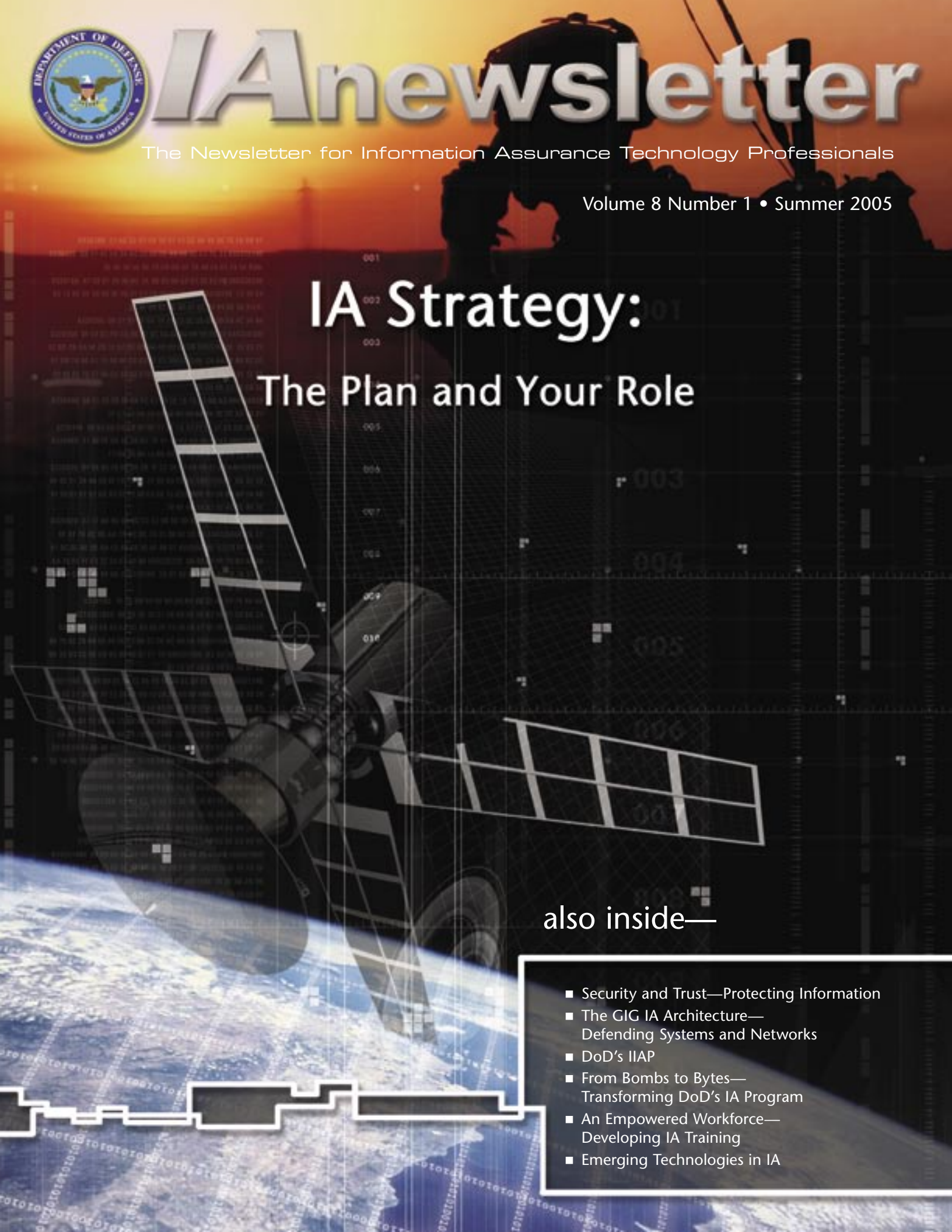


IAnewsletter

The Newsletter for Information Assurance Technology Professionals

Volume 8 Number 1 • Summer 2005

IA Strategy:

The Plan and Your Role

also inside—

- Security and Trust—Protecting Information
- The GIG IA Architecture—Defending Systems and Networks
- DoD's IIAP
- From Bombs to Bytes—Transforming DoD's IA Program
- An Empowered Workforce—Developing IA Training
- Emerging Technologies in IA

contents

feature

IA initiatives

in every issue

About IATAC & the *IAnewsletter*—

IAnewsletter is published quarterly by the Information Assurance Technology Analysis Center (IATAC). IATAC is a Department of Defense (DoD) sponsored Information Analysis Center, administratively managed by the Defense Technical Information Center (DTIC), Director, Defense Research and Engineering (DDR&E).

Contents of the *IAnewsletter* are not necessarily the official views of or endorsed by the U.S. Government, DoD, or DDR&E. The mention of commercial products and/or services does not imply endorsement by the DoD or DDR&E.

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

IATAC Director: Gene Tyler
Deputy Director: Greg McClellan

IAnewsletter Staff—

Creative Directors: Christina P. McNemar, Ahnie Senft
Art Director: Bryn Farrar
Designers: Dustin Hurt, Holly Shipley
Copy Editor: Diane Ivone
Editorial Board: Greg McClellan, Jim Peña, Ron Ritchey, Tara Shea, Gene Tyler

IAnewsletter Article Submissions

To submit your articles, notices, programs, or ideas for future issues, please visit http://iac.dtic.mil/iatac/IA_newsletter.html and download an "Article Instructions" packet.

IAnewsletter Address Changes/Additions/Deletions

To change, add, or delete your mailing or E-mail address (soft-copy receipt), please contact us at—

IATAC
Attn: Peggy O'Connor
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

Deadlines for future issues—
Fall 2005 June 2, 2005

Cover design: Ricardo Real
Newsletter design: Ahnie Senft

Distribution Statement A:

Approved for public release; distribution is unlimited.

IATAC Chat

Gene Tyler, IATAC Director

This edition of the IAnewsletter is dedicated to one topic—the Department of Defense (DoD) Information Assurance (IA) Strategy. The DoD IA Strategy was developed under the Leadership of Mr. Bob Lentz, Director of the Information Assurance Directorate, Office of the Assistant Secretary of Defense – Networks and Information Integration (ASD–NII).

The strategy is the result of a community effort lead by ASD–NII and the Defense-Wide Information Assurance Program (DIAP), and worked in conjunction with senior IA leadership from the Services, Joint Staff, U.S. Strategic Command (USSTRATCOM), Defense Information Systems Agency (DISA), and National Security Agency (NSA)—a true collaborative effort.

The importance of the Strategy to the DoD IA community has been significant, and the process to develop and inculcate it into daily IA activities is an ongoing effort. The development of the Strategy took over a year and it was presented to and approved by a number of senior bodies: the Military Communications–Electronics Board in August 2002, the CIO Executive Council in December 2002, and then formal presentation to the IA Community in February 2003 at the 7th Annual DoD IA Workshop.

The heart of the Strategy is the five goals: Goal 1: Protect Information; Goal 2: Defend Systems and Networks; Goal 3: Provide Integrated IA Situational Awareness/IA Command and Control; Goal 4: Transform and Enable IA Capabilities; and, Goal 5: Create an IA Empowered Workforce. Each Goal has an OSD level senior leader overseeing the progress of the Goal, acting as an advocate for resourcing, and generally shepherding any aspect of the Goal. Mr. Lentz oversees the Strategy process and interfaces with senior DoD leadership: Goal point of contacts are:

- **Goal 1**—Mr. Gary Windham (DIAP)
  gary.windham@osd.mil
- **Goal 2**—Mr. John Hunter (DIAP)
  john.hunter@osd.mil
- **Goal 3**—Mr. Tim Bloechl (OSD ASD–NII)
  tim.bloechl@osd.mil
- **Goal 4**—Ms. Vivian Cocca (OSD ASD–NII)
  vivian.cocca@osd.mil
- **Goal 5**—Mr. George Bieber (DIAP)
  george.bieber@osd.mil

Goals 1 and 4 have four strategic objectives and the other three Goals each have five strategic objectives to assist in defining the scope of the Goal. There are a number of key initiatives, milestones, and tasks that complete the strategic process. Leaders in ASD–NII and the DIAP believe the Strategy is on target as the Goals and strategic objectives have stayed constant over the past three years.

To "operationalize" the IA Strategy, that is to make it useful for the Department, and to keep it current, vigorous efforts are underway to make the IA Strategy a "living and breathing" document. The key initiatives, milestones and tasks are constantly evolving to stay aligned with DoD Transformational efforts. It is through this process that the Strategy Team ensures the IA Strategy continues to evolve to meet DoD needs.

Some recent successes at "operationalizing" the Strategy and ensuring it is current, can be seen in the alignment of resources through Program Objective Memorandum (POM) and other budget actions. In addition, the last two DoD IA Workshops used the IA Strategy as a format for logically presenting information to the attendees. The Strategy is valuable to the IA process. Please read on and contact the IA Goal Leads if you want to know more. ■

by Gail Tryon, CISSP

The long-term vision of the U.S. Department of Defense (DoD) Information Assurance (IA) Strategy is to achieve dynamic IA for the Global Information Grid (GIG) through systematic transformation of our operations, technologies, processes, and people. The principal objective of the Strategy is to get the right information to the right person at the right time at the right place.

This article focuses on Goal 1 of the Strategy. The objective of Goal 1 is to safeguard data (as information) as it is being created, used, modified, stored, moved, and destroyed at the client level, within the computing environment, within the enclave, at the enclave boundary, and across the networks. It also ensures that all information has a level of trust commensurate with mission needs.

Goal 1 efforts are divided into four Strategic Objectives:

- Developing and promulgating the IA Component of the GIG Architecture
- Developing protection criteria for Network-Centric Operations [*e.g.*, Internet Protocol Version 6 (IPv6), DoD Policy, National Security Agency (NSA) Advisories, Data Strategy, Metadata Protection]
- Developing and deploying protection capabilities across the enterprise [*e.g.*, GIG Bandwidth Expansion (GIG-BE), Crypto Modernization, High-Speed Encryptors, Cross-Domain Solutions, Secure Wireless Solutions]
- Transforming the Security Management Infrastructure (SMI) [*e.g.*, Identity Management, Public Key Infrastructure (PKI), Public Key Enabling (PKE), Key Management Infrastructure (KMI), Modernization, Biometrics]

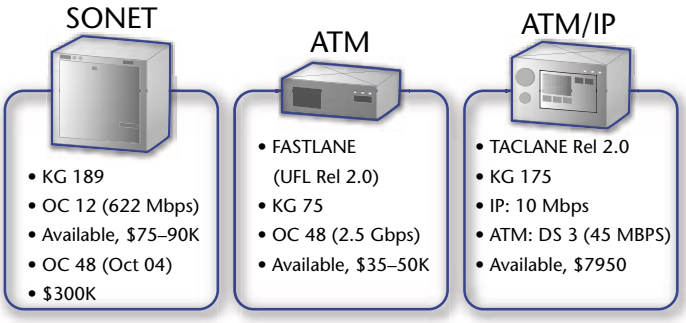
Two key points in this effort are different from the traditional approach of simply encrypting information while it is in transit. The first is that information must be protected from end to end. The second is that the level of trust in the information must be commensurate with mission needs. The four Goal 1 Strategic Objectives focus on near-term and long-term efforts to achieve end-to-end protection commensurate with these needs.

Our first Strategic Objective is developing and promulgating the IA Component of the GIG Architecture, which is also referred to as the IA Architecture. There is service and agency agreement on the first increment. The IA Architecture is being incorporated into the Net-Centric Operational Warfare (NCOW) Reference Model and IA Tactical Framework. The IA requirements that are imbedded in DoD's Joint Vision 2020 and other documents are being documented in the IA Initial Capabilities Document (ICD) to support the Joint Capability Integration and Development System (JCIDS) process. This approach is being used to improve IA in joint and coalition operations.

The second Strategic Objective, developing protection criteria for Network-Centric Operations, focuses on the policies and standards needed to protect information. Recent DoD instructions and policies in this area are shown in Table 1.

