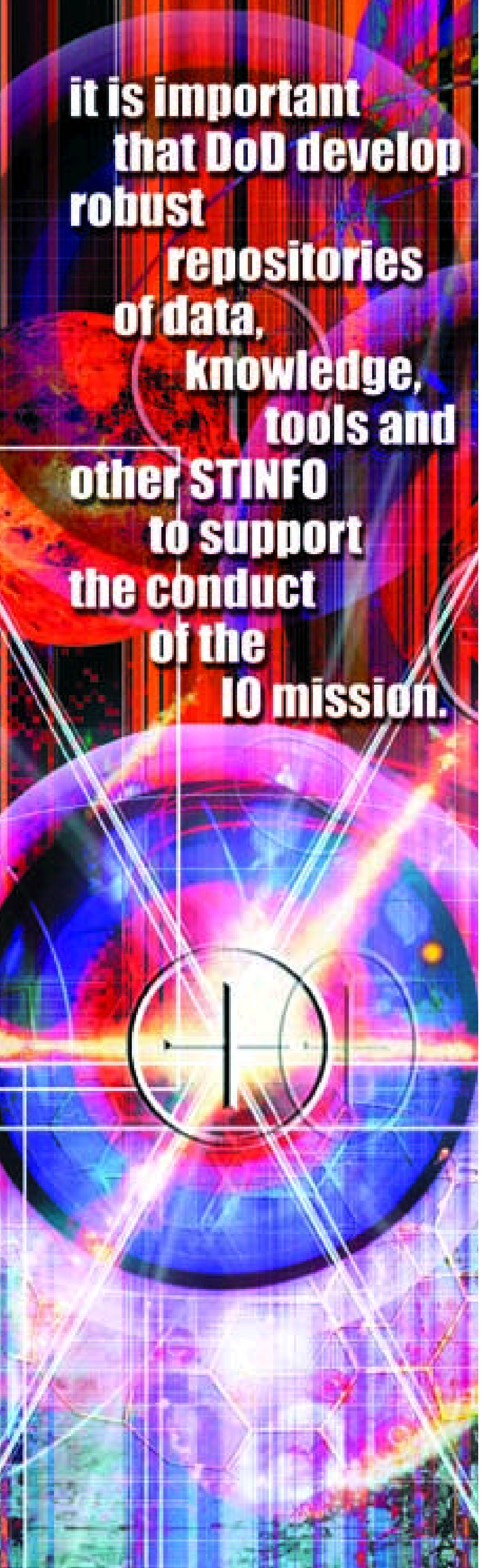
- Specific IA/IO focused organizations were identified, and points of contact in each of these organizations were sought to solicit involvement.
- A list was developed of other Government and commercial organizations whose primary mission might not be IA/IO related, but who might have a need to use some form of IA/IO M&S tool. Again, specific points of contact in each of these organizations were sought.
- Several group E-mail lists and E-mail reflectors within the IA M&S community, including the Simulation Interoperability Standards Organization (SISO) C4ISR reflector, were employed to which broadcast messages were sent with the survey attached.



In total, some 100+ organizations were contacted, and over 70 surveys were returned. The survey responses were analyzed to assess which responses met the agreed definition of an M&S research activity or M&S tool. For each response that met the definition, its primary functional application was assessed, causing the activity or tool to be grouped with like responses.

The IA/IO M&S tools were composed across the various functional categories. M&S related research in each area was also reviewed and assessed. Recommendations were made for future research and development investments to help further advance IA/IO M&S.

From a security perspective, many of the tools, techniques, and research in the field of



it is important that DoD develop robust repositories of data, knowledge, tools and other STINFO to support the conduct of the IO mission.

IA/IO are highly sensitive. The survey focused on resources that could be discovered in the open, unclassified arena.

The responder's descriptions were accepted with no change; that is, the accuracy of the description was not questioned, only whether it—

- met the definitions
- was sufficiently mature to be considered
- was adequately described to be understood.

Lastly, in terms of the scope of the assessment, the list of tools presented, although not necessarilly complete. Rather, it is believed that this is one of the most comprehensive assessments to-date, and is representative of what exists across the greater IA community. The success of any survey of this kind irelies on the willingness of organizations to share data as well as their personnel's availability to take the time to complete a survey. IA M&S research activities and tools described represent the relative quantity and quality of activities across the various functional application areas that have been defined. In other words, it is contended that there was an adequate sample size in the set of 70+ responses to portray the overall state of the art of IA M&S today.

The importance of IO to the warfighter is clearly articulated in JV 2020, which describes Information Operations as one of the five fundamental aspects of the "*Conduct of Joint Operations.*" JV 2020 states that "*Information Operations are essential to achieving full spectrum dominance.*" Even more strongly, it goes on to describe the criticality of the IO mission in terms of the following: "*...operations in the information domain will become as important as those conducted in the domains of sea, land, air and space.*" Joint Vision 2020 further acknowledges the roles of some of the various components of the IO mission when it states "*Activities such as information assurance (IA), computer network defense and counter-deception will defend decision-making processes by neutralizing an adversary's perception management and intelligence collection efforts, as well as direct attacks on our information systems.*"

With this increasing criticality of IO and its various components to the success of the warfighter, it is important that DoD develop robust repositories of data, knowledge, tools (including models and simulations) and other Scientific and Technical Information to support the conduct of the IO mission. Indeed, Joint Vision 2020 confirms this need when it states that "*The task of integrating Information Operations with other joint force operations is complicated by the need to understand the many variables involved. Our understanding of the interrelationship of these variables and their impact on military operation will determine the nature of information operations in 2020.*"

An understanding of the variables involved in IO and IA requires the development of an authoritative body of knowledge that captures such information. How these variables impact military operations can be studied with the development of proper modeling and simulation tools.

To understand modeling and simulation, the DoD Defense Modeling and Simulation Office developed the following definitions—

- **Model:** *"A physical, mathematical, or otherwise logical representation of a system, entity, phenomenon, or process."*
- **Simulation:** *"A method for implementing a model over time."*

The 2000 Defense Technology Area Plans provided further evidence of the emerging widespread recognition of the need for IA/IO M&S tools.[3] The Defense Technology Objectives for 2000 under the sub-heading of Information Systems Technology Objectives, IS.56 Information Assurance and Survivability Systems (IA&S), lists the following—"*The objective of the IA&S Systems programs is to provide information system defense capabilities against sophisticated adversaries to allow sustained critical information systems functionality. They will do so by creating design techniques, tactical and strategic operational control techniques, and advanced flexible technology.*" Among the aspects of the IA&S Systems' programs that point to a need for IA M&S tools are efforts that seek to—

"create a science-based environment for system design and assessment that will yield improved assurance and eventually allow for faster design and assessment at less cost;

create an operational human decision-making framework by creating cyber situation understanding techniques and course-of-action (COA) generation and analysis techniques that give the ability to orchestrate actuators to carry out an effective information warfare defense despite imperfect systems and limited resources."

In summary, an increased need for and attention to IA M&S provided the impetus for the assessment. The report shows that much progress has been made in developing and applying M&S tools to support IA. As organizations suffer dire consequences from attacks, they become more motivated, as do others, to invest in understanding how to better protect their infrastructure. The assessment shows that there has been a tremendous increase over the past several years in the diversity of M&S tools developed to support IA practitioners. It also shows that considerable good work is emerging to set the initial foundation for further development of IA M&S tools.

It appears that the overall state of IA/IO M&S is quite healthy today, as many different M&S tools are being used or under development to address a variety of IO and IA related issues. In comparison to the results of a similar IATAC assessment conducted over three years ago, many more organizations are now investing in developing M&S tools to address a variety of analytic needs that incorporate some aspect of IA. Furthermore, the need for continued investment in a variety of IA/IO M&S tools is recognized at the highest levels of DoD. Despite all this investment and attention, IA/IO M&S tool development is still very much in its infancy, with much work still to be done to provide an authoritative body of knowledge to support future tool developments.

IA/IO M&S Progress over Last Few Years

In revisiting the conclusions from the IATAC IA M&S tools report of 1997,[4] considerable progress has been made over the past few years. Below are the four principal conclusions from the prior report, each followed in italics by the new assessment of how things have changed—

1 **Future warfighting capabilities depend on IA.** While granting that to succeed in military affairs the information environment must be dominated, the prior report went on to stress that unclassified models, simulations, and tools for IA evaluations, training, and acquisition generally do not exist.

There has been considerable growth in the number and diversity of IA M&S tools at the unclassified level have grown considerably to address a variety of needs.

2 **Metrics are needed for IA assessments.** The prior report concluded that development of models to evaluate IA has not kept pace with the evolution in information systems, their application, and their role in decision making.

Considerable progress has been made in developing various bodies of metrics to assist with IA assessments, though there is still a general lack of authoritative and complete data sources.