Table 1: Recent Goal 1 related policies

DoD Directive/ Instruction	Number	Title
DoDD	8500.1	Information Assurance (IA)
DoDI	8500.2	Information Assurance (IA) Implementation
DoDI	8520.2	Public Key Infrastructure (PKI) and Public Key Enabling (PKE)
DoDI	8320.2	Data Sharing in a Net-Centric Department of Defense
DoDI	8100.2	Use of Commercial Wireless Devises, Services, and Technologies in the DoD GIG



High Assurance IP Encryptor (HAIPE)

Contractor Funded Development (CCEP)

L3 Communications	**ViaSat**	**General Dynamics** Decision Systems	**General Dynamics** C4 Systems
• Red Eagle INE–100 • KG 240 • 100 Mbps • HAIPIS Compliant • Available $10,500	• AltaSes • KG 250 • 100 Mbps • HAIPIS • Available $9900	• Sectera Rel 3.1 • KG 235 • 20 Mbps • HAIPIS Compliant • Available $10,950	• E-100, Rel 2.1E • 100 Mbps • Available $10,950

NSA Co-Funded Developments

L3 Communications	**General Dynamics** Decision Systems	**ViaSat**
• GX1, 1.0 Gbps, KG 245 Dec 04* • GX10, 10 Gbps Apr 05*	• KG-175A • TL-GigE • 1.0 Gbps • Available	• KG-255 • AltaSec 1000 • 1.0 Gbps Jun 05*

Figure 1: Network encryptor product family

The third Strategic Objective of Developing and Deploying Protection Capabilities Across the Enterprise includes protection of data in transit, one of our strongest and most mature protection techniques (see Figure 1). We have been focusing on replacing legacy encryptors with more secure reprogrammable encryptors. The revolution in wireless computing, networks, handheld computers, and higher-speed Gigabyte optical networks is providing "power to the edge" along with the need for "protection to the edge" (see Figure 2 below). This is a challenging area, but we are making progress. We are developing High Assurance Internet Protocol Encryptors (HAIPE). The first HAIPE Encryptors have been delivered and installed as part of the GIG-BE program. New encrypted cell phones and Secure Terminal Equipment (STE) devices using Future Narrow Bandwidth Data Transfer (FNBDT) have been developed and are in use by our troops. Advanced waveforms for increased security are being developed and delivered to support the Joint Tactical Radio System (JTRS) program. Fifteen commercial products to protect sensitive but unclassified data have been successfully tested and certified by Common Criteria. These products can be purchased to help protect data at rest on our mobile devices, such as laptops and Personal Digital Assistants (PDAs). E-mail across the DoD has been PK Enabled, allowing e-mail to be sent and stored encrypted, as needed. Also included in our protec-

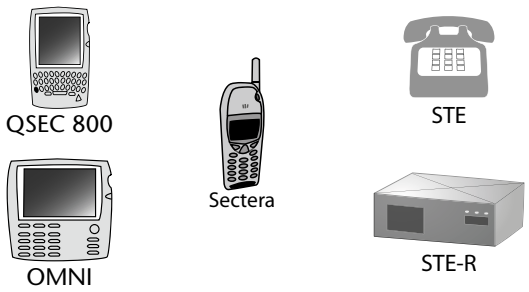


Figure 2: Wired and wireless products

continued on page 8…

The GIG IA Architecture—

Defending Systems and Networks

Goal 2

Defend Systems and Networks by recognizing, reacting to, and responding to threats, vulnerabilities, and deficiencies, ensuring that no access is uncontrolled and all systems and networks are capable of self-defense...

—from the DoD IA Strategic Plan Framework
Dynamic Information Assurance for the Global Information Grid (GIG)

by John Hunter and Rick Aldrich

The approach established for realizing Goal 2 of the IA Strategic Plan comprises five Strategic Objectives, each of which are discussed below.

"Establish the Global Information Grid (GIG) Network Defense architecture and to-be baseline roadmap to respond to known and advanced threats."

Because the GIG is so large and constantly changing, establishing an "as-is" Computer Network Defense (CND) architecture is challenging. A somewhat more manageable task is to determine a "notional" CND architecture. Such a notional architecture would depict things as they should be if all policies, directives, instructions, and other controlling regulatory guidance were followed. The "to-be" architecture has been established in the IA component of the GIG Architecture. The GIG IA Architecture posits incremental "to-be" positions for 2008, 2012, 2016, and 2020. However, to move from DoD's current position to the "to-be" positions requires knowing not only what policy changes will be required (from the notional architecture) but what implementation changes will be necessary. Various mapping tools, combined with the results of DoD's annual CND Assessment and the Enterprise Sensor Grid/User-Defined Operational Picture (ESG/UDOP) survey, are currently being considered for use in assessing this gap analysis.

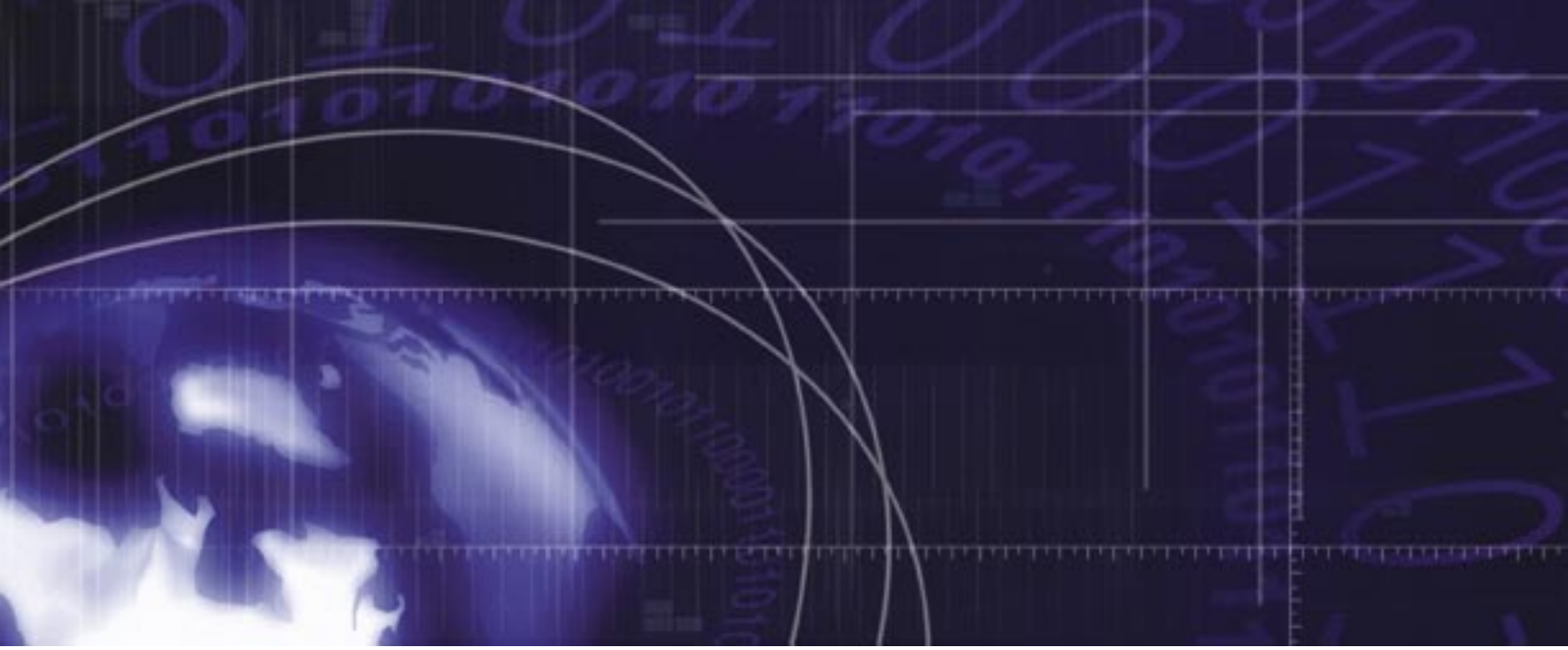
With the establishment of DoD's Enterprise-Wide Solution Steering Group (ESSG), DoD has made a major stride in more centrally managing the defense of DoD's systems and networks. The ESSG is chaired by the U.S. Strategic Command (USSTRATCOM), and the voting members of the body include representatives from each Service, USSTRATCOM, the Joint Forces Command (JFCOM), the Defense Information Systems Agency (DISA), the National Security Agency (NSA), and the Defense-Wide Information Assurance Program (DIAP). The ESSG, working closely with its Technical Advisory Group (TAG) and Acquisitions Working Group (AWG), has already facilitated the prompt selection, acquisition, and deployment of enterprise-wide licenses for a vulnerability-scanning tool and a vulnerability-remediation tool. In the near future, ongoing efforts should result in the selection of enterprise-wide tools to help combat spyware, the insider threat, and several other problem areas. Efforts in the near term will also support implementing an enterprise-wide Situational Awareness capability, developing the enterprise sensor grid, implementing Demilitarized Zones (DMZ's), providing for the hardening of secure networks within DoD, and continued implementation of the ports and protocols management process.

"Develop and enforce CND policies across the enterprise to achieve an optimal readiness posture against the outsider "nation state" attacker as well as the threat posed by the insider."

DoD has been especially active in developing CND policies to help lay the foundation for improving DoD's CND posture. Just within the past year, DoD has published the following documents in Table 1.

Table 1: Recent DoD policy issuances related to CND

DoD Directive/ Instruction	Number	Title
DoDD	8100.2	Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG)
DoDI	8520.2	Public Key Infrastructure (PKI) and Public Key (PK) Enabling
DoDD	8570.1	Information Assurance Training, Certification, and Workforce Management
DoDI	8580.1	Information Assurance (IA) in the Defense Acquisition System



DoD Directive/ Instruction	Number	Title
CJCSI	6510.01D	IA and CND
DoDI	8551.1	Ports, Protocols, and Services Management
ASD–NII	Policy Memo	Elimination of Unauthorized Peer-to-Peer (P2P) File-Sharing Applications Across DoD
CDRUSSTRATCOM & ASD–NII	Memo	CND Strategy for DiD

Through the annual CND Assessment, DoD has also tracked compliance with key CND policies by each component in DoD. Red Teams, Blue Teams, Green Teams, and White Teams further help units to identify key vulnerabilities and weaknesses in their CND architecture and implementation. Pursuant to Congressional direction, the Director, Operations Testing and Evaluation (DOT&E), has been participating in component exercises to better assess the CND posture under exercise conditions. Currently, DoD is attempting to join and cross-correlate the results of these diverse surveys, assessments, and tests to produce better metrics by which to assess the progress of DoD and its constituent components in defending their systems and networks.

"Evaluate and deploy CND tools and capabilities in a coordinated manner to achieve required operational capability."

DoD has recently been quite successful with respect to this objective, having tested and acquired an enterprise-wide vulnerability-scanning tool and an enterprise-wide vulnerability-remediation tool. This enterprise-wide acquisition follows in the footsteps of the successful deployment of an enterprise-wide suite of anti-virus tools a few years ago. Both the vulnerability scanning and remediation tools are now being deployed across the enterprise. DoD has conducted pilot studies of an anomaly-detection tool, is working toward enterprise-wide acquisitions in several other key CND areas, and hopes to have several more tools deployed within the next year. In keeping with its Defense-in-Depth (DID) strategy, DoD is also working toward implementing Demilitarized Zones (DMZs) across the GIG to provide an additional layer of defense. Finally, significant strides are planned to improve CND on DoD's secure networks.

"Establish mechanisms and procedures within CND response-action guidelines that effectively utilize developed CND tools and capabilities to react and respond to events."

Over the past year, DoD conducted a tabletop wargame exercise, "Bulwark Extender," to test the CND Response Action (CNDRA) Concept of Operations (CONOPS). A smaller tabletop exercise was also conducted by legal and technical personnel from DoD and several Five Eyes partners. The results from both are being used to further refine DoD's CNDRA policy. Additional war-game exercises are planned for the near future.

"Mitigate the Insider Threat across DoD through the implementation of advanced tools, processes, and operational capabilities."

Pursuant to the Intelligence Authorization Act of 2004, DoD coordinated with the Intelligence Community (IC) to conduct a survey of its respective stakeholders to gather information on current practices, to analyze results, and to create a report for senior DoD leaders and Congress. This classified report will be delivered to Congress in the near future. DoD, through the ESSG, has also sought possible enterprise-wide solutions for the insider threat. The Counterintelligence Field Activity (CIFA), pursuant to Congressional direction and in coordination with the ASD–NII and DIAP, is also pursuing an implementation plan, including an acquisition and integration strategy, to identify promising tools to combat the insider threat.

continued on page 21…

…continued from page 5

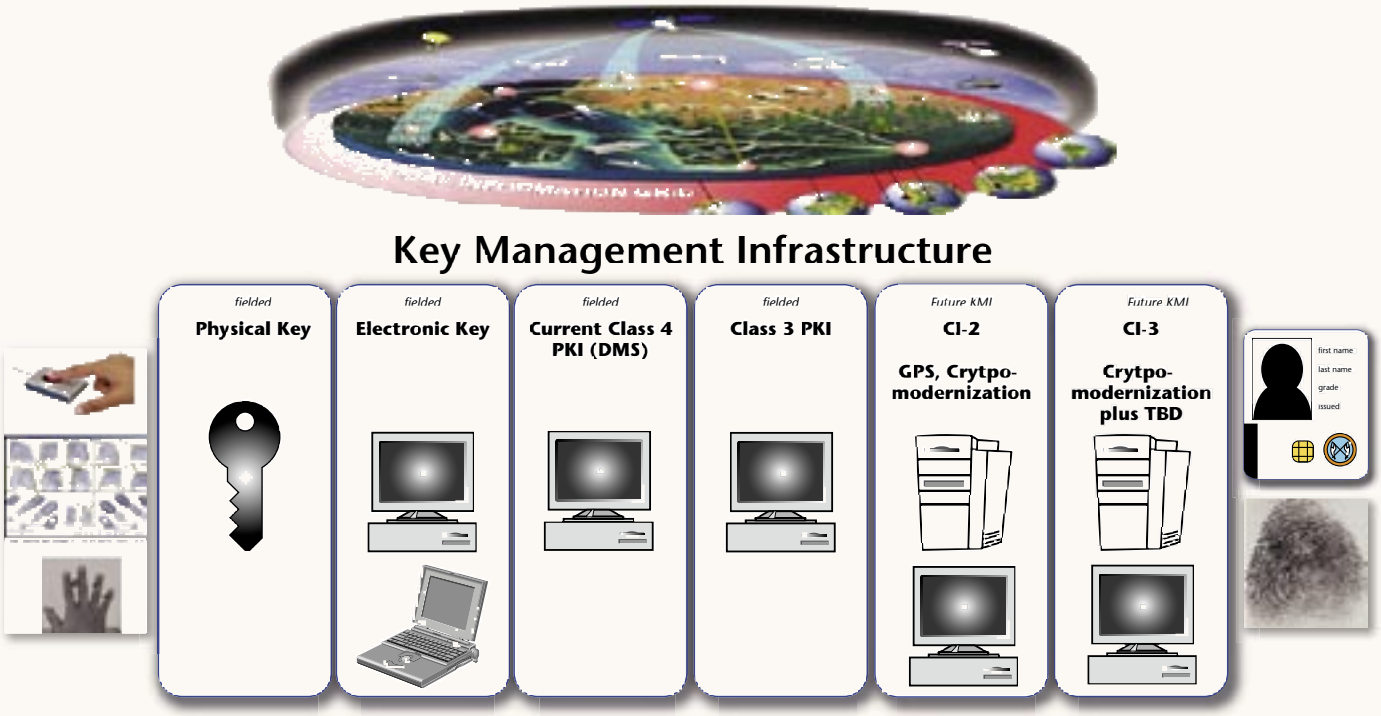


Figure 3: Transforming the Security Management Infrastructure (SMI)

tion capabilities are Cross Domain Solutions (CDS). With the need to share information with our Allies and Coalition Partners, CDS has become more important to assured sharing of information. Collaboration and Browsing (CAB) CDS are being developed along with advanced file-sharing CDS. We are transforming CDS from point-to-point solutions to net-centric solutions.

The fourth Strategic Objective to Transforming the SMI to support Net-Centric Operations includes not just traditional key management but also Identity Protection and Management. As we look at how our forces will be fighting in 10 to 20 years, we will need to respond to threats instantly. SMI must be able to support the dynamic nature of algorithm, key, and authorization changes that are part of the GIG vision. We must transform SMI while maintaining our current SMI capabilities, so that operations are not degraded.

Manual changing, verification, and use of keys will need to be automated and streamlined. We are transforming encryption key ordering and delivery from a manual process of delivering paper keys to faster electronic ordering and delivery (see Figure 3 above). Use of digital certificates with strong authentication must be a natural part of all systems. Identity Protection and Management has gained attention as identity theft has become a constant threat. DoD is investing in programs such as PKI, Biometrics, Common Access Control (CAC) Cards, and electronic key management to provide the tools and infrastructure for authenticating users and encryption. Enhanced certificate checking is now being deployed to allow authentication of identity within DoD. We have been working closely with agencies across the federal government to implement a standard identity for employees and contractors as directed by Homeland Security Presidential Directive–12 (HSPD–12), without compromising the level of trust we have that identities are not false or stolen. ■

About the Author

Gail Tryon

Gail Tryon served on active duty from May 15, 1976, through September 1, 1996, when she retired from the U.S. Navy with the rank of Commander. She has worked for BBN, Coopers and Lybarnd, and PricewaterhouseCoopers. She is currently a Managing Consultant and Certified IBM consultant at IBM in the Security and Privacy Practice. She has been supporting the DoD Information Assurance Program and the IA Strategy Goal 1: Protect Information since December 2002. She holds a BS from Edinboro University of Pennsylvania, and a MS from Central Michigan. She is a graduate of the Advanced Management Program at the Information Resources Management College at the National Defense University. She is certified as a Certified Information Systems Security Professional (CISSP), (ISC)2, Project Management Professional (PMP), PMI, and Certified Business Manager (CBM), APBM.

IATAC Spotlight on Research

The Pennsylvania State University

by Ronald Ritchey

This article is the second in a series that spotlights important activities in Information Assurance (IA) education and research and will describe the latest projects in some of the nation's best IA academic centers.

The National Centers of Academic Excellence in Information Assurance Education (CAEIAE) are ideal institutions in which to seek high-quality IA academic programs. CAEIAE is sponsored by the National Security Agency (NSA) and the U.S. Department of Homeland Security (DHS). As stated on the CAEIAE Web site, "the goal of the program is to reduce vulnerability in our national information infrastructure by promoting higher education in Information Assurance (IA) and producing a growing number of professionals with IA expertise in various disciplines."[1]

Nearly 60 colleges and universities are currently designated as Centers, having passed a rigorous screening process. Each school's IA courses must meet IA education standards set by the Committee on National Security Systems (CNSS). Also, each school's IA capabilities are scored against 10 criteria that include the number of full-time IA faculty members, the number of students in IA programs, and the amount of IA research performed by both faculty and students. [2] Students in the Centers' IA programs may apply for scholarships from the U.S. Department of Defense (DoD) Information Assurance Scholarship Program [3] (for DoD personnel only) or from the Federal Cyber Service Scholarship for Service (SFS) Program. [4] SFS allows students to receive funding for IA degrees in exchange for working for the Federal government for at least two years.

The CAEIAE program profiled in this article is the Center for Information Assurance (CICA), located at The Pennsylvania State University (PSU), University Park, PA. [5] Several colleges within PSU are part of CICA, including the School of Information Sciences and Technology (IST), the College of Communications, the College of Engineering, and the Smeal College of Business Administration. Dr. Chao-Hsien Chu and Dr. Peng Liu, both of IST, are the coordinators for CICA, which became a CAEIAE Center in 2003. According to Dr. Liu, PSU pursued the CAEIAE accreditation for two reasons: the need for more IA expertise for government and industry and the interest in IA expressed by students.

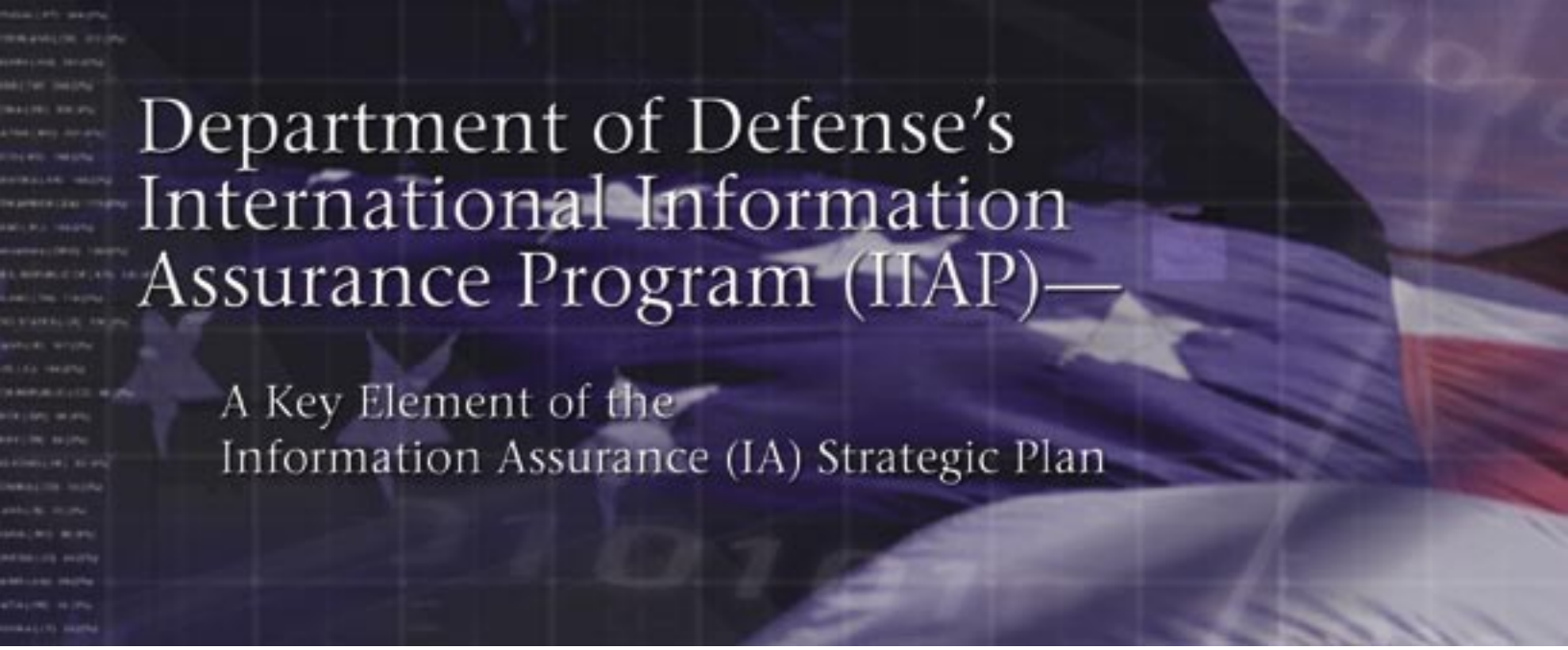
CICA offers several IA courses for B.S., M.S., and Ph.D. students and has over 20 faculty and staff members. Two of CICA's undergraduate students have already received DoD IA scholarships, and this year more students are applying to DoD and SFS for scholarships. CICA began offering an IA track for undergraduates in 2004, and the program has proven to be very popular. There are currently about 60 students pursuing this degree program.

Another important feature offered by a CAEIAE Center is the opportunity it affords faculty and students to conduct research in many different areas of IA. About 15 graduate-level research projects are currently under way within CICA. [6] Examples of topics addressed by these efforts include Internet security test-bed systems, cyber infrastructure security, self-healing databases, incentive-based attack prediction, and privacy-preserving computing.