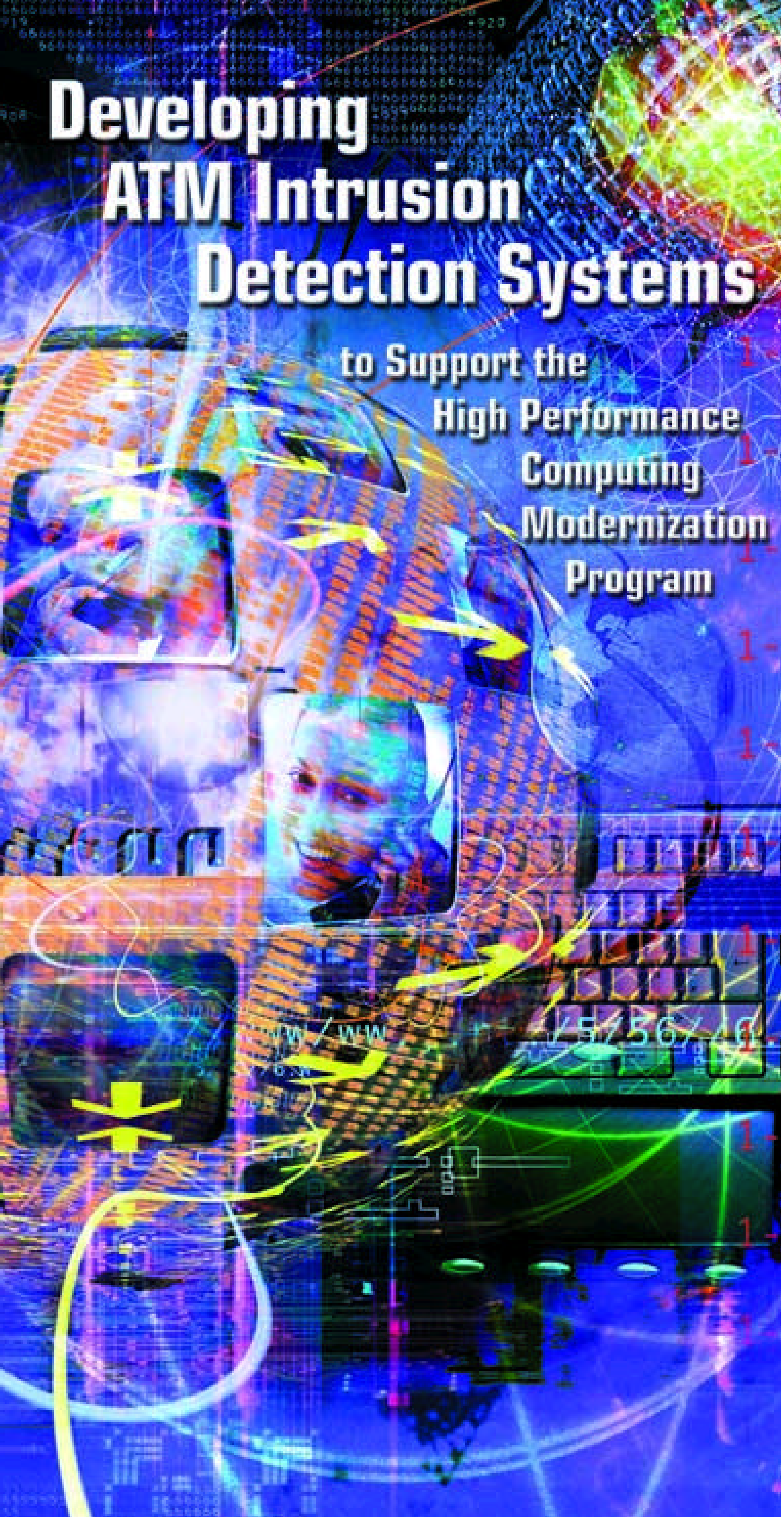
3 **Additional M&S tools are needed to support IA.**

Numerous IA/IO course of action tools have been developed over the past few years to support prioritization and allocation decisions at varying levels of command and various levels of detail.

4 **IA M&S capabilities are nascent.** The prior report concluded that because of the youth of IA M&S, there are many gaps in the tools, models, and simulations inventory of

continued on page 12

Developing ATM Intrusion Detection Systems to Support the High Performance Computing Modernization Program



by Mr. Joseph Molnar

The Defense Research Engineering Network (DREN) is a sophisticated and robust DoD communications network. As a virtual private network over a commercial grid, DREN leverages public sector investments in the telecommunications infrastructure to provide interoperable asynchronous transfer mode (ATM) and Internet Protocol (IP) services for video, audio, imaging, and digital data. DREN enables over 5,200 scientists and engineers at defense laboratories, test centers, universities, and industry sites throughout the United States to use High Performance Computing Modernization Program (HPCMP) computing resources and to collaborate on distributed Research, Development, Test & Evaluation (RDT&E) and Modeling and Simulation (M&S) experiments and demonstrations.

The network links user sites to four major shared resource centers (MSRCs) and 17 distributed centers (DCs) collectively referred to as Shared Resource Centers (SRCs). DREN already has 77 sites; more than 46 are ATM sites, and the rest are IP sites. The network provides DS3 or OC-3 connectivity to most user sites and several DCs, and provides OC-12 to the four MSRCs and selected DCs. The HPCMP plans to establish OC-48 (2.4 Gbps) connectivity in the future for the MSRCs.

HPCMP Security Architecture

The HPCMP is responsible for ensuring that the DREN provides security measures that are equivalent to those employed by other DoD networks. The HPCMP security architecture is shown in Figure 1. From a network perspective this means that, at the boundary between the internet and the DREN, protective measures are in place. As currently implemented, this consists of Access Control Lists (ACLs) on the gateway routers and Intrusion Detection Systems (IDSs) placed to monitor all exchanged network traffic. The DREN also implements router ACLs and IDSs to buffer selected sites from the DREN. From DREN's perspective, sites represent enclaves. In the case of ACLs, central monitoring and control is maintained by the DREN Intersite Services Contract Network Operations Center (DISC NOC), under the direction of the HPCMP with technical assistance from the DREN Technical Advisory Panel. Similarly, IDS systems are centrally monitored by the HPC Computer Emergency Response Team (HPC CERT). Additional protections beyond these buffering measures are implemented by the site, according to the site's military Service policy. Often these include firewalls, service IDSs, virus filters, etc. To further enhance DREN security, plans are in place to implement, in the follow-on contract, additional means to ensure the protection of data.

HPCMP has the responsibility of ensuring that the supercomputer resources are protected within the SRC's site infrastructure. The use of traditional UNIX static passwords is very risky and subject to a variety of hostile attacks. To mitigate those risks, Kerberos with SecurID authentication must be used instead of traditional UNIX passwords for accessing HPCMP resources. To further enhance the security posture, Security Test & Evaluations (ST&E), Security Assistance Visits (SAVs), and National Security Agency (NSA) assessments are performed on a regular basis, with at least one of these evaluations performed yearly.

ATM IDS Development

All of the elements to support the HPCMP security architecture are not commercially available. IDSs to support network interfaces, other than Ethernet and Fibre Distributed Data Interface (FDDI), are not commercially available. To address this deficiency, the HPCMP invested in a cooperative development project with the Department of Energy's (DOE) Lawrence Livermore National Laboratory (LLNL). The agreement provided the HPCMP with access to the LLNL's Joint Intrusion Detection System (JIDS) source code and provided LLNL with access to DREN's ATM interface capabilities and associated improvements. The goal of the effort was to provide ATM IDS systems to support the HPCMP and LLNL security architecture as well as facilitate a transition to the operational components of the DoD and DOE.

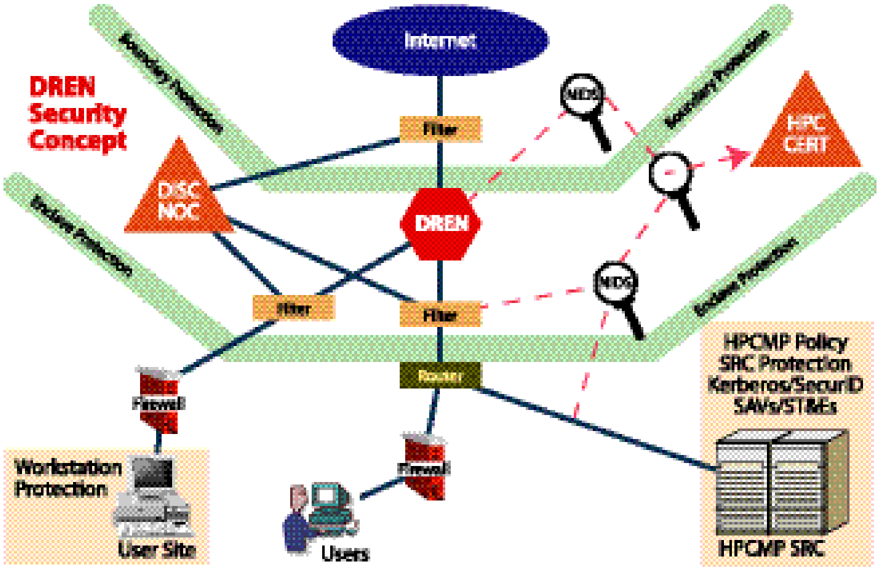


Figure 1. High Performance Computing Modernization Program (HPCMP) Security Concept

The project consisted of several technical development efforts and practical integration challenges. The technical development challenges consisted of developing ATM driver and software interface components to capture the network traffic consisting of ATM cells, identifying TCP/IP packets, and reassembling the packets into coherent communications sessions. The integration challenges consisted of identifying a method to capture the data without introducing latency or loss, determining the critical elements of the hardware computing platform and the associated components, selecting the operating system, and optimizing the performance. Although the OC-3 and OC-12 development paths contained several

continued on page 10

diverse elements, the common architecture of each consisted of using an optical coupler to tap the fiber optic connection between switches. The coupled signal from the fiber in each transmission direction is provided to the receive port of the two ATM computer interface cards. The computer is used to process the capture of data and an additional network interface card is used to retrieve processed data from the IDS. Figure 2 shows the ATM data collection architecture. The motivation behind the OC-3 and OC-12 development was to ensure that the IDSs would be available to meet the network interfaces deployment schedule.

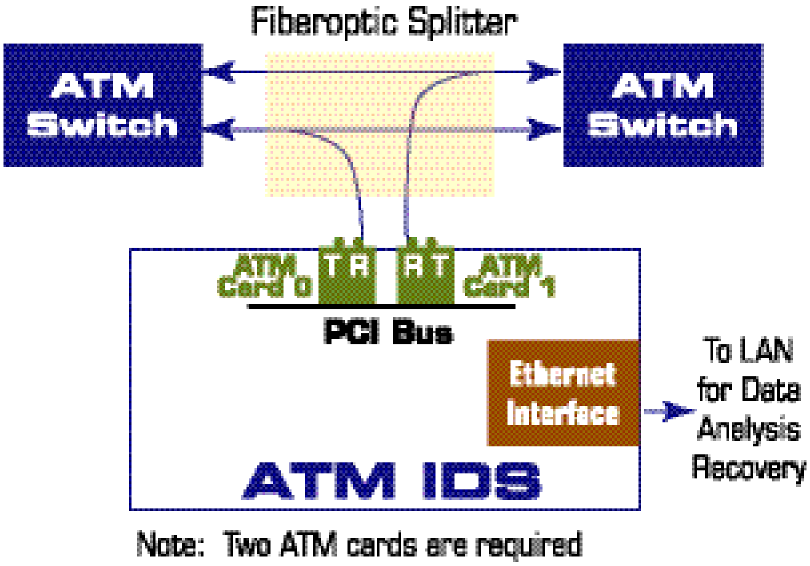


Figure 2. ATM Data Collection Architecture

OC-3 ATM Development Challenges and Solutions

The OC-3 development was performed on an INTEL based computer platform using LINUX as the operating system and FORE PCA200E interface cards. The selection of the hardware platform was based partially on cost considerations and partially on the availability of general interface driver technology. The driver was originally developed for ATM data collection to feed ATM analysis software as part of the OCxMon project with CAIDA and MCI. It is a research project and is not commercially supported. The driver was originally written as part of the FreeBSD kernel and was ported to LINUX to facilitate the driver development.

The driver facilitates communications between the kernel and the hardware and provides a device interface to the kernel. The driver supports the standard device methods of open, close, read, write, poll, etc. The driver does not interface with the LINUX network drivers and does not feed or read data to/from the IP stack for interpretation. Use of this device driver does not produce a network interface, and does not allow IP traffic to be sent or received via standard methods. The only way to access the data and operations of the ATM card is by direct connection to the LINUX device.

The device driver for the FOREore PCA-200E ATM cards has been designed and optimized for data collection versus normal network operations. It does not provide an ATM network device as a normal network driver would and cannot be used in such a manner. The driver is meant to work in conjunction with a set of firmware images, which run on the ATM card itself, and with an application that directly accesses the output of the card and driver operations.

The driver keeps a vector of 16 data blocks (1 MB each) to feed up to the application. This allows for limited buffering of bursts of traffic if the application cannot process the blocks fast enough. The application calls the driver to gain access to buffered data blocks. When access is gained to a data block, the previously read data block is returned to the driver for use by the card. If the application is backlogged by data processing and has not returned the data blocks to the driver, a lock condition exists. The driver flags all blocks as belonging to the application, and cannot feed new blocks to the card. At this point, the card cannot Direct Memory Access (DMA) any new blocks to the host and simply throws them away. This condition will exist until the application reads new blocks, thereby releasing the previous blocks. As long as the application is able to read and process new blocks (by requesting them from the driver), the bottleneck can be cleared by itself. The driver will log a message to the kernel’s log facility when it stops collecting data due to filled buffers.

The driver artificially limits the number of ATM cards supported to a maximum of 2 cards. Each card has its own minor device number. Due to performance reasons and potential bottlenecks, the number of applications that can simultaneously open a single device should be limited to one. Since the driver does not currently have the capability to manage multiple contexts for multiple processes that have opened the device, a buffering architecture was developed.

OC-3 Integration Challenges

The OC-3 integration challenges consisted primarily of identifying the constriction points and integrating a viable system that could be fielded. The latency issue was removed by deciding on a passive capture mechanism. This meant that the IDS did not have to participate in the network in an active manner, nor did it present the challenge that IDS failure could impact the network operations. Passive capture has the additional benefit of masking the IDS from the network it is monitoring.

The selection of OC-3 interface cards was based on availability. The FORE PCA-200E cards were readily available and supported by the OcxMon driver interface. For optimal performance, a computer platform was selected that used a dual PCI bus architecture. The dual PCI architecture was implemented to ensure that captured data would not be limited by the internal architecture of the computer. A final feature that was decided on was a computer system that employed multiple processors in a symmetric multiprocessor (SMP) architecture. The systems fielded would support either two or four processors. A conceptual picture of the advantage that the SMP capability adds is shown in Figure 3, where multiple streams of analysis can be performed simultaneously.

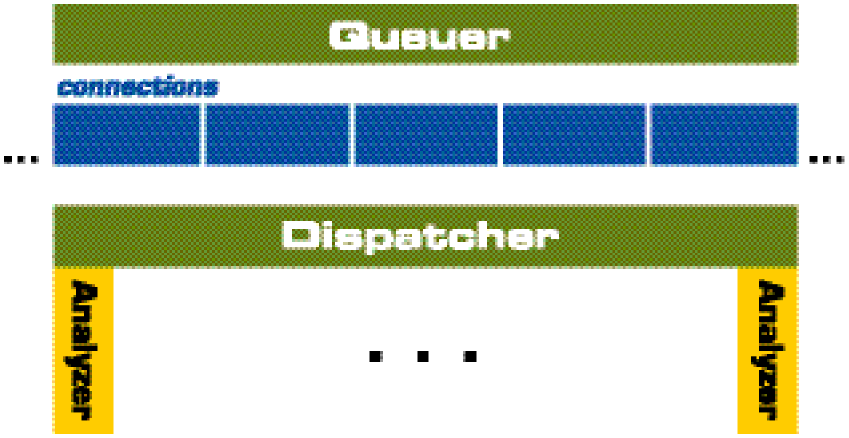


Figure 3. SMP Process Queueing System Executing Multiple Analysis Processes

OC-12 IDS – New Challenges Met

The OC-12 IDSs began as an expansion of the OC-3 development by implementing OC-12 ATM network interface cards. This approach did not support the schedule for OC-12 network deployment. The primary hurdle was that the OcxMon drivers did not support the OC-12 ATM network interface cards. To accelerate the development, a path was chosen that identified drivers for FORE HE-622 interface cards on Sun Solaris. The source code for these interface cards was available through a FORE developer's license. From that point given the experience with the OC-3 development, the OC-12 development proceeded at an accelerated pace. Where the development of the OC-3 solution took over a year to complete and field (starting in January 2000), the OC-12 development took only six months after the Sun Solaris path was selected. The first prototype was tested in September 2000, with the first operational system fielded in October. A complete complement of systems to cover all DREN OC-12 sites was achieved by January 2001.

Challenges Ahead

The development effort continues on ATM JIDS to incorporate additional features and capabilities. The development of the OC-12 IDS pointed to the fact that the streams processing architecture utilized in Sun Solaris provided the benefit of not only faster development, but also the capability to run multiple data analysis processes on the same data capture stream. This is a more efficient method of handling the data than buffering it to disk. As a result, a much cleaner programming interface was developed to interface to the ATM cards. Future plans call for employing a

continued on page 26

which only some are being addressed.

Considerable progress has been made. The assessment indicates that despite this progress, it seems the community has only begun to scratch the surface of what is needed to provide a robust set of M&S tools.

IA/IO M&S—DoD Recognition of Need

The need for continued investment in a variety of IA/IO related M&S tools is recognized at the highest levels of DoD, as demonstrated by several "Milestones/Metrics" from the 2000 Defense Technology Area Plans.[3] Listed among the Defense Technology Objectives for 2000 under the sub-heading of Information Systems Technology Objectives, IS.56 Information Assurance and Survivability Systems (IA&S) are the following—

- **FY2000—**Demonstrate automated capabilities that enable dynamic, secure collaboration between enclaves, including data and invocation flow rules. Conduct initial experiments with information assurance design methodologies, emphasizing application of science-based metrics in assessment activities. Investigate impacts and effects of dynamic response as well as active techniques for traceback and automated response. Develop initial situation analysis techniques to derive strategic attack hypotheses.
- **FY2001—**Conduct a series of experiments to foster the initial incorporation of developments in IA sciences, mathematics, and metrics into a set of design and assessment tools. Develop light autonomic systems capable of effective local adaptation. Develop preliminary attack situation forecasting techniques. Investigate initial methods for strategic attack mission-level impact and damage analysis.
- **FY2002—**Demonstrate an initial system assurance model coupled with advanced Red Team processes. Investigate increased assurance for a larger set of systems with dissimilar mission priorities. Demonstrate C2 information warfare situation understanding and COA (Course of Action) assessment.

IA/IO M&S—Still in its Infancy

A common theme was encountered repeatedly in the open literature search: IA M&S is still in its infancy. This could be attributed to the difficulty of modeling a phenomenon that is so complex that it is not fully understood. Accordingly, the "science" of describing IA/IO methods and their resulting effects is immature with much room for improvements in our understanding of the physical as well as human behavioral cause-effect relationships.

A reference to this relative immaturity of IA/IO M&S was found in several open sources, as follows:

- Fred Cohen asserts that "*The use of a cause-effect model for analyzing attacks and defenses in computer networks appears to have a bright future...but clearly this work is in its infancy*." [5]
- The Military Operations Research Society, in their October 1998 Workshop,[6] concluded, "*Current DoD analysis tools lack the capability to facilitate detailed IA analysis because C4ISR requirements generally have not addressed the need to support IA*."
- John Garstka asserts that "*Intuitively, warfighters understand that a relationship exists between information and combat power. However, capturing and quantifying this relationship has been, and continues to be, an analytical challenge of the first order*."[7]

IA/IO M&S—Current Needs

IA/IO M&S has made considerable progress in the past several years with the availability of a wide diversity of tools to address different needs and many others that will be available soon. Despite this progress, there seems to be the following major deficiencies in the current state of the art—

- A need to develop a common and agreed IA/IO Body of Knowledge (BOK), concentrating on establishing a commonly agreed and accepted lexicon, taxonomy and set of quantitative metrics
- A need for more research into human behavioral modeling so as to better and more accurately reflect the impact of the human operator and/or decision maker involved in IA/IO operations
- A need for tools that better account for the relative cost versus benefit of different IA/IO measures and actions
- A commonly agreed-upon manner in which to aggregate the detailed IA/IO activities that may occur within a conflict into campaign and/or theater-level effects (many tools provide the detailed insights, while a few tools attempt to provide the aggregate perspective, but the linkage between the two sets of tools is weak to non-existent)
- A need for a central repository for all of the above BOK products and M&S tools
- A need to develop and promote of standards that incorporate all of the above to facilitate re-use and interoperability of IA/IO M&S tools

The SOAR provides a wealth of detailed information, which could only be summarized within the bounds of this article. Still, this article offers sufficient insights to convince the reader of the value and importance of this driving document. Additionally, this article provides a valuable introduction into the evolving field of IA/IO M&S as well as it provides a comprehensive overview of the current state-of-the-art in these fields. As a final reminder, the full IA M&S SOAR may be obtained from either the IATAC or MSIAC http://www.msiac.dmso.mil/.

References

1 *National Information Systems Security (INFOSEC) Glossary*, NSTISSI No. 4009, January 1999.

2 *U.S. Joint Vision 2020", OPR Director for Strategic Plans and Policy*, J5, Strategic Division, http://www.dtic.mil/jv2020/jvpub2.htm.

3 https://ca.dtic.mil/dstp/2000docs/dtos/dtos.htm Restricted to Government and registered contractors.

4 IATAC TR-97-002, *Modeling and Simulation Activities in Support of Information Assurance*, December 1, 1997.

5 Cohen, Fred, *A Preliminary Classification Scheme for Information System Threats, Attacks, and Defenses; A Cause and Effect Model; and Some Analysis Based on That Model*, September 1998.