Also of interest, CICA has developed a framework for proactive worm containment, which is intended to identify worms early in the infection process so that even worms that spread very quickly can be slowed more effectively. For worm detection, the framework favors speed over accuracy; when a worm-containment system identifies network activity as suspicious, it delays that activity for a few seconds. The primary goal for worm-containment systems is to stop worms from leaving an individual organization's networks and propagating across the Internet to other networks. ■

References

1. http://www.nsa.gov/ia/academia/caeiae.cfm
2. http://www.nsa.gov/ia/academia/caeCriteria.cfm?MenuID=10.1.1.2
3. http://www.defenselink.mil/nii/iasp/
4. http://www.nsf.gov/pubs/2005/nsf05507/nsf05507.pdf
5. http://net1.ist.psu.edu/cica/
6. http://ist.psu.edu/s2/



Department of Defense's International Information Assurance Program (IIAP)—

A Key Element of the Information Assurance (IA) Strategic Plan

by Timothy Bloechl and Jeffrey Wright

Defend the Global Information Grid. This monumental task itself provides ample reason to ensure the Department of Defense's (DoD's) Information Assurance (IA) program is linked to Allies and Coalition partners. Given the global, interconnected nature of the Global Information Grid (GIG) and the increasing interdependence of DoD on infrastructure owned and operated by the private sector, DoD clearly cannot proceed alone in daily network operations conducted by a globally postured and deployed force. Even more important for DoD's operational force is the continuing strategic and operational emphasis on coalition operations. As modern operations continue to emphasize coalition partnerships and interoperability, so too must network operators develop methods for continued close coordination with operational allies and Coalition Partners.

The increased need for international information sharing is complemented by increased reliance on common infrastructures. The trend towards globalization and interdependence among critical infrastructures (*e.g.*, finance, telecommunications, power), driven by information-age advances in computers, networks, and communications, suggests international cooperation is imperative if DoD is to be truly capable of protecting the GIG and mitigating systems' vulnerabilities. The international imperative is recognized in both the U.S. National Strategy to Secure Cyberspace and DoD's IA Strategic Plan. The Government and DoD are firmly committed to cooperating in cyberspace to provide greater protection to our networks and information systems:

> *"[The U.S. will] foster the establishment of national and international watch-and-warning networks to detect and prevent cyber attacks as they emerge."*
>
> **National Strategy to Secure Cyberspace**

DoD IA Strategic Plan

Vision: "Industry, Allies, and Coalition partners are integrated as appropriate in daily operations."

Goal 3—Provide integrated IA situational awareness/IA Command and Control (C2)

- Integrate relevant and timely Intelligence and Enterprise Sensor Grid data and analysis, and industry, law enforcement, interagency, international military, and worldwide Computer Emergency Response Team (CERT) information into the IA I&W process.
- Establish active relationships with other governmental, academic, civilian, international, and coalition agencies and organizations to provide critical data interchange.

Goal 4—Transform and enable IA capabilities

Enable efficient information sharing and collaboration across traditional boundaries:

- Identify and mitigate policy and regulatory impediments to efficient information sharing for Allies and Coalition partners.

International IA program objectives

Successful military operations in an increasingly complex global environment require regular and adaptive international cooperation. For the U.S. warfighter, international cooperation yields focused benefits through the execution of a standardized, department-wide International IA Program (IIAP). The benefits of IA/Computer Network Defense (CND) cooperation include the following—

- Improved information control and management
- Enhanced analysis and warning capabilities (*i.e.*, new sources, normalized reporting, more diverse reporting, greater depth of reporting)
- New, non-traditional insights, approaches, and solutions
- Enhanced situational awareness and understanding across the GIG

- Better integrated warning and improved reactions
- Increased U.S./Coalition protection and defenses
- Comprehensive and proactive defensive-mission collaboration
- Improved synergy, interoperability, and force synchronization

IIAP objectives guide DoD's international outreach and operational activities, within existing and future IA/CND cooperative relationships, to develop comprehensive, interoperable, and enhanced defensive capabilities, including the following:

- **Foster integrated Defense-In-Depth (DID) capabilities**—Robust defensive capabilities permit synchronization of comprehensive defenses; Tactics, Techniques, and Procedures (TTPs); Standard Operating Procedures (SOPs); day-to-day IA/CND operations; a shared, common operational IA/CND picture; and enhanced common guidance (policies, strategies, standards, and protocols, etc). In conjunction with transparent information sharing, these tasks serve to collectively enhance DoD and Allied/Coalition defensive capabilities and extend our defensive perimeters.
- **Foster development of enhanced technological capabilities**—A common understanding of technologies and applications, related technical approaches, and solution vectors will standardize and synchronize evolving technology solutions into military operational environments. Whenever feasible, this serves to optimize resource efforts and leverage existing capabilities and approaches.
- **Foster dynamic defenses**—Fielding adaptive and proactive defensive capabilities (*e.g.*, common network and Internet connections and intersections, automated tracking/monitoring tools and applications, and integrated and innovative analysis capabilities) enhances compatibility and interoperability.
- **Foster shared awareness and understanding**—Education equates to "raising the bar" of U.S. Government/DoD defensive understanding that adversaries must surmount. This includes sharing lessons learned; training initiatives; "best practices"; and innovative, conceptual, out-of-the-box thinking.

Information-sharing relationships

Establishing information-sharing relationships is at the core of the IIAP. To maximize resource investment and remain focused on support to critical operations, IIAP employs a hierarchical scheme to identify Allied and Coalition Partners in current operations, other Allied nations, and friendly countries with developing capabilities, as shown in Figure 1 (see next page). Graduated types of IA/CND cooperation generally correspond to the depth of interaction ranging from full-spectrum cooperation at the high end to awareness building at the low end. Stronger historical institutional relationships and the mature policies that result from them will generally allow for more robust information sharing at varying levels of classification.

Phased-relationship building

The IIAP process of building international IA/CND cooperation and operational relationships is divided into six distinct phases (see Figure 2 on page 13). These phases are intended to graphically demonstrate the general course of relationship building. These phases also provide a guide to validate existing and future IA/CND relationships, delineate organizational responsibilities by identifying a most likely DoD lead for each phase, and establish a planned structure for achieving the goals and objectives of the IIAP strategy.

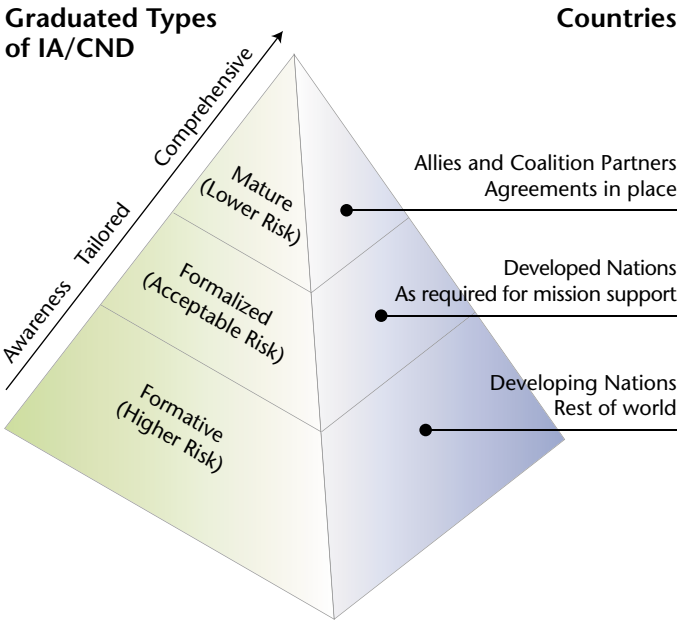


Figure 1. Relationship, risk, and cooperation levels

Phase 1—Initial contact

Initial contact can occur as a result of direction from the Office of the Secretary of Defense (OSD), at the request of a combatant commander, under the initiatives of another government agency (*e.g.*, Departments of State, Homeland Security, or Justice), or at the request of a foreign defense organization. Phase 1 ends when the parties agree to explore a more formal effort. As a policy initiative, the DoD lead will normally be the Office of the Assistant Secretary of Defense for Networks and Information Integration (OASD–NII), supported by the Joint Staff, the United States Strategic Command (USSTRATCOM), regional Combatant Commands (COCOMs), the Joint Task Force–Global Network Operations (JTF–GNO) and/or in-theater IA/CND organizations.

Phase 2—Relationship building

During Phase 2, exploratory talks are held to assess whether cooperation furthers DoD capabilities and objectives and enhances the DID of DoD and Coalition networks. Typical activities include working-group meetings, country visits, and exercises. The lead agency for Phase 2 will normally be OASD–NII, although this may be delegated to a regional COCOM. Phase 2 ends when both OASD–NII and the specified country representative make a policy decision to move forward to establish a formal relationship.

Phase 3—Formalize relationship

Phase 3 represents the transition to operations. To support more robust cooperation, DoD and its partner put in place the legal and policy framework necessary to govern the IA/CND relationship. A formal agreement such as a Memorandum of Understanding/Agreement (MOU/MOA) and a supporting Standard Operating Procedure (SOP) are developed and approved to govern information sharing, cooperation, and operational activities. Disclosure policies and authorities must also be established to authorize the sharing of information with the partner country. OASD–NII normally leads this Phase through the conclusion of a formal MOU/MOA, with regional COCOM support through the formulation of objectives and operational parameters. The regional COCOM assumes the lead role at the conclusion of an IA/CND MOU/MOA. Phase 3 ends when the required agreement is in place to enable day-to-day cooperation.

Phase 4—Operationalize relationship

During this phase, the DoD and its partner country begin day-to-day IA/CND information sharing, cooperation, and operational activities. Normally, this occurs at the regional operational level between the designated COCOM lead and the IA/CND organizations, in conjunction with Allied counterparts. For specific multilateral groups that cross Areas of Responsibility (AORs) or strategic, bilateral relationships designated by OASD–NII, USSTRATCOM and JTF–GNO serve as the main operational interfaces. The SOPs developed in Phase 3 are refined and established to govern operational interaction. Phase 4 ends when DoD and the partner country agree to expand cooperation beyond CND operations to full-spectrum IA activities.

Phase 5—Expansion

In Phase 5, the relationship deepens and expands cooperation beyond day-to-day operations to investigate the creation of common standards, training, policy, and procedures; establishes best practices; and leverages each partner's training and technical capabilities. The DoD lead agency generally remains a regional COCOM with OASD–NII, the Joint Staff, and other DoD agencies or organizations providing support based on specific details of the engagement.

Training and exercise initiatives under IIAP

Building relationships includes support to a participating nation's training and exercise requirements. Throughout the six phases of the IIAP plan, training and exercises provide important venues for cooperation.

Organizational responsibilities

For a Department-wide program such as IIAP to successfully achieve its objectives, a team effort is required from strategic to tactical levels. Key organizations include OASD–NII, Joint Staff/J–6, USSTRATCOM, regional COCOMs, JTF–GNO, and CND Service Providers from both the Services and the Defense Information Systems Agency (DISA). As the program matures, broader participation is anticipated, including guidance from the Director, Operational Test & Evaluation (DOT&E), acquisition staffs, institutional training organizations, and functional COCOMs.

OASD–NII maintains overall responsibility for the IIAP and provides policy oversight for international IA/CND efforts. OASD–NII chairs working groups to assess and facilitate U.S. international activities. Working-group activities will normally include periodic meetings leading to a U.S. decision on whether to operationalize a given cooperative relationship and to report progress to OASD–NII and other organizations, as appropriate.

Joint Staff/J–6 supports engagement and information sharing at the Department/Ministerial level, provides overarching IA/CND policy and doctrine to counterpart militaries, and seeks to expand IA/CND strategic international interaction.