6 Military Operations Research Society, C4ISR Workshop Proceedings, October 1998. http://www.mors.org.

7 Garstka, John *Network Centric Warfare: An Overview of Emerging Theory*, PHALANX, December 2000.

Gary L. Waag lead this study effort in support of IATAC and the Modeling and Simulation Information Analysis Center (MSIAC). He currently manages a team of M&S professionals who provide support across the U.S. national intelligence community. He has over twenty years of engineering experience supporting diverse DoD and NATO M&S activities, including design, development, employment and management of constructive and virtual simulations used for analysis, acquisition and training support. Mr. Waag holds a M.S. in Mathematics, a M.E. in Electrical Engineering, and a B.S. in Electrical Engineering from Rensselaer Polytechnic Institute. He also holds an MBA from Pepperdine University, and has recently obtained a Graduate Certificate in C3I Systems Engineering from George Mason University. He is the chair of the Simulation Track of the 2001 ASD/C3I Command and Control Research and Technology Symposium. He is also currently the Chair of the Simulation Interoperability Standards Organization (SISO) IO-ISR Planning and Review Panel (PRP) and a member of the SISO C4I PRP.

Dr. Jerry M. Feinberg is the Chief Scientist for the MSIAC in Alexandria, Virginia. Dr. Feinberg holds a Ph.D. and M.S. in Mathematics, and an M.S. in Physics, from Stanford University, and a B.S. in Mathematics from the California Institute of Technology.

Ms. Lesley J. Painchaud is a Senior Military Analyst for MSIAC in Alexandria, Virginia. Recently retired from the US Navy, her final tour of duty was at DISA's Center for Advanced Technology. She is currently working primarily on projects to increase interoperability between simulations and C4ISR systems. Ms. Painchaud holds an M.S. in Operations Research from the Naval Postgraduate School, an M.A. in Managerial Economics from the University of Oklahoma, and a B.A. in Economics from the University of South Florida.

Mr. R. Kenneth Heist manages a number of information assurance activities including his organization's participation in the IATAC where he led the recent IATAC-sponsored Critical Review and Technology Assessment of Data Mining. Mr. Heist has been involved in information assurance, information security and communications security for 37 years. This includes a 34-year career at the National Security Agency. Mr. Heist holds an M.S. in Electrical Engineering from the George Washington University and a B.S. in Electronic Engineering from Lehigh University.

International Technology Watch Partnership

by Mr. Steven J. Sampson

The International Technology Watch Partnership (ITWP) Web site was created to provide users a near real-time venue to identify and understand international science and technology. Access to this information will allow users to make personal contacts and obtain more detailed information. Collaborative teambuilding will result through the monitoring of global science and technology research. Civil and defense developments worldwide affect our ability to ensure or maintain technological superiority. New motivations for international defense cooperation are becoming increasingly important. Thus, more informed decision-makers lead to higher payoff cooperation including involvement and accessibility with our Allies' help.

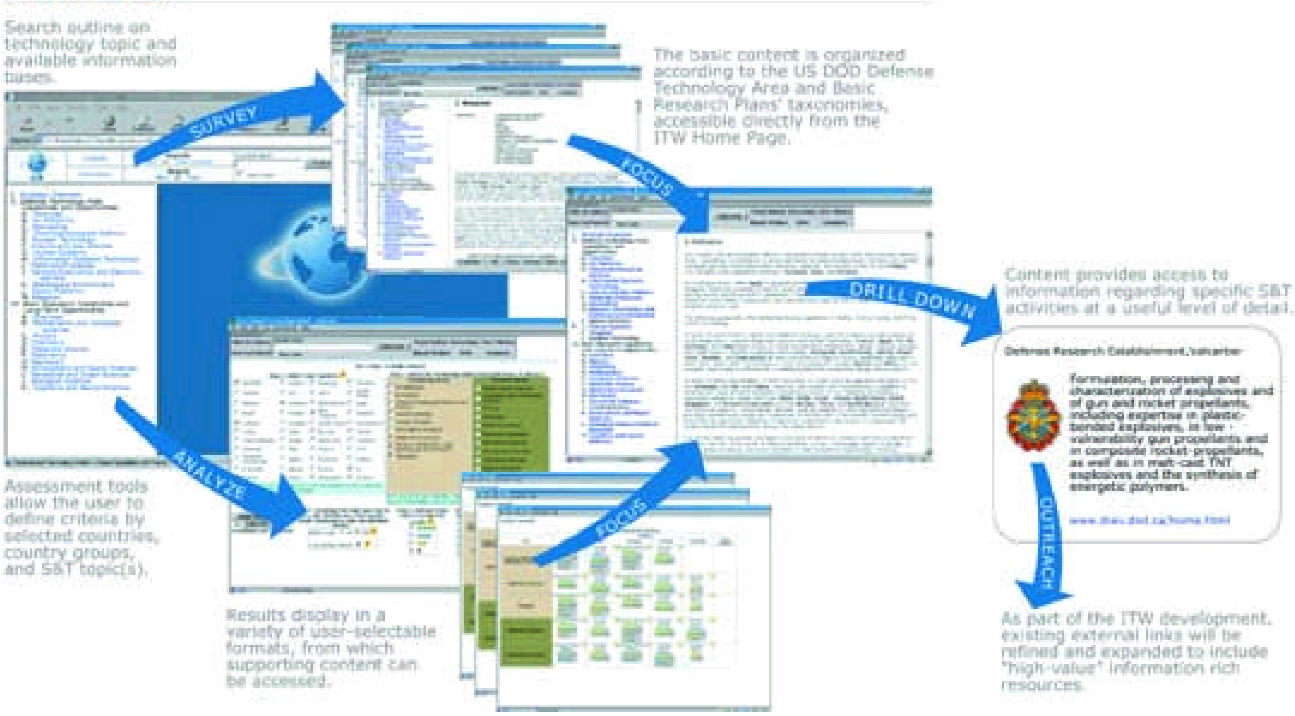
The ITWP supports a broad range of stakeholders from science and technology executives to bench level scientists and engineers. Currently, the major data partners include—

- The Technical Cooperation Program (TTCP) nations
- US Office of the Deputy Under Secretary of Defense for Science and Technology, International Plans and Programs
- US Defense Technical Information Center, Information Analysis Centers
- US Army, Air Force, and Naval Research Laboratories
- European Community Research and Development Information Service
- Asian Technical Information Program
- World Technology Watch.

The ITWP Web site will be available in 2001 to users who have registered with the Defense Technical Information Center through the US International Plans and Programs Web site at http://www.dtic.mil/intst/. The Web site uses the Internet to query worldwide organizations active in science. It creates reports using the Deputy Under Secretary of Defense, Science and Technology [DUSD(S&T)] taxonomies developed for the Defense Technology Area Plan (DTAP) and Basic Research Plan. The ITWP user completes forms from this Web site to profile the user's technical interests.

The site will also have access to information about domestic research activities through an interface with the Virtual Technology Expo (VTE) Web site.

The ITW Web Site



Search outline on technology topic and available information bases.

The basic content is organized according to the US DOD Defense Technology Area and Basic Research Plans' taxonomies, accessible directly from the ITW Home Page.

Content provides access to information regarding specific S&T activities at a useful level of detail.

Defence Research Establishment Valcartier

Formulation, processing and characterization of explosives and of gun and rocket propellants, including expertise in plastic-bonded explosives, in low-vulnerability gun propellants and in composite rocket propellants, as well as in melt-cast TNT explosives and the synthesis of energetic polymers.

www.drev.dnd.ca/home.html

Assessment tools allow the user to define criteria by selected countries, country groups, and S&T topic(s).

Results display in a variety of user-selectable formats, from which supporting content can be accessed.

As part of the ITW development, existing external links will be refined and expanded to include "high-value" information rich resources.

Virtual Technology Exposition (VTE)

by Ms. Joanne Spriggs

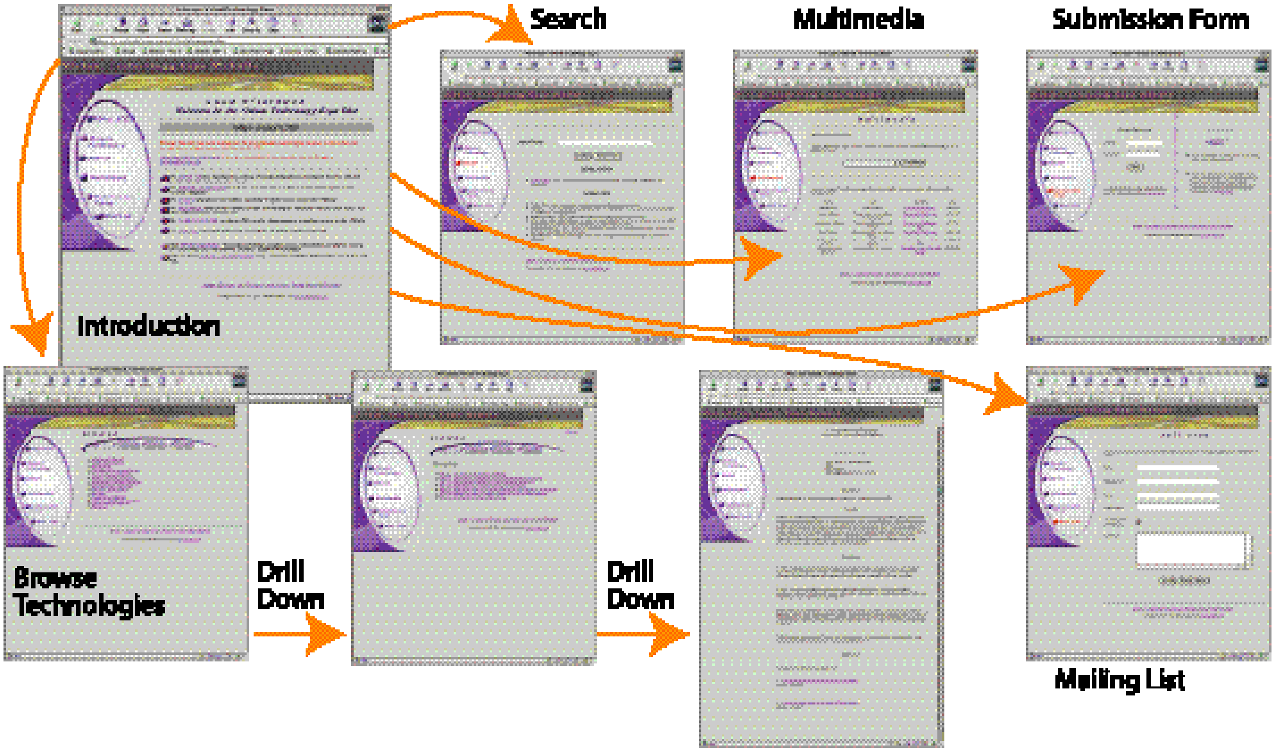
The Virtual Technology Exposition (VTE) was created to provide the defense community with information on the latest technological advancements from the defense and commercial sectors. Access to this information will enable program managers to integrate advanced research into more extensive developmental activities and reduce product life-cycle costs. The Web site (https://vte.dtic.mil) is provided as a restricted service by the Deputy Under Secretary of Defense, Science and Technology [DUSD(S&T)].

The VTE provides the S&T community, industry, academia, and the acquisition and requirements community with advanced browse technology, full-text search capabilities, multimedia tools, the ability to submit information, and E-mail services that let users know of updated information. The VTE contains reference information, points of contact, descriptions of technology advancements, articles from professional journals, and references to related Web sites on a wide variety of subjects.

A new Web site, the VTE is continually expanding its database of information on emerging technologies. As it matures, its advanced features should enable users to—

- Assist Program Managers to plan for future technology upgrades
- Monitor commercial technology and product development
- Look for technologies that show promise of enhancing Military capabilities
- Choose which technologies to leverage and which to develop with their own investments
- Access information that can lead to developing and refining requirements
- Check on the availability of resources for analysis of alternative assessments
- Obtain better information to better leverage ongoing and future technology development
- Assist industry in planning for future business opportunities
- Showcase research efforts to a broader audience.

The site will also have access to information about international research activities through an interface with the International Technology Watch Partnership (ITWP) Web site.



Life Cycle Security and DITSCAP

by Mr. John Kimbell and Ms. Marjorie Walrath

For a successful technology, reality must take precedence over public relations, for nature cannot be fooled.

—Richard P. Feynman

With the announcement that the Department of Defense (DoD) will be spending $1.5 billion on information systems security, many organizations, both public and private, have presented themselves as experts in network security in order to take advantage of this windfall. But posturing does not guarantee professional results and, in reality, many of those claiming to be security engineers and certifiers/accreditors have little in-depth experience in the field. In some cases, organizations are not familiar with DoD or federal department-specific regulations. They cannot relate to the manner in which the DoD Information Technology Security Certification and Accreditation Process (DITSCAP) should be applied. Only an informed community can separate the nascent from the experts.

The Good, The Bad, and The Ugly

The relationship between security certification/accreditation and the information network system is a life cycle commitment; therefore, it is appropriate to be wary of an organization or business with a miraculous "one price, guaranteed delivery by a certain date" sales pitch. Some organizations approach security in the same manner as their other business practices, relying heavily on marketing techniques to overcome their shortcoming. It is important to remember that although it is the foremost goal of a business to make money, the paramount goal of Government is to spend money for the general welfare of its citizens.[1] We in DoD have a well-defined responsibility to the American people, and must remember that if we make a mistake, we can damage the security posture of the entire nation.

Certification—Not Always Understood

Frequently, the C&A process is misunderstood. Many, if not most, people think that once their system has been certified they have a guarantee that it is operating in a totally secure mode. That is not what certification is all about. Consider the United States Department of Agriculture (USDA). Most of us are familiar with the phrase "Certified USDA prime," or similarly, "Certified USDA Choice." The USDA has seven different "Applicable Quality Grades" for beef.[2] The highest of these is "Prime" and the lowest is "Canner." When a shipment of beef arrives for quality grading, it is certified as to its quality, processing, size, packaging, and delivery. Each shipment is graded against these requirements. Therefore, even though all shipments are certified, there are varying degrees of quality. The same idea holds true for the security certification for information systems.

Certification in the context of information systems security means that the system has been analyzed as to how well it meets all of the security requirements that have been levied against it from various sources [AR380-19, the Orange book,[3] specific system standard operating procedures (SOPs), etc.] So the final certification statement is really saying, "We have compared your system to all of these requirements (just like the USDA) and here is what we have found— your system meets 82% of these requirements. Of the 18% of the requirements that your system does not meet, X% are vulnerabilities that lead to extremely high risk, Y% are vulnerabilities that lead to high risk..." and so on.

Promises, Promises, Promises...

The DITSCAP is flexibly designed to accommodate the changes that are an integral part of the security certification and accreditation process. Many inexperienced companies drop the ball here. Their claim to provide a total systems C&A in a specified time is not achievable. First, if they are going to be involved in the certification process they must be involved in all four phases of that process, and there is simply no way to determine how long each phase will last. Additionally, at the completion of each phase and before the next phase begins there is a chance for each of the proponents to negotiate or re-negotiate what they will do, and a chance to renegotiate cost. As the process unfolds there will quite often be changes to the system, and the DITSCAP's flexibility allows for these changes. However, many of the organizations claiming to be C&A experts choose to ignore the fact that these changes will occur in the development of any new system. They ignore the realities of changing requirements, thus inviting slipped timelines and additional costs. It is not enough to "certify the box"—they must be willing to look behind the box, around the box, and to see where the box leads. C&A is an iterative and evolutionary process.

Phase 1: Definition

The main proponents of the C&A process come together for the first time in phase one. These proponents are the designated approving authority (DAA), user representative, project manager (PM), and certifier. The DAA is the individual responsible for ensuring that the system operates with an acceptable level of risk. The certifier is the individual responsible for ensuring that the DAA has been given sufficient information regarding those risks.

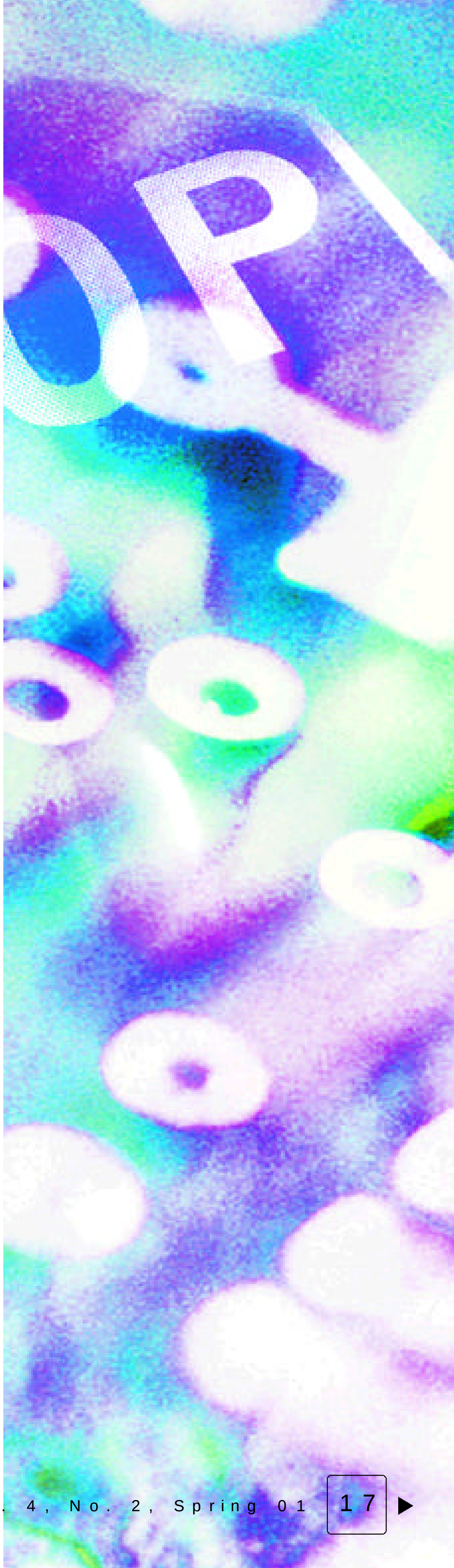
It is in this initial phase that the DAA appoints the certifier by issuing an actual appointment letter listing that individual as certifier for the specific system being certified. For the remainder of the process the certifier will—

- Act as a trusted agent of the DAA
- Provide support to the DAA by conducting a comprehensive evaluation of both the technical and non-technical security features of the system under evaluation.
- Recommend to the DAA whether or not to accredit the system after the certification process is completed.

The DITSCAP also allows for the creation of certification teams under the direction of the certifier to support the certifier in the actual security testing.

During this phase the level of the certification effort must be defined, and the requirements that affect the system must be determined. The DITSCAP calls for four different levels of certification. See Table C3.T8 of the DoD 5200.40-M.

- **Level 1: Minimum Security Checklist.** Requires completion of the minimum security checklist. The system user or an independent certifier may complete the checklist. This required checklist can be found in Appendix 2 of DoD 8510.1-M, the DITSCAP Application Document.
- **Level 2: Minimum Analysis.** Requires completion of the minimum security checklist and independent certification analysis as defined in the verification and validation phases.
- **Level 3: Detailed Analysis.** Requires completion of the minimum security checklist and more in-depth, independent analysis as defined in the verification and validation phases.
- **Level 4: Extensive Analysis.** Requires completion of the minimum securi-



ty checklist and the most extensive independent analysis as defined in the verification and validation phases.

To determine the required analysis level, refer to Table C3.T9 (System Characteristics) of the DITSCAP Application Manual 8510-1.M (Figure 1). Select the alternative for each of the characteristics that describe the system. Each characteristic has an assigned weight, which is entered in the right column. The total of these weights is used to determine the appropriate certification level.

Characteristic	Alternatives and Weights	Weight
Interfacing Mode	Benign (w = 0), Passive (w = 2), Active (w = 6)	
Processing Mode	Dedicated (w = 1), System High (w = 2), Compartmented (w = 5), Multilevel (w = 8)	
Attribution Mode	None (w = 0), Rudimentary (w = 1), Selected (w = 3) Comprehensive (w = 6)	
Mission-Reliance	None (w = 0), Cursory (w = 1), Partial (w = 3), Total (w = 7)	
Availability	Reasonable (w = 1), Soon (w = 2), ASAP (w = 4) Immediate (w = 7)	
Integrity	Not-applicable (w = 0), Approximate (w = 3), Exact (w = 6)	
Information Categories	Unclassified (w = 1), Sensitive (w = 2), Confidential (w = 3), Secret (w = 5), Top Secret (w = 6), Compartmented/ Special Access Classified (w = 8)	
	Total of all weights.	