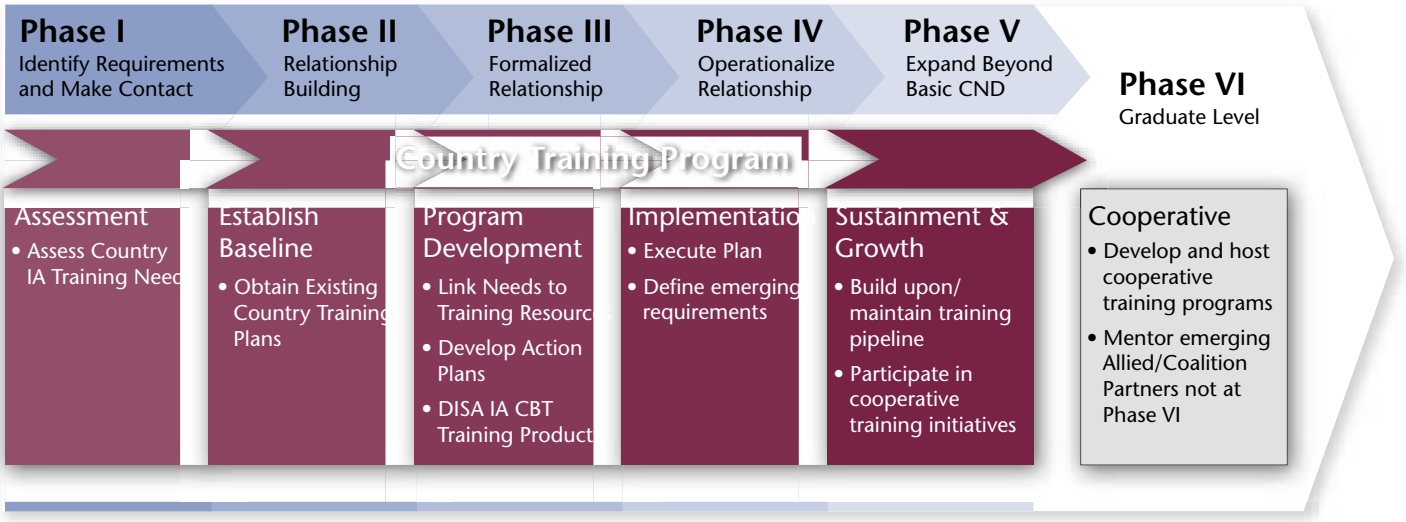


Figure 2. IIAP Relationship phases overview

As the military lead for CND under the Unified Command Plan, Commander, USSTRATCOM is responsible for operational oversight of military CND, advocating CND requirements, planning for CND operations, and establishing procedures for assigned components. USSTRATCOM also assists regional COCOMs in their respective CND efforts. USSTRATCOM plays a key supporting role, both directly and through JTF–GNO, to OASD–NII's engagement during Phases 1, 2, and 3. USSTRATCOM will typically provide oversight and guidance, as appropriate, for cooperative efforts in Phases 4 and 5.

JTF–GNO is the operational component of USSTRATCOM responsible for the CND mission. The command serves as the operational expert for CND as a primary component of its NetOps mission for tactics, techniques, procedures, planning, and technology. JTF–GNO plays a key support role in Phases 1, 2, and 3 and can assume the operational lead for designated relationships in Phase 4 and beyond, in some cases.

Regional COCOMs are responsible for integrating IA/CND into Theater Security Cooperation Plans (TSCP), executing IA/CND operations for coalition networks, and providing CND play in theater-level exercises. The COCOMs are critical participants who lead information sharing, cooperation, and operational activities in Phases 4, 5, and 6.

CND service providers, under the Heads of Service Components and DISA, conduct and coordinate operational activities with Allies and Coalition Partners in support of the DoD lead agency/command in each phase of IIAP. Regional and in-theater CND organizations may serve as operational interfaces with counterpart organizations in partner nations.

The evolution of DoD to a NetOps-enabled force requires a transformation of both the "how" and "who" of operations. While the operational force has embraced and begun to master coalition operations, the networked force is in its dynamic infancy. DoD's IIAP lays the foundation for the operational force to become a NetOps-enabled coalition force, bringing to culmination DoD's transformation of IA operations, technologies, processes, and people. ■

About the Author

Timothy Bloechl

Tim Bloechl is the Director, International IA Program for OASD–NII. A 1979 graduate of West Point, he is a retired U.S. Army military intelligence officer, a veteran of Operations JUST CAUSE, DESERT SHIELD, and DESERT STORM, and served with JTF–CND/CNO before joining the OSD staff.

Jeffrey Wright

Jeff Wright is the Director, Exercise Program for the National Cyber Security Division of DHS. Prior to joining DHS, Jeff supported the OSD International IA Program and led international CND efforts for JTF–CNO/GNO. A retired Field Artillery officer, Jeff was commissioned in 1982 from Davidson College, served in Operation URGENT FURY and also had tours in India and Pakistan as a Foreign Area Officer. He holds an MPA from Cornell University.

From Bombs to Bytes—

Transforming DoD's IA Program

by Vivian Cocca

Net-centric operations and warfare have changed the way the US Department of Defense (DoD) uses information. During the industrial age, military power came from mass. We would saturate targets with bombs delivered from squadrons of B–29s, each requiring a crew of 10 and associated ground support. These missions also consumed amassive amounts of ammunition and fuel. Now power comes from information, access, and speed. The US Air Force reports that a target that once took 1,000 bombs to destroy can now be destroyed by one bomb. What's the difference? It's the information content of that one bomb that makes the difference. Information replaces mass in the conduct of war, and this substitution is fundamentally changing how DoD trains, equips, and fights. Not only is this transforming how we fight, but it is also transforming how DoD provides for and assures that information.

The Global Information Grid (GIG) is our leaders' vision in realizing the effects a highly networked force has on operations. It provides the information, speed, and access that fuels our forces and delivers combat power. Our challenge now becomes how to ensure that soldiers, sailors, airmen, and marines can trust the information that is supplied to them through their sensors and networks, as well as the information used by weapons systems to create battlefield effects. This idea of trust in information is what Information Assurance (IA) is all about. It is the DoD IA community's challenge to transform how we secure that trust and this, in turn, requires changes in culture, values, and methods of operation.

The DoD IA Strategic Plan provides the roadmap to guide the way in which we employ IA for DoD. It outlines five core competencies or "strategic goals" that will enable us to deliver trusted information to the warfighter. It is the fourth goal, "Transform and Enable IA Capabilities," that serves as the driver for required changes within the IA community. It seeks to provide a culture that embraces new ideas, cultivates innovative thinking, and encourages collaboration. Senior leaders in the DoD IA community recognize the need to take a more active role in setting a new path for IA in terms of policy, operations, and capabilities, and they envision using this goal as a mechanism for change. The goal comprises four different approaches to affect culture change:

1. Reaching out to other communities and influencing departmental processes
2. Enhancing leadership, decision making, and management
3. Encouraging innovation
4. Sharing information and collaboration

A word on "culture change"

The information environment is complex and constantly changing. The average life cycle of technology is 12–18 months, which is shorter than the average DoD policy life cycle. Moreover, our adversaries are much more agile and adaptive; we struggle to devise ways to outthink and outmaneuver them, especially in the information domain. As a community, we are just beginning to understand how we need to change our culture to effectively address this reality. We talk about changing from "risk aversion" to "risk management," yet commonly used and available technologies are barred from use within DoD because of the "unknown" risk to security factors. This illustrates an old paradigm that does not enable the DoD IA Community to quickly adapt to customer needs. The customer is not asking if they can use the technology; they are asking, "What is the risk to my operation when I use this technology?" and "What can I do—or what can you do—to reduce my risk to an acceptable level?" This is a different way of thinking and operating for the IA community.

Instead of talking in terms of technological risk, we need to begin to think in terms of risk to mission. Permit the mission commander to decide if he or she wants to accept the risk that adopting a certain piece of technology will incur both locally and globally. As part of ensuring a "highly available" network, one of the major culture challenges we face is how to best understand and manage risk to operations and to missions. A major thrust for this coming year is to reach out to the warfighting community and find a way to communicate the value of the IA investment to their operations. This is a crucial first step in linking IA capabilities to mission

outcomes and to better understanding how to communicate risks in terms our customers understand. Secondly, in our own community, we need to create an improved information network. One that asks the right questions and provides the right data is a solid beginning. It is incumbent on senior DoD IA leadership to define and agree on the information they need to make those decisions. By instituting an enterprise IA metrics and reporting capability aligned with strategic and operational goals, we will begin to build an information base with which to empower a more informed and aware leadership that can effectively provide assurance to warfighters in a net-centric operating environment.

Influencing departmental processes

Because IA is pervasive, everyone in DoD and even outside DoD has a role to play. Transformation includes education and awareness facilitated by policies that target those processes that touch the most influential pieces of the GIG. Through active participation in key departmental processes; [*e.g.*, the Joint Capability Integration and Development System (JCIDS)]; Acquisition; and the Planning, Programming, Budgeting, and Execution System (PPBES), we are beginning to integrate IA into large programs throughout their development cycles. Using the IA acquisition policy (DoDI 8580.1, Information Assurance (IA) in the Defense Acquisition System), we are gaining insight into how IA is engineered into major acquisition systems and programs. This policy requires that program managers plan and build IA into their programs from inception to fielding. The Director, Operational Test and Evaluation (DOT&E) is improving the test and evaluation of IA by plugging IA events into associated exercises to gain critical insights into the effectiveness of the IA being built into these systems. This year, we are also seeking to build greater reserves and capabilities to ensure that Information System Security Engineers (ISSEs) are available for programs.

Leadership, governance, strategic management

Transforming how we lead, govern, and manage in a net-centric operating environment is a significant challenge for the upcoming year. Establishing the IA Domain Owner—the Office of the Secretary of Defense/Information Assurance (OSD/IA) Director—and the Domain Agent—the National Security Agency (NSA)—late last year was a crucial first step in developing a new construct for managing the provisioning of IA for DoD. Other crucial steps were defining the IA component of the GIG architecture and determining how to manage IA investments as a portfolio. As these concepts take shape, we expect to see improved performance in providing and delivering IA capabilities in response to emerging warfighting needs.

Streamlining, clarifying, and aligning strategic documents from organizations with enterprise responsibilities is also a priority for the coming year. The OSD, Joint Staff, and NSA are critical players in defining the road ahead for the Services and Combatant Commands. We must speak as one voice and be heard as one voice.

Innovation and outreach

Innovation is at the very heart of transformation and best describes how the IA Community should think about transformation. Innovation comes from everywhere, and we leverage "lessons learned" to share experiences. However, we typically look to industry, academia, and our own Research and Development (R&D) communities to discover answers to our toughest challenges. Last year, we initiated several "experiments" to build Communities of Interest (COIs) around these key groups. This year, we plan to continue these experiments to increase efforts on several key projects. Reaching out to the IA Centers of Excellence and providing them with research topics of interest to DoD is one area of focus. We also recently began work on implementing a "Commercial Innovation Integration" capability. This capability assists OSD and DoD in understanding the offerings of the commercial sector. To encourage technology partnerships, it also assists companies in locating the appropriate DoD customer earlier rather then later in the interaction process. At the IA Workshop, we began to organize the IA R&D community around the technology needs of the community. Workshop sessions focused on developing technology roadmaps for Secure Mobile Wireless and Assured Sharing.

These roadmaps will align and deconflict the activities of IA R&D communities with the anticipated effect of greater outcome linked to customer needs. Continued work during the past year with the Office of the Under Secretary of Defense (USD) Acquisition Technology and Logistics (AT&L) and with the office of the Director of Defense Research & Engineering (DDR&E) to create partnerships with the Venture Capital community has fostered several successes as well. This year, we plan to move into Phase II of this project, which will establish an office dedicated to developing and strengthening DoD to Venture Capital contacts and information exchanges (see Figure 1.)

Information sharing and collaboration

Innovation comes from sharing and collaborating on available data, information, and knowledge and provides the foundation from which we are able to transform ourselves. This is why making data and information available and visible to others in our community is paramount to the IA mission. Remember: "Innovation happens elsewhere." Whatever you're doing, and no matter how many smart people are on your team, there are always "more and smarter" people elsewhere.

Collaboration is also critical to innovation; it often acts as the catalyst for new ideas or approaches. At this year's Windows Hardware Engineering Conference, Microsoft chairman Bill Gates introduced an "innovative" new PC design, co-developed by Microsoft and Hewlett-Packard. The new PC, code name "Athens," features a wide-screen, flat-panel display, high-quality audio, "intuitive and consistent" controls, "truly quiet" operation, and "appliance-like availability." Microsoft's press release described the new PC as "just one example of the type of innovation required to address the needs of users—innovation that is only possible when hardware and software are developed together."