Figure 1. Table C3.T9, System Characteristics

Table C3.T11 (right) shows an example of a completed System Characteristics table. From this, we see that the system had a total of 27 points.

Characteristic	Alternative	Weight
Interfacing Mode	Active	6
Processing Mode	System High	2
Attribution Mode	Basic	3
Mission-Reliance	Total	7
Availability	ASAP	4
Integrity	Approximate	3
Information	Sensitive	2
	Total of all weights	27

Figure 2. Table C3.T11, Certification Level Example

Based on the total weights calculated, the next step is to select the certification level from table C3.T10 of the DITSCAP 8510-1.M. This brings to light an interesting point.

Table C3.T10 shows the areas of possible contention from using the DITSCAP. From the table we see that the areas between 12 - 16, 24 - 32, and 38 - 44 overlap. This means that either a level one or two, level two or three, or level three or four certification could be required if the total points from table C3.T9 fall into one of those ranges. This is where the "negotiation" aspect of the DITSCAP enters in play. The DAA, certifier, PM, and user representative must collectively agree on the level of effort to be expended on the certification. This is normally accomplished with a minimal amount of bloodshed, and the final decision rests with the DAA, as the DAA will be the official responsible of accepting the risk.

Requirements Traceability Matrix (RTM)

Task 1-5 of the DITSCAP requires the determining of the system's security requirements. This includes the requirements of the DITSCAP, Army Regulation 380-19,[4] DISC4 policy memos, patches to the operating system or applications, the system SOPs, and any other requirements that apply to the system. The proponents, specifically the security engineer and the certification team, must analyze the directives and security requisites to determine the applicable security requirements that apply to the system. They will normally take a section of a directive and parse it into a basic security requirements

Certification Level	Weight
Level 1	If the total of the weighing factors in Table 3-1 are < 16
Level 2	If the total of the weighing factors in Table 3-1 are 12-32
Level 3	If the total of the weighing factors in Table 3-1 are 24-44
Level 4	If the total of the weighing factors in Table 3-1 are 38-50

Figure 3. Table C3.T10, DITSCAP Levels of Certification

statement. The security requirements will then be entered into the RTM to support the remainder of the C&A effort.

In the example below the matrix shows the "Source Document," or regulatory requirement, and the specific paragraph of the requirement that is to be tested.

A spreadsheet format serves well as an RTM, and a comment block may be added to supply more specific details. The RTM follows the requirements through the System Security Requirements Specification (SSRS), and shows the specific paragraph in the Security Test and Evaluation (ST&E) procedure where the requirement is actually tested. The "Evaluation Method" column indicates the type of assessment made—DITSCAP uses I= Interview; D= Document review; T=Test; and O= Observation. A legend explaining these methods may be provided within the spreadsheet as well. The next block shows whether the requirement was met or not. The certifier uses the RTM to follow the progress of the certification effort throughout the entire process. Moreover, at the completion of the certification it provides a handy overview of the entire effort. The RTM makes it easy to see at a glance which requirements were either met or not.

At the end of the first phase, the proponents have an understanding of exactly what resources the certification process will require. The level of certification has been negotiated, as have the requirements that will be tested or verified during phase two. At the end of this phase, the proponents sign the System Security Authorization Agreement (SSAA), meaning that they all agree to fulfill these requirements.

Source Document	Paragraph	SSRS Reference	Certification Procedure Ref.	Evaluation Method	Met	Not Met
AR 380-19	2-3a(2)	2.2.1.1	4.2.1.3.1	I	X	
AR 380-19	2-14i	2.2.2.5	4.2.2.3.9	O	X	
AR 380-19	2-14h	2.2.2.13	4.2.2.3.21	D	X	
AR 380-19	2-24e	2.2.1.9	4.2.1.3.13	T		X

Figure 4. Requirements Traceability Matrix

Phase 2: Verification

The major occurrences that take place during this phase are—

The System Security Authorization Agreement (SSAA) is refined. During this phase, the SSAA is being updated as changes occur. It is important that all of the proponents are made aware of any changes made to the system, because any change can affect the scope of the C&A effort. This is a good example of why some organizations in the C&A business fail to complete the certification process. They may be under the impression that theirs is a limited role, while the exact opposite is true. The certifier and the team must be actively involved in each event that occurs throughout the entire process.

The system is developed. As the system is developed it is likely that changes will also occur that may impact the C&A process. It is possible that significant changes will even change the certification level itself. It is also important to remember that the requirements of the SSAA are followed throughout the life cycle of the system. As the size and complexity of the system under development changes, so will the security requirements and thus the C&A effort.

The certification process is analyzed to ensure that it is sufficient. Because of the changes that have been made to the system, it is necessary to evaluate the security requirements as well to insure their adequacy. This evaluation may lead to the introduction of new or more stringent requirements, or it may necessitate the removal of some of the require-

ments decided upon in Phase 1. Table C4.T1 of the DITSCAP application manual[5] defines seven certification tasks to be conducted during this phase.

1. System Architecture Analysis
2. Software Design Analysis
3. Network Connection Rule Compliance Analysis
4. Integrity Analysis of Integrated Products
5. Life Cycle Management Analysis
6. Security Requirements Validation Procedures Preparation
7. Vulnerability Assessment

The system is ready. Before entering the actual Validation Phase (Phase 3) the determination is made that the system is ready to be certified. This means that the system is deemed ready for testing of the fully integrated system and its environment, both hardware and software. The system has been evaluated at each step of its development, and any discrepancies identified by the certification team are brought to the attention of the PM, DAA, and user representative so that corrections or modifications may be made.

Any additional resource requirements are reported to the DAA. These additional resources may be required because of a significant change to the scope of the certification effort. Even seemingly insignificant changes to the system design during this phase may require a much more stringent approach to the certification process.

Phase 3: Validation

This is the phase that most people think of when they think of certification, and that which causes the most confusion to those with doubtful credentials. It is imperative that the certifier and certification team have been active throughout the entire process, and not just this single phase. The certifier and certification team have been instrumental in getting the process to this point, and have provided critical input as to the level of certification, the requirements to be leveled against the system, and in the overseeing of the system development. Now the certifier and certification team have the lead in the C&A effort.

System Test and Evaluation (ST&E).

At the heart of this phase lies the ST&E procedure, a detailed description of the testing of security features to be performed during development in its fielded environment in support of certification. It describes the specific requirement (referenced to the RTM), states the purpose of the test, and delineates the criteria for success. Given the variance and complexity in systems, it is impossible at this time for one set of requirements to effectively fulfill these criteria. Exercise caution when faced with claims that a single tool can do this job – one size does not fit all! The DoD application manual provides an example of the format for each of these test procedures as shown below (comments are italicized)—

1.0 *(Security Policy, or other heading for the major functional area under test)*

1.1 RTM# *(reference to the specific requirement in the RTM)*

Source: *(AR 380-19, Orange Book, etc.)*

1.1.1 Requirement to be tested—*The actual verbiage from the source*

1.1.2 Test Objective (Purpose)—*The reason that this specific test is being conducted*

1.1.3 Test Method (Inspection, Test, or Analysis)—*(Inspection, test, evaluate, demonstration; or:* I= Interview; D = Document review; T = Test; and O = Observation)

1.1.4 Test Scenario (Test Setup)—*A description of any requirements needed to conduct a test, such as setting up user accounts, or test equipment*

1.1.5 Test Procedures—*An exact, detailed explanation of how the test was conducted. This area must contain a detailed, step-by-step list of exactly how the requirement was tested so that the results can be duplicated*

1.1.6 Expected Results—*The expected outcome of the test*

1.1.7 Actual Results—*The actual result of the test. May be "As Expected," if the test passed*

1.1.8 Overall Results/Conclusions— □ Met □ Not Met *Whether or not the requirement was met*

1.1.9 Comments—*Any comments that the certification team feels necessary to explain the result obtained goes here*

1.1.10 Date Tested, Tested By. *It is important that the person actually conducting the test fill this out when the test is performed. An actual certification will usually have several hundred of these procedures, and this is how it is determines that the test was actually performed.*

Other testing areas required under the DITSCAP are penetration testing, verification of TEMPEST compliance (if required), verification of communications security (COMSEC) (if required), a system management analysis, a site accreditation survey, an evaluation of the contingency plan, and a risk management review. Also, in most cases a review of the documents listed below is also required. These documents are generally received from the security engineer—

- System Design Plan (SDP)
- Threat Description
- Security Policy (includes system, network, & physical policies)
- Configuration Management Plan (CMP)
- Certification Plan (with certifier)
- Continuity of Operations Plan (COOP)
- System Security Requirements Specification (SSRS - developed with input from the certifier)
- Security Training & Awareness Plan
- Trusted Facilities Manual (TFM)
- Security Features Users Guide (SFUG)
- Incident Response Plan

The certification team works closely with the security engineer and system engineer throughout this phase, as well as throughout the entire process. The security engineer and the certifier maintain a close relationship during the C&A process so that problems may be identified and resolved as soon as possible. It is important that the security engineer be made aware of any extremely high risks as soon as they are identified so they can be mitigated.

Additional Documents Produced

In addition to the ST&E procedures, the certification team must also provide the following documents: Risk Assessment Report (RAR—previously known as the Security Risk Management Review), Certification Evaluation Report (CER), and the Certification Statement. Each of these documents is discussed below.

Certification Evaluation Report (CER)

The CER contains the "raw" results of the certification testing (ST&E) and forms the foundation for certification. It presents the overall security test philosophy, the detailed ST&E procedures, and the test results with comments from the testers.

The number of attachments to the CER depends on the system's complexity. For instance, they can be organized by function and have one attachment for routers, one for terminal servers, one for print servers, one for E-mail servers, etc. Or, they might be organized by equipment and have one for Windows NT servers, one for Windows 95 platforms, one for CISCO devices, etc.

There may also be a separate section showing the actual results from any automated scanning tools that were used on the system, and one providing the results of the Site Accreditation Survey.