Innovation happens when an organization supports individuals and small teams in their efforts to think and act innovatively. This year, one major effort of the Defense Information Systems Agency (DISA) is establishing an IA Knowledge Management initiative. Using portal technology, DISA plans to develop a method to facilitate the organization of COIs with the IA community to facilitate information sharing and collaboration. This effort, if successful, will facilitate work efforts across the IA community, synchronize major projects, and reduce redundant work efforts.

IA is critical to net-centric operations and warfare. Just how critical, DoD customers have yet to come to terms with. Consider the following:

1. In military exercises, networks and information are used extensively to plan and execute operations.
2. Red Team operations in these exercises are severely restricted and closely controlled.

Until the military commander allows Red Teams to operate unfettered in exercises, warfighters will neither trust the networks and information they rely on to execute the mission nor will they trust their capability to successfully deter or defeat an attack on their information networks. This is perhaps the greatest challenge to the DoD IA community—to develop capabilities that provide that trust to warfighters and promote those capabilities in terms they can understand.

Do our people, operations, and capabilities support our need to transform or even "leap ahead" to some new way of organizing and operating? Can we "keep pace" with rapid technological change? Can we really transform ourselves in both operations and technology to stay one step ahead of our adversaries? In the realm of information warfare today, our enemy is infinitely more agile and adaptable and continues to move at will between networks, exploiting well-known vulnerabilities and then stealing, manipulating, or destroying sensitive data. The DoD IA Community must come to terms with this reality. We must develop the right strategy to address known, evolving, and future threats to ensure DoD's continued warfighting success in a net-centric operating environment. Transformation is the process, and innovation is the engine. ■

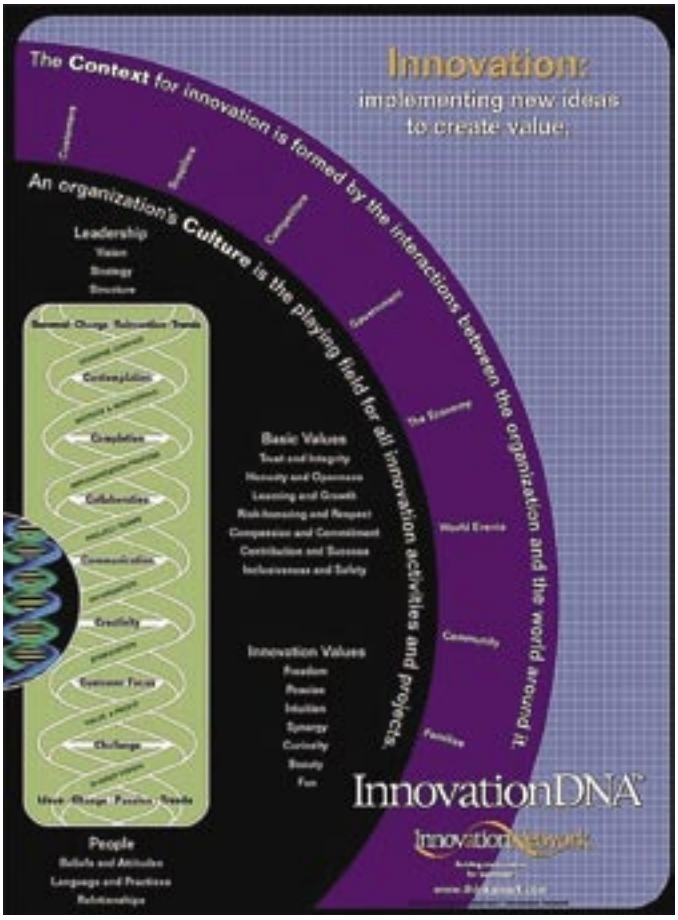


Figure 1: Innovation Chart

About the Author

Vivian Cocca

Vivian A. Cocca has served the Department of Defense (DoD) for over 20 years in the areas of intelligence, operations, and information security. She began her career as an Army intelligence officer assigned to air defense, cavalry, and special operations units. She was assigned to the Pentagon in 1997 as an executive assistant to the Deputy Assistant Secretary of Defense for Intelligence, Programs & Evaluation in Command, Control, Communications, and Intelligence (C3I), where she managed a variety of special projects and ensured efficient staff operations. Ms. Cocca is currently responsible for developing DoD's IA Strategy and oversees the strategic management process, manages all corporate communications, and develops and defines business relationships with critical industry partners. She holds a B.S. degree in Geography, an M.S. degree in Strategic Intelligence, is CIO Certified, and is a Certified Information Security Systems Professional (CISSP).

IATAC Spotlight on Subject Matter Expert (SME)—Dr. Peng Liu

by Ronald Ritchey

This article is the second in a series of profiles of members of the Information Assurance Technology Analysis Center (IATAC) Subject Matter Experts (SMEs) program. Information Assurance (IA) and Information Operations (IO) experts from many different types of organizations volunteer to be IATAC SMEs and provide information on their areas of expertise, education and training, professional certifications, inventions, and patents. When the Department of Defense (DoD) or other government personnel contact IATAC with questions regarding IA or IO, IATAC can leverage its SME database to identify people who are particularly well suited to answering those questions. SMEs are also encouraged to contribute papers and other materials to the IATAC Scientific and Technical Information (STI) collection. The work of the SMEs furthers our understanding and capabilities in IA.

The IATAC SME profiled in this article is Dr. Peng Liu, an assistant professor at the School of Information Sciences and Technology (IST) [1] at The Pennsylvania State University (PSU) in University Park, PA. [2] Dr. Liu is also the director of the Cyber Security Lab at PSU [3] and a Faculty Coordinator for PSU's Center for Information Assurance (CICA). [4] His primary areas of research are self-healing systems, economics-based attacker modeling, worm containment, and secure information sharing and integration. Dr. Liu received his Ph.D. in Information Technology from George Mason University in 1999. He is the co-author of *Trusted Recovery and Defensive Information Warfare* and has contributed chapters to several other IA-related books. Dr. Liu has served on the program committees for many recent IA-related conferences, and he has also been a referee for dozens of IA journals. Dr. Liu is the author of the article "Emerging Technologies in IA," which begins on page 22 of this newsletter.

One of Dr. Liu's most recent endeavors is his work incorporating game theory to model a defender's network in conjunction with an attacking system. [5] The model is based on the assumption that, although an attacker wants to cause maximum damage, the defender has many security controls in place that could detect and defeat the attacker. Accordingly, the modeling is based not only on the potential rewards—but also the potential risk—to the attacker. The model evaluates the options available to the attacker at every step and determines the likelihood of each option being chosen by using economic theories to analyze the trade-offs between reward and risk. Dr. Liu and his fellow researchers have performed various attack-prediction simulations, including Distributed Denial of Service (DDoS) attacks. One possible outcome of this research is the development of a method for profiling attackers. By analyzing an attacker's actions, an attack-prediction system could determine the actions most likely to be performed in the attack.

Dr. Liu has also been performing extensive research into self-healing databases—databases that can repair themselves after an attack. [6] The motivation behind the project is data manipulation by insiders (*e.g.*, someone could change a value in a database field from 100 to 1000), causing someone else to make an incorrect and potentially damaging decision. The project uses existing techniques for detecting that certain transactions are suspicious or malicious and may have corrupted the data; the focus of the project is not on detection but on developing more robust recovery capabilities. It is relatively simple to replace corrupted data with previous versions of the same data, but it is much more challenging to also address all subsequent transactions that were dependent on the corrupted data.

If you have a technical question for Dr. Liu or other IATAC SMEs, please contact iatac@dtic.mil. The IATAC staff will assist you in reaching the SME best suited to helping you solve the challenge at hand. If you have any questions about the SME program or are interested in joining the SME database and providing technical support to others in your domains of expertise, please contact iatac@dtic.mil, and the URL for the SME application will be sent to you. ■

References

1. http://ist.psu.edu/
2. http://www.psu.edu/
3. http://ist.psu.edu/s2/
4. http://net1.ist.psu.edu/cica/

by George Bieber

Goal 5 initiatives empower the DoD IA workforce to support the changing demands of the Information Assurance/Information Technology enterprise.

The Defense-Wide Information Assurance Program (DIAP) is making significant progress toward achieving the objectives for Goal 5, Create an IA-empowered Workforce, of the DoD Information Assurance (IA) Strategic Plan. Goal 5 addresses IA awareness, technical training and education, and workforce management. IA awareness is targeted to all DoD employees from entry level to Senior Executive Service (SES) and Flag Officers. Technical training and education focuses on system and network administrators and personnel performing IA functions on DoD workstations, systems, and networks. IA management training requirements support IA Officers (IAOs), IA Managers (IAMs), and Designated Approving Authorities (DAAs) and their staffs. Goal 5 comprises four key objectives, shown in Table 1 below.

Table 1. Goal 5 objectives

Objective	Impact
[1] Certify the workforce	Personnel performing IA functions trained and certified to recognized, national certifications
[2] Manage the workforce	IA billets identified and occupied by trained personnel
[3] Sustain the workforce	Training funds available to enable personnel to maintain currency of their IA skills
[4] Extend the discipline	IA infused in other training and awareness disciplines for specialty workforces, including acquisition, legal, and test and evaluation

A key milestone for Goal 5 was the signing in August 2004 of DoD Directive 8570.1, *IA Training, Certification, and Workforce Management*. While the Directive touches on all four Goal 5 objectives, its primary emphasis is on certifying and managing the IA workforce. The policy establishes a framework that will ultimately allow both Components to better manage their IA personnel and also underpin DoD's goal to create and foster an IA professional workforce.

The reality of 8570

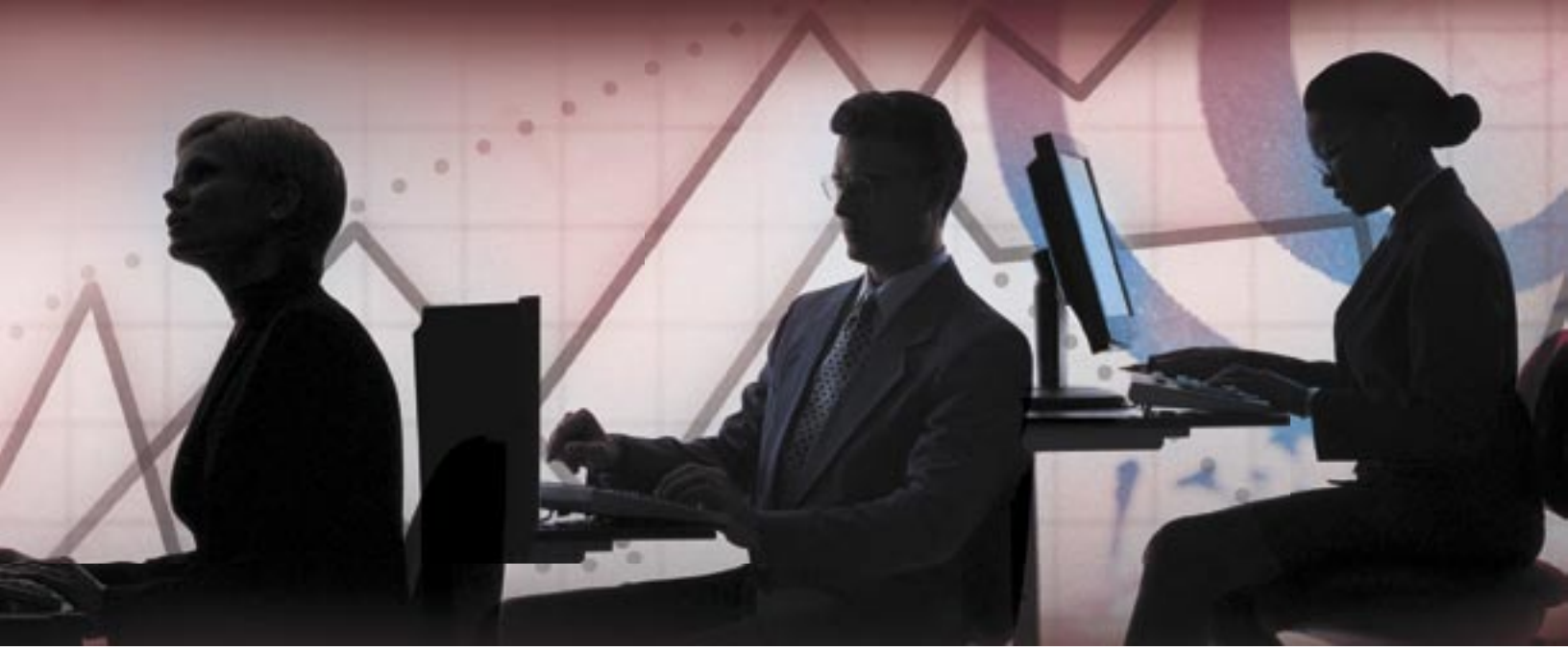
It is important to note that 8570 is one step in a long process to transform DoD's IA workforce. While there will be successes along the way, there are likely to be many questions and challenges as Components work to implement the policy. Nor will 8570 solve all the training issues of DoD's IA; it is never easy to provide a "one-size-fits-all" solution, especially in an organization as complex as the DoD.

The Directive, however, represents a critical step in strengthening and building the IA professional workforce within DoD. The ultimate vision of the Directive is a sustained, truly professional IA workforce with the knowledge, skills, and tools to effectively prevent, deter, and respond to threats against DoD information, information systems, and information infrastructures—and with the ability to put the right people with the right skills in the right place at the right time.

8570 support of Goal 5 objectives

Certify the workforce

Since 1998, DoD Components have been required to certify their IA workforces. However, without formal policy guidance at the DoD level, the results have been mixed. Components report that their workforces are certified, but it's not clear precisely what this may mean. Component "certifications" generally are unique to that organization, are not portable, and are unlikely to satisfy the requirements of other Components or of Combatant Commands. Even within an individual Service, there is a lack of uniform certification. The military IA workforce receives its training from one source and may be "certified" by its occupational specialty training. The civilian and contractor workforces receive their training from multiple sources and may or may not have formal commercial certifications. Yet military personnel, civilians, and contractors all operate on DoD systems and networks together. There



has been no enterprise-wide solution, despite the fact that the DoD fights jointly—and will "Fight the Net" jointly—across the IA workforce.

Directive 8570.1 provides the basis for an enterprise-wide solution. It requires privileged users and IA managers to be trained and certified to a DoD baseline requirement. The Directive's accompanying Manual, currently in SD106 review, comprises the certifications that will determine the scope of the Directive's enterprise-wide certification program. Components may require their IA workforces to receive additional training or certifications, but all personnel performing IA functions must meet the DoD baseline.

Meeting these requirements may not be as difficult as it first appears. DIAP is undertaking a number of initiatives to assist Components in preparing to meet 8570 requirements. For example, the DIAP is conducting IA training-course assessments. At the invitation of the Army and the Navy, the DIAP evaluated two primary courses against the Computing Technology Industry Association (CompTIA) Security+ certification. The content of both the Army IA course at Fort Gordon, GA, and the Navy IA course at Fleet Training Center (FTC), San Diego, CA, were found to prepare personnel well for the Security+ test. These IA course assessments suggest that training already available throughout DoD, with little or no modification, can prepare IA personnel to meet the 8570 requirements. The DIAP is currently examining an Information Assurance Policy & Technology (IAP&T) course developed by the Defense Information Systems Agency (DISA) as well as a subset of the Web-Based Training (WBT) products proposed by DISA. Also, many Components have site licenses for online training through Netg or PeopleSoft, and both of these commercial providers have specific products designed to prepare personnel for various IA certifications.

Manage the workforce

DoD Directive 8570 focuses heavily on workforce management. It seeks to provide the tools to facilitate both component management of its IA workforce and the insight of the Office of the Secretary of Defense (OSD) into DoD's overall IA workforce status and certification posture. Components must identify both IA positions and the personnel performing IA functions and ensure that the personnel filling those positions meet training and certification requirements related to their job functions.

Personnel, manpower, and training databases of record currently can't do all that is required of them. Work has begun to upgrade the Defense Civilian Personnel Data System (DCPDS), and requirements have been submitted to the Defense Integrated Military Human Resources System (DIMHRS). Existing military personnel and manpower databases and all other databases will also require upgrading. To provide the enterprise perspective, the Defense Manpower Data Center (DMDC) will be the collection point for relevant data from Component databases. DMDC will also provide the tools in the form of the Defense Enrollment Eligibility Record System (DEERS) and Common Access Card (CAC) to support 8570 requirements that pertain to contractor IA personnel and other special cases.

The long-term success of the certification program depends on the alignment of positions and personnel, the requirements of operational mission and force structure, and the availability of budgetary resources to develop and sustain the professional IA workforce, as shown in Figure 1.

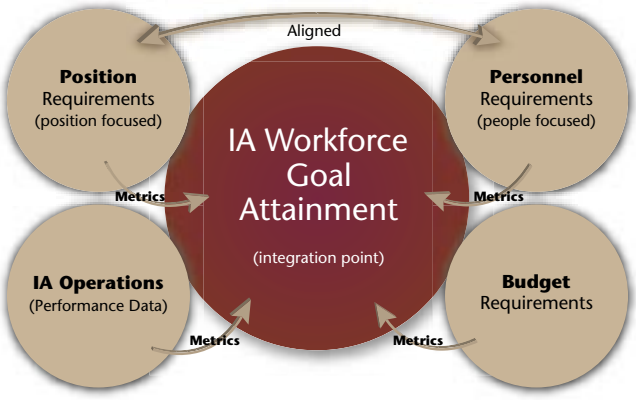


Figure 1. IA workforce goal attainment

Sustain the workforce

Training is often the first area to suffer whenever there is pressure on budgets. Sustaining the workforce is intended to ensure that the DoD IA workforce receives continuous learning opportunities, their IA skills are kept current, and DoD's ability to recruit and retain high-caliber talent to defend its systems and networks is strengthened. Continuous learning and/or periodic re-testing is required for maintaining an IA baseline certification. A variety of in-house training products exist that may serve to satisfy a continuous learning requirement. These include courses at Service schools; the Information Resources Management College (IRMC); Fort McCoy, WI; the DISA WBTs; and other in-house sources. In addition, the DIAP proposes that an individual's participation in the Air Force Black Demon exercise or the multi-service Black Demon+ be counted as continuous learning credit toward maintaining certification status.

Extend the discipline

Extending the IA discipline infuses IA into areas that traditionally have not considered security or cybersecurity a high priority. One example is the acquisition workforce: virtually all weapon systems contain software, and many are linked to the Internet. Acquisition program managers need to consider IA up front, and "bake it in" to a system during development rather than "brush it on" after the fact. Last year, in collaboration with the Defense Acquisition University (DAU), the DIAP produced an IA for Program Managers online course. This year, because of recent policy changes, the course will be updated. Another example is the legal community. The DIAP, DISA, and a legal-issues working group comprised of lawyers from throughout DoD, collaborated on an IA training product for lawyers. The Cyber-Law I WBT is available through DISA's Information Assurance Support Environment (IASE) site (http://iase.disa.mil). Currently, DIAP and DISA are collaborating on two additional products to extend IA training to non-IA disciplines. The first, developed in collaboration with DoD and the offices of Service Inspector General (IG) and Service IA Subject Matter Experts (SMEs), will be a WBT focusing on IA fundamentals for IGs and auditors. The training tool will include the latest DoD policy developments and the impact of the Federal Information Security Management Act (FISMA) on DoD Components, IGs, and auditors. The second project, involving the Director Of Operational Test & Evaluation (DOT&E), along with the DIAP and DISA [the Field Security Operations (FSO) division and the Joint Interoperability Test Command (JITC)], will address IA in the test and evaluation processes.

DoD IA Scholarship Program

The DoD's Information Assurance Scholarship Program (IASP) provides educational incentives to foster the recruitment and retention of qualified IA/Information Technology (IT) personnel. As a resource for DoD IA professionals to continuously enhance their skills and to keep current with technology and threats, the IASP supports the Goal 5 objective to sustain the IA workforce.

The National Security Agency (NSA) is the IASP executive agent and manages the program on a day-to-day basis. In 2004, the program provided scholarships to some 100 students engaged in IA studies and capacity building and research grants to more than 25 universities. Supervisors of personnel who earned a degree through the IASP ranked IASP graduates as "better" or "far superior" then non-IASP graduates in their overall knowledge of IA trends, issues, and priorities; their ability to apply IA skills and education to the current environment; their overall caliber; and the ease with which they transitioned into new roles. Information on the IASP is available at http://www.defenselink.mil/nii/iasp.

The devil in the details

The details of 8570 requirements and implementation are in the Manual, which is scheduled to complete formal SD106 coordination by early April. When all comments have been received, DoD will know what is possible with regard to creating a professional IA workforce based on a program of enterprise-wide baseline certification. The Manual will provide the following information:

- Define IA workforce categories (technical, management); levels within categories (I, II, III); and functions within levels.
- Identify specific certifications as the DoD baseline for each category and level.
- Seek a degree of rigor and independent third-party review of certifications used to meet the DoD IA requirement.
- Allow for "equivalent" certifications, if approved by a DoD IA Certification Review Board.
- Require a minimum number of continuous learning hours for individuals to maintain certified status.

Current priorities

The 9th Annual IA Workshop, held February 7–10 in Philadelphia, Pennsylvania, provided valuable input from Components on their issues, concerns, and the status of 8570 implementation planning. Actions relevant to Goal 5 that were identified at this year's workshop include the following:

- Engage Personnel and Readiness (P&R), the human resources community, and operations at all levels to enhance effective implementation of and compliance with 8570.
- Host implementation workshops to assist Components, particularly agencies, to better understand the requirements.
- Co-host, with P&R, IA workforce data-management workshops to coordinate data-exchange requirements with personnel, manpower, and training database owners throughout DoD.
- Provide a database of Component-sponsored training to support DoD's certification program.
- Examine in-house training for alignment with certification requirements.

The road ahead

As discussed earlier, the 8570 Directive represents a beginning. Much remains to be accomplished. To this end, a number of initiatives are planned or are currently under way to support overall implementation efforts:

- **New legislative proposal**—The U.S. Navy has proposed legislation to amend Chapter 101 of Title 10, United States Code, to permit the Services to use appropriated funds to pay for commercial certifications (tests) for uniformed personnel. The proposal was approved by DoD and, as of early March, is under review by the Office of Management and Budget (OMB). If passed by Congress, the law would give uniformed personnel parity with civilians.

- **IA skill standards development**—To enable better mapping of certifications against jobs, DoD recognizes the need to document its IA jobs and knowledge to define a common language of IA-related work and worker requirements. Assistant Secretary of Defense for Networks and Information Integration (ASD–NII) is currently working to integrate existing IA Job Task Analysis (JTA) and skills standards from across DoD as the first step toward certification "product improvement."

- **Enterprise-wide solutions**—DIAP will pursue initiatives with enterprise-wide potential to enhance training outcomes through hands-on IA training tools and exercises. These will serve to quickly build experience, as new threats and vulnerabilities appear and new tools and techniques are fielded.

There will be many challenges to fully implementing 8570. It won't happen overnight. But Directive 8570.1 represents the first step toward building and strengthening the IA professional workforce within DoD. ■

About the Author

George Bieber

Mr. Bieber is Deputy Director, Human Resources and Training, Defense-wide Information Assurance Program (DIAP). He has oversight responsibility for all aspects of the Department's IA education, training, and awareness activities, including the DoD IA Scholarship Program, and IA workforce management issues.

His most recent efforts have centered on development and coordination of DoD Directive 8570.1, IA Training, Certification and Workforce Management, and its implementing manual.

Previously he was at the Defense Information Systems Agency, where he managed the development, production and dissemination of Department of Defense (DoD) IA training and awareness distributive training products.

Mr. Bieber has served on the Education Standing Committee of the President's Critical Infrastructure Protection Board, and as a member of the Executive Board of the Federal Information System Security Educators Association (FISSEA). He was the FISSEA 2000 Educator of the Year, and a recipient of the Federal Computer Week's Federal 100 award for 2003.