Risk Assessment Report (RAR)

The DITSCAP calls for a document that provides an analysis of the ST&E failures. This document includes an examination of the threats, vulnerabilities and the resulting risks to the system. In this document each requirement that was not met during the ST&E is viewed as a vulnerability and assigned a risk

continued on page 22

continued from page 21

level. The associated risk may be classified as either extremely low, low, moderate, high, or extremely high. This classification is determined by the certification team, and is discussed with the security engineer before a final determination is made. For each risk that is extremely high, this document describes the security weakness and explains why it constitutes vulnerability. Fixes (enhanced or additional countermeasures) are suggested, along with an explanation of how they would reduce the risk. "Initial risk" (as is) and "residual risk" (with the additional countermeasures) are estimated.

Certification Statement

The Certification Statement is the Certification Authority's report to the DAA on the results of the certification testing. It includes a recommendation to either accredit the system, or not. It may recommend an Interim Approval to Operate (IATO) for up to six months while "High" or "Moderate" risks are being fixed.[6] The Certification Statement is prepared by the Certifying Agent, and is signed by both the Certification Agent and the certifier. The Certification Statement will contain one of the following recommendations:

- **Full Accreditation—**The system is approved to operate with acceptable risk in the intended environment as stated in the SSAA.
- **Interim Approval to Operate (IATO)—**The system contains unacceptable long term risk but mission criticality mandates the system become operational. Use of the IATO requires a return to Phase 1 to negotiate accepted solutions, schedules, necessary security activities, and milestones. After the six-month period, those risks will be looked at again, and the threat to the system reassessed. Before any IATO may be issued, Phase 2 and 3 activities must be completed and appropriately documented. This ensures the repeatability of the process.
- **Disapprove Accreditation—**The system contains extremely high risks. The liability is too great to allow the system to be operational. This type of recommendation requires a return to Phase 1 to renegotiate previously accepted solutions, necessary security activities, and milestones. The system must complete Phases 2 and 3. Again, as stated above, this ensures repeatability in the process. If the DITSCAP process is rigorously followed by competent security experts it is unlikely that a recommendation to disapprove accreditation should ever be made.

Phase 4: Post Accreditation

Phase 4 contains process activities necessary to operate and manage the system so that it will maintain an acceptable level of residual risk. It begins after the system has been integrated into the operational computing environment and accredited, and continues throughout the life of the system. It is the responsibility of the Information System Security Officers (ISSO), the DAA, and system operators and administrators to maintain the security posture of the system. The claim of some organizations to make the re-accreditation process easier for their customers can be misleading, as the role of the certifier is somewhat limited. Army Regulation 380-19 requires re-accreditations within three months following any event below—

- Addition or replacement of a major component or a significant part of a major system
- A change in classification level of information processed
- A change in security mode of operation
- A significant change to the operating system or executive software
- A breach of security, violation of system integrity, or any unusual situation that appears to invalidate the accreditation
- A significant change to the physical structure housing the AIS that could affect the physical security described in the accreditation
- The passage of 3 years since the effective date of the existing accreditation
- A significant change to the threat that could affect Army systems
- A significant change to the availability of safeguards
- A significant change to the user population

AR 380-19 is very specific as to what must be accomplished, and even the timeframe in which re-accreditation must be accomplished. Re-accreditation will include the same steps accomplished for the original accreditation; however, those portions of the documentation that are still valid need not be updated. Therefore, as long as there

continued on page 26

Today's Information Security Challenge CyberWolf

by Mr. Jim Litchko

Recent high-profile information security breaches illustrate the crippling impact that a single cyber attack can have on an otherwise well-established business. Over the past decade, hundreds of technical security countermeasures [i.e., firewalls, routers, authentication servers, intrusion detection systems (IDS), secure E-mail, virtual private networks (VPNs), etc.] have been deployed to counter this growing threat.

The fundamental flaw of these security countermeasures stems from the proprietary detection and reporting methodologies that the devices use to record network activity and generate security alarms. Designed for auditing, not monitoring, these reporting systems generate an immense volume of data that is virtually impossible to interpret. Even the most experienced security engineers often struggle to separate critical security events from large volumes of log data. Compounding this problem, many IT departments lack the resources to dedicate qualified security experts to continuously monitor and update security devices deployed throughout the network.

In sum, effective information security practices depend upon an organization's ability to monitor, maintain, and quickly re-configure critical systems to protect against emerging threats. As such, in-depth and ever-evolving information security expertise and the ability to manage security components are the two cornerstone requirements of an effective information security program. Failure to meet these requirements diminishes an organization's ability to defend against the latest information security compromises.

CyberWolf enables the capture of expert knowledge of the Security Analyst/administrator. It employs advanced communications, reasoning and analytical technologies to maximize the effectiveness of the Security Analyst/Administrator. Developed under the Defense Advance Research Project Agency (DARPA), CyberWolf has been proven in deployments, over and over, to be versatile, scaleable, and highly effective in leveraging sensor and knowledge bases. Vendor independent, CyberWolf augments existing and future system security components (such as firewalls, VPNs, etc) withing the security infrastucture of an enterprise.

CyberWolf aims to reduce the workload of an overworked, understaffed, untrained and more often under-trained security management team that is responsible for the security of an enterprise. The software device experts contain knowledge about how to process a security component's audit information. The Device Experts use this expert knowledge to filter and interpret the audit events as they are produced by the security components to identify significant security events and/or alarms and forward only the relevant security information to a higher-level server used by the security administrators/analysts. Device Experts may reside on or outside the security components depending on the implementations they are required to support. A security manager which resides on a trusted server and contains knowledge about how to correlate information from heterogeneous streams of information and knowledge about the enterprise to declare and respond to incidents in real-time. A real-time rule-engine is used in the security manager to process the event/alarm streams in real-time, correlate it with other events, generate tracking rules on the fly and automatically produce incidents tickets. This real-time rule-engine, being light-weight in nature, is also used in Device Experts to reason about audit streams. A database is used in the security manager to capture the events and incidents for persistence and tracking of low-intensity events/alarms. A simple user interface presents the security administrator/analyst with a list of incidents and drill-down capability to facilitate reasoning about the incident and bring it to closure. Finally, a messaging system supports the ‘secure’ collection and distribution of from heterogeneous sources with built-in failure modes to prevent loss of data during intermittent connections.

CyberWolf presents a small list of incidents that require the Security Administrator/Analyst with the most important information that requires attention. Conclusions as opposed to raw events are generated by the system. Detailed information that supports these conclusions are correlated and tracked in the same incident ticket. Any actions taken either by the system and/or by the Security Administrator/Analyst are captured in the same incident ticket to avoid confusion.

CyberWolf is currently being used throughout the government to manage and monitor IT security operations. Three examples are the Federal Emergency Management Agency (FEMA), U.S. Navy, and the U.S. Air Force.

FEMA has deployed CyberWolf to monitor the Agency's network perimeter defenses. FEMA is currently the largest deployment of CyberWolf supporting a network that has 10 thousand nodes deployed over 10 regions in the United States. CyberWolf requires only one-half person to monitor and manage the following security components within the FEMA system:

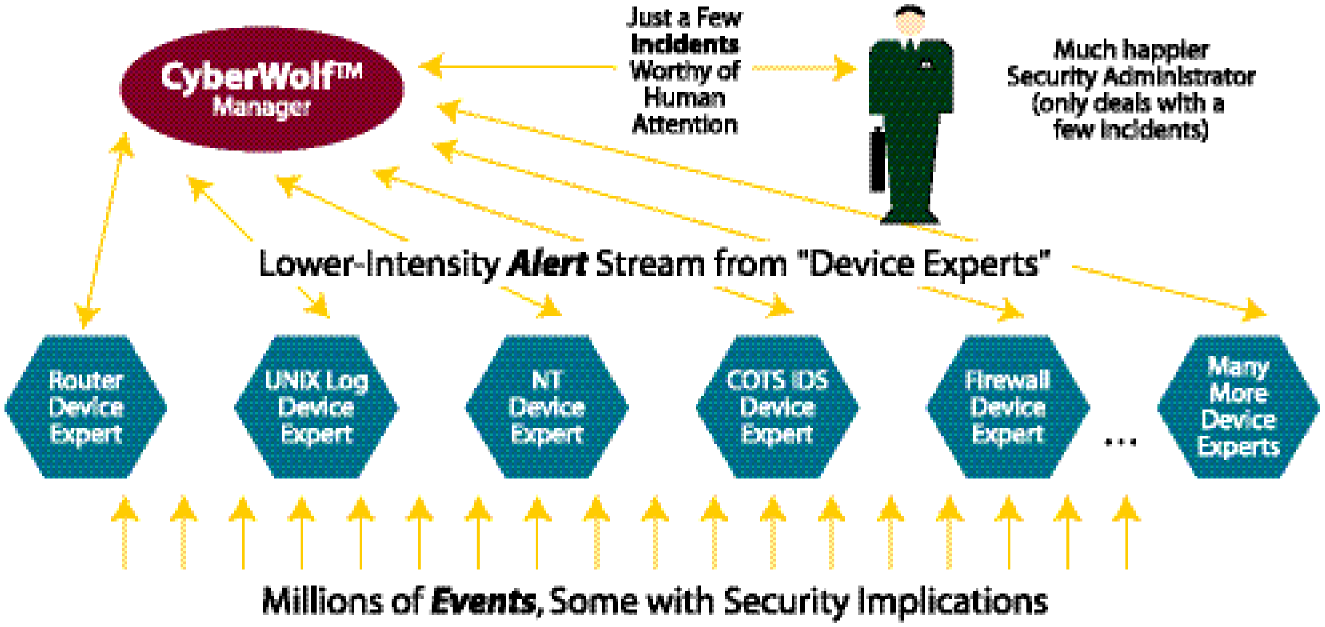
- 5+ Internet and Intranet firewalls
- 200+ routers
- 1 authentication server
- 100+ dial-up modem connections
- 3 IDS systems
- 15+UNIX and NT servers/workstations

During a resent IG audit, CyberWolf allowed the system security manager to track the attacks being conducted by a professional commercial red team. IG Auditors have labeled FEMA perimeter defenses as 'Strong'.

CyberWolf is being tested and refined to correlate network management and intrusion detection data – In this capacity, CyberWolf aims to reduce false positives generated by IDS. Both IDS and Network Management information streams are fed into the CyberWolf system. CyberWolf correlates the streams of information to—

- Identify malfunctioning hardware from network management information to negate the false positive generated in the IDS system in response to the hardware failure
- Identify unauthorized changes using network management information streams and correlate it with relevant information from the IDS streams of information
- Identify changes in the network maps as indicated by the network management information streams and correlate this information with those streams from the IDS systems
- Activate responses to attacks using the network management elements that CyberWolf is tied into
- Provide asset optimization information based upon the data collected
- This could enable improved routing of traffic, best case re-routing when under attacks and also improved use of assets

United States Navy, in a SPAWAR/NAVSEA/USJFCOM Content-based Information Security (CBIS) Advanced Con-


CyberWolf™ Manager
Just a Few Incidents Worthy of Human Attention
Much happier Security Administrator (only deals with a few incidents)
Lower-Intensity Alert Stream from "Device Experts"
Router Device Expert
UNIX Log Device Expert
NT Device Expert
COTS IDS Device Expert
Firewall Device Expert
...
Many More Device Experts
Millions of Events, Some with Security Implications

cept Technology Development (ACTD) program, is using CyberWolf to support security management of the future deployment multilevel security systems that will allow the Navy to reduce the number of LANs and workstations onboard ships. CyberWolf's role in this system is to protect the shipboard resources against unauthorized 'everything' using device experts and secure communications.

CyberWolf is being deployed as a secure-mode verification system to protect unsecured workstations. In this capacity, CyberWolf aims to—

- Identify when a workstation is reconfigured or its baseline configuration is changed
- Ensure the authenticity of the device experts themselves
- Identify when a change in the application baseline occurs
- Identify when an incorrect encryption algorithm is used and when verification techniques are bypassed by the operator
- Support multiple configurations on different workstations and migrating security configurations

Operationally Proven Advantages

CyberWolf is already being used in the field to augment various Government information assurance implementations.

- The use of rule-bases and knowledge-bases to capture the day-to-day analysis activities of a security administrator. Knowledge is captured in-house and stays within the organization when the security analyst leaves.
- The use of high-speed intelligent device experts instead of database triggers and replication, ensuring scalability and robustness.
- The device experts collect significant security events by accepting incoming events/alarms from heterogeneous sources and document in detail, using easy-to-read rules, the process and configurations of the security components that transfer information through the system. Any changes in the process only requires updates to rules as opposed to major rewrite of software components or changes to the database structure or triggers.
- Device experts, along with authentication capability, enables the collection of critical/classified events and alarms that need to be protected and forwarded to DOD CERT or an External CERT, ensuring that the critical/classified information is handled appropriately and that the source is authenticated.
- Incident Lists and Incident Tickets provide a user interface capability to present users with current summary information. All information relevant to an incident is gathered and interpreted in one display window. Other information such as conclusions and user actions are also carried in the incident ticket.
- Easy-configuration of reports and the ability to change them in real-time by using simple rules. The user is able to control the generation of conclusions for notifying managers of strategic attack indications, the automated integration of databases (i.e., AFCERT, NAVCIRT, etc.), and the automated generation of incident tickets.

The knowledge required to effectively reason about the security stance of an enterprise is substantial. Although CyberWolf does have its own standard set of device experts, it relies on components within the security infrastructure for its data sources. Following is a sample list, of sources of information that CyberWolf can reason about.

- Firewalls–Raptor/Axent, Gauntlet/Network Associates, PIX/CISCO, Socsk/LINUX, Firewall-1/CheckPoint
- Routers–CISCO, Ascend
- Systems–LINUX, Solaris, NT
- Intrusion Detection Systems –CISCO NetRanger, ISS RealSecure, NetRadar, SNORT
- Authentication Servers–TACACS
- Network Management–HP OpenView

CyberWolf also understands the role that a critical system plays within an organization. Therefore knowledge about the following types of servers is also included with the system.

- Web servers–IIS/MicroSoft, Apache
- ftp servers–SOLARIS
- DNS servers–SOLARIS

For addional information, E-mail Jim Litchko at jim@litchko.com, call 703.538.1919 or visit our Web Site www.mountainwave.com/cyberwolf.

ATM Intrusion Detection Systems continued

continued from page 11

streams architecture for the OC-3 IDSs.

The multiprocessing capabilities have not fully been exploited in the currently fielded IDSs. Additional effort needs to be expended to optimize the SMP architecture. One area that could benefit greatly from further SMP refinement is the area of near real-time processes. A goal of the HPCMP is to implement a near real-time IDS capability; to achieve this further optimization of the SMP architecture will be critical.

Finally, currency with the most recent JIDS release is critical to support issues. During the development of the ATM IDS, enhancements were made to the standard JIDS code. The ATM IDS code must merge with the standard version and remain current in the JIDS update process to be fully supported.

Mr. Joseph Molnar is an Information System Security Officer for the High Performance Computing Modernization Program. He earned his B.A. from Washington & Jefferson College in 1981 and his M. S. from The Pennsylvania State University. Both degrees were in physics. He may be reached at molnar@ hpcmo.hpc.mil.

continued from page 22

were no changes to the TFM, SFUG, or any of the other documentation, there is no need to look at them again.

It is also a good idea to conduct on-site interviews to ensure that the security training and awareness program works, to conduct scans of the system, and to take another look at the minimum security checklist. The team will probably want to conduct spot checks of previously tested procedures on a random basis as well.

Conclusion

By now you can see that the C&A process, which may initially seem complex, has an underlying logic. It's not all smoke and mirrors—indeed, the flexibility built in to this process helps to ensure its success. Modern-day networks are inherently heterogenous, complex and ever changing[7] and even after a system has been certified it is still necessary to maintain that level of security. The virtual and physical assets involved normally contain sensitive information, and if shared, create great national security risks. If the DAA, PM, user representative, ISSO, and system administrators all do their jobs, then reaccreditation after three years will be much easier, and the system will also be more secure throughout its entire life-cycle. An agency must take an informed approach to security certification and accreditation to preserve the public trust in their ability to leverage information technology, while avoiding unintended consequences.

For more information on Certification and Accrediation, visit one of these Web sites—

- https://www.isec-sig.army.mil/isectech/teal/tealframe.cfm?skill=secucert&foldername=IE
- http://www.isec-tech.hqisec.army.mil/isectech/index.htm
- https://iase.disa.mil/ditscap.html
- http://www.p-and-e.com/documents/DITSCAP.pdf

Mr. John Kimbell has worked in the computer industry for over 30 years in a wide variety of positions, including the engineering of and modification to secure digital message switching centers, local and wide area networks, and a variety of secure communications systems. He has certified and assisted in the certification of numerous DoD and Army systems, and is presently the Critical Skills Expert in security certification for the United States Army Information Systems Engineering Command (USAISEC) at Fort Huachuca, Arizona. Mr. Kimbell holds a B.S. degree in Computer Science from Chapman University, and a M.S. in Information Systems Engineering from Western International University. He may be reached at kimbellj@HQISEC. Army.mil.

Ms. Marjorie Walrath is a technical editor assigned to USAISEC, Fort Huachuca, Arizona. She is currently at work on a bachelor's degree in communications.

Endnotes

1. Kuzniar, Paul, *Government from the View of Business*, Government Executive, April 2000, p. 97
2. U.S. Department of Agriculture *Inspection and Grading* [on line], http://www.fsis.usda.gov/oa/pubs/ingrade.htm August 1998
3. DoD 5200.28 Standard,Department of Defense Trusted Computer System Evaluation Criteria, December,1985
4. Army Publication & Printing Command, Information Systems Security AR 380-19, sec.2.3, March 1998, http://books.usapa.belvoir.army.mil/cgi-bin/bookmgr/BOOKS/R380_19
5. DoD Application Manual 8510.1-M
6. AR 380-19, ch.3 sec. 3.10
7. Casti, John l. *Would-be Worlds: How Simulation is Changing the Frontiers of Science*, John Wiley & Sons, Inc., 1997, p.x

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

O June 2000

Critical Review and Technology Assessment (CR/TA) Reports

O Biometrics O Computer Forensics* O Defense in Depth O Data Mining

O IA Metrics O Modeling & Simulation* O **Configuration Management—NEW!**

IA Tools Report

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

State-of-the-Art Reports (SOARs)

O Data Embedding for IA O IO/IA Visualization Technologies O **Modeling & Simulation for IA—NEW!**

O Malicious Code Detection* [o TOP SECRET o SECRET] ______________________________

Security POC ______________________________ Security Phone

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

UNLIMITED DISTRIBUTION

Newsletters *(Limited number of back issues available)*

o Vol. 1, No. 1 o Vol. 1, No. 2 o Vol. 1, No. 3

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

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

o Vol. 4, No. 1 o Vol. 4, No. 2

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

May 21–25

DoD-Wide 2nd Annual Computer Crime Workshop
Colorado Springs, CO
www.technologyforums.com

22–25

2001 USPACOM Information Assurance Conference
Ilikai Hotel, Waikiki
Honolulu, HI
www.iaevents.com/Pacom/Pacom.html
COME VISIT OUR EXHIBIT

June 4–8

Action Officer Computer Network Operations (CNO) Requirements Conference
Colorado Springs, CO
To bring together IA/CND/CNO SOs from the CINCs, DoD and other Governement Agencies that develop CND/CNA requirements.
POCs: Mr. Mack Sharp, malcolm.sharp@cheyennemountain.af.mil
Mrs. Janet Ross, janet.ross@cheyennemountain.af.mil

June 4–14

Information Operations Course
Camp Johsnon, Colchester, VT
A 10-day resident course focused on IO planning in support of Army tactical and operational commands. Register for this course through your training section.
POC: MAJ Dan Molind, 802.338.3224

June 14

IA Technical Framework Forum
Documenting User Requirements
NIST, Gaithersburg, MD
niemczuk_john@bah.com

June 11–15

National Operations Security Conference & Exposition
Westin Innisbrook Resort
Tampa, FL
www.ioss.gov/html/opsec_conferences/national2001/overview.html

July 9–20

Joint Information Warfare Staff and Operations Course (JIWSOC)
Joint Forces Staff College
Norfolk, VA
Designed for individuals assigned or enroute to an IO cell on a Unified Command or JTF Staff.
www.jfsc.ndu.edu/jciws/jciws.htm/iw.htm

July 10–11

Intelligence Support to Force Protection Conference
US Southern Command
Miami, FL
POC CPT Jones, 305.437.2140

July 23–27

Joint Warrior Interoperability Demonstration 2001 (JWID 01)
Joint C4ISR Battle Center,
Suffolk, VA
A Joint Staff-sponsored event where Government and private industry join forces to demonstrate new and emerging technologies that will shape the battlespace of the future.
www.jwid.js.mil

IATAC

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