The GIG IA Architecture—Defending Systems and Networks (Goal 2)

…continued from page 7

Notwithstanding all the successes that Goal 2 has achieved, hackers, cyberterrorists, foreign nation states, and insiders continue to pose a constantly evolving threat. To protect the systems, networks, data, and critical-information infrastructure on which DoD's net-centric operations depend, DoD must also continue to evolve and improve its defenses. Through the leadership of USSTRATCOM, the DIAP, the ESSG, and the cooperation of the Combatant Commands, Services, Agencies, and field activities, DoD is making steady progress toward better protecting the entire enterprise through Department-wide and interoperable tools obtained through both centralized funding and standardized and streamlined acquisition processes. The net-centric manner in which DoD now operates, both in peacetime and in conflict, requires no less. ■

About the Authors

John Hunter

John Hunter is the Deputy Director for Operations in the Defense-Wide Information Assurance Program (DIAP), under the Assistant Secretary of Defense for Networks and Information Integration. He is currently on loan to the DIAP from the Defense Information Systems Agency (DISA). Before assuming his current position, he held multiple senior level technical and management positions within DISA, including serving as the Information Assurance Program Manger. Prior to DISA, he served in senior level positions within the U.S. Army Information Systems Engineering Command. He has a Bachelor of Science degree in Electrical Engineering from Western New England College, a Master of Science in Telecommunications from the University of Colorado, and a Master of Science in Management from Frostburg State University.

Rick Aldrich

Rick Aldrich is the Senior Computer Network Operations Policy Analyst for the Information Assurance Technology Analysis Center (IATAC). Before assuming his current positions, he served as the Deputy Staff Judge Advocate for the Air Force Office of Special Investigations, specializing in the cybercrime and information operations portfolios. He has been awarded several grants by the Institute for National Security Studies to study the legal and policy implications of cybercrime and information warfare. He has multiple publications in this field; most recently with the inclusion of a chapter on information warfare in a national textbook on National Security Law. He has a Bachelor of Science degree in Computer Science from the U.S. Air Force Academy, a Juris Doctor from UCLA, and a Master of Laws in Intellectual Property Law from the University of Houston.

Emerging Technologies in Information Assurance (IA)

by Dr. Peng Liu

As society increasingly relies on digitally stored and accessed information, traditional Information Security (IS) technologies, policies, management, and practices are found to be more and more limited in satisfying the security and assurance needs of modern information systems and applications, for several reasons. In general, because IS addresses only the protection of information against unauthorized disclosure, transfer, modification, or destruction, traditional IS cannot deliver the level of Information Assurance (IA) that modern applications require.

First, digitally stored and accessed information increasingly relies on the availability of information and the reliability of the corresponding information system. However, availability and reliability are largely neglected by traditional IS. Second, although information confidentiality, privacy, and integrity protection are certainly crucial in meeting the security needs of modern applications, not all attacks can be prevented. These attacks can cause substantial losses in confidentiality and privacy (by unauthorized disclosure of information), substantial integrity loss (by unauthorized modification of information), substantial availability/reliability loss and serious denial of service (by destruction of some critical components of the information system), and substantial non-repudiation loss (by destruction of evidence and audit data). When applications were lightly dependent on digitally stored and accessed information, such IS losses might have been tolerable. But as digitally stored and accessed information proliferates, such security losses can be disastrous. Hence another fundamental limitation of traditional IS is how to address these successful attacks or intrusions.

Because of these concerns, meeting the security and assurance needs of modern information systems and applications from a broader perspective is introduced. In addition to preventing information from being disclosed, modified, or destroyed, intrusions should be detected; countermeasures (responses) to intrusions should be planned and deployed in advance; security and fault-tolerance mechanisms should work together to ensure confidentiality, privacy, integrity, non-repudiation, authenticity, availability and reliability in the presence of attacks; and the damage caused to the information and the information system should be repaired and restored (or recovered). This total effort is referred to as Information Assurance (IA). For example, from the military perspective, IA must address the delivery of authentic, accurate, secure, reliable, and timely information, regardless of threat conditions, within the distributed and heterogeneous computing and communication environment.

The basic meaning of IA is well captured in the National Information Systems Security Glossary:

> *Information Assurance (IA): Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.*
>
> **National Information Systems Security (INFOSEC) Glossary, NSTISSI No. 4009, August 1997**

Compared with the concepts of IS, whose definition is quoted below, it is not difficult to see that the concept of IA is much broader than that of IS:

> ***Information Security**—The protection of information against unauthorized disclosure, transfer, modification, or destruction, whether accidental or intentional.*

- The focus of IS is on protection or prevention, while the focus of IA is on integrating protection, detection, and reaction.
- Intrusion detection and reaction are not a major concern of IS, but they are certainly crucial for IA.
- Attack recovery or restoration may be a topic out of the scope of IS, but it is a critical component of IA.
- The goal of IS technologies is to prevent attacks from happening, while the goal of IA is to ensure that even if some attacks penetrate an information system, certain levels of availability, integrity, authentication, confidentiality, or non-repudiation can still be guaranteed.

There is no doubt that IA involves many disciplines and has various aspects, such as the policy, legal, ethical, social, management, evaluation, and technical aspects of IA. Compared with traditional IS practices, IA not only involves designing and developing various new security technologies but also involves a number of emerging policy, legal, ethical, social, economic, management, evaluation, and assurance issues as IA drives people's practices of IS at an ever quicker pace. Nevertheless, to make this article more tangible, it will primarily focus on the technical aspect of IA, though some relevant policy, management, and evaluation issues will also be addressed.

Overview of IA technologies

In this section, we will provide a comprehensive overview of IA technologies, with a focus on the emerging third-generation IA technologies and their relation to more established intrusion-prevention and -detection IA technologies.

Three generations of IA technologies

In general, existing IA technologies can be "clustered" into three generations. There is a natural evolution or maturing that has occurred in the IA community, and these generations offer evidence of this evolution.

- **First generation**—Prevent intrusions. In this generation, the goal is to prevent attacks from succeeding. The representative technologies are Trusted Computing Base, access control and physical security, multiple levels of security, and cryptography.
- **Second generation**—Detect intrusions. Since not all attacks can be prevented, intrusions will occur. Hence, the goal of this generation of IA technologies is to detect intrusions. Representative technologies at this level are firewalls, intrusion-detection systems, and boundary controllers.
- **Third generation**—Operate through attacks (or survivability). Since some attacks will succeed, we need third-generation IA technologies, the goal of which is to enable information systems to continue delivering essential services with security assurance in the presence of sustained attacks. Some representative technologies at this level are real-time situation awareness and response; real-time trade-off of performance, functionality and security; intrusion tolerance; and graceful degradation. It should be noted that third-generation IA technologies do not simply focus on the availability domain; their dimensions are much broader. In particular, without delivering such security assurance as confidentiality (privacy), integrity, authenticity, and non-repudiation, essential services cannot be continuously delivered under sustained attacks. In general, survivability not only means availability under attacks but also confidentiality (privacy), integrity, authenticity, and non-repudiation under attacks. Moreover, in many situations, survivability implies reliability.

It should also be noted that among the three generations of IA technologies, each generation is crucial in achieving the goals of IA, and one cannot replace another. (Second-generation IA technologies do not subsume first-generation IA technologies, and third-generation IA technologies do not subsume second-generation IA technologies.) To begin with, first-generation IA technologies build the foundation for IA, because without strong protection of information confidentiality, privacy, integrity, authenticity, and non-repudiation, there can be too many successful attacks for the information system to survive. Moreover, intrusion prevention, intrusion detection, and intrusion tolerance (or survivability) actually share primarily the same goal—to ensure information confidentiality, privacy, integrity, availability, authenticity, and non-repudiation in the face of attacks. A highly trusted and assured information system should be able to prevent as many attacks as possible from penetrating the system, detect the attacks that could not be prevented with accuracy and agility, and robustly operate through and recover from these successful attacks without losing availability, reliability, and accountability. Second, third-generation IA technologies are largely dependent on second-generation IA technologies, because many third-generation IA technolo-

gies assume that intrusions can be detected in a timely manner with good accuracy (*e.g.*, with low false-positive and false-negative rates).

Nevertheless, in this article we will focus on the third-generation IA technologies, because first- and second-generation IA technologies are well illustrated in the current literature.

Third-generation IA technologies

Related to the fault-tolerance concept and drawing from that discipline is the area of intrusion tolerance or survivability. Intrusion tolerance is emerging as one of the most important Research & Development (R&D) areas in Cyber Operations today. The systems and networks we depend on must continue to operate through intrusions and keep operating, although in a degraded mode, in spite of a sequence of successful cyber attacks.

Classification of survivability technologies

We can classify existing survivability technologies into two categories: intrusion masking and Defense-in-Depth. Two well-known intrusion-tolerance research programs are the Malicious- and Accidental-Fault Tolerance for Internet Applications (MAFTIA) and the Organically Assured and Survivable Information Systems (OASIS) projects.

- **Intrusion masking**—From a design perspective, one system design can be inherently much more attack resilient than another. The goal of intrusion masking is to redesign a regular, vulnerable computer system with enough redundancy so that the new, survivable design can function correctly even if part of the system is hacked. In this case then, we say the new survivable design can mask intrusions. Techniques in this category focus on how to enhance the inherent resilience of a secure system, and their effectiveness is typically much less sensitive to the agility and accuracy of intrusion detection than pragmatic, run-time intrusion-response techniques. General principles in developing attack-resistant designs include, but are not limited to, (a) redundancy and replication, (b) diversity, (c) randomization, (d) fragmentation and threshold cryptography, and (e) increased layers of indirections. Techniques in this method include, but are not limited to, Byzantine intrusion-masking techniques that follow the redundancy and replication principle, threshold-cryptography-based, attack-resilient systems that follow the fragmentation principle; multi-path routing that follows the redundancy principle; and resilient overlay networks that follow the "increased layers of indirections" principle.
- **Defense-in-Depth (DID)**—Instead of redesigning a system, the goal of DID technologies is to arm the system with a set of attack- and threat-response facilities which, with the help of intrusion detection, can respond to intrusions in a way that will permit the system to operate through attacks. Technologies in this category include (a) boundary controllers, such as firewalls and access control; (b) intrusion detection; and (c) threat/attack/intrusion response. It is well known that boundary controllers cannot prevent every attack.

Intrusion detection—This technique is a key part of many survivable systems, but existing intrusion-detection technologies in general suffer the high false-positive and false-negative rate problem, especially when the detection is anomaly based or specification based. Since intrusion-detection techniques cannot guide us to respond to intrusions, existing Defense-in-Depth technologies focus on intrusion response, which can be classified into three categories:

- **Type 1: Reactive response**—Techniques in this category are activated only when an intrusion is identified and their effectiveness is highly dependent on the accuracy and latency of intrusion detection. For example, attack-recovery techniques belong in this category. If the detection is quick and accurate, then the contaminated part of the system can be quickly repaired without causing serious integrity degradation. However, if there are many false alarms, many clean elements could be corrupted by wrong "repairs." Some other Type 1 techniques include, but are not limited to, reactive one-phase damage-containment techniques, detection-based (firewall) reconfiguration techniques, and patching techniques.

- **Type 2: Proactive response**—Based on suspicious activities (or signs), techniques in this category are proactively triggered before an intrusion is confirmed. Although proactive response may consume more resources, it may immunize the system from damage caused by many attacks. Moreover, many proactive response mechanisms are transparent to users. Type 2 techniques include, but are not limited to, isolation, multi-phase damage containment, and sandboxing.

- **Type 3: Adaptive response**—Feedback-based adaptation is an attractive feature of many survivable systems, in which the defense posture (*i.e.*, the security mechanism configuration of the system) is dynamically adjusted based on the changing environment. Adaptive-response addresses the reconfigurable computing and communication aspect of survivable information systems. Type 3 techniques include, but are not limited to, the OASIS Willard project and the adaptive Intrusion Tolerant Database (ITDB) system.

Because intrusion detection makes the system attack aware but not attack resilient (*i.e.*, intrusion detection itself cannot maintain confidentiality, integrity, and availability of information in the face of attacks), intrusion response is crucial to building survivable systems.

Compared with intrusion-masking technologies, in which many attacks may be masked without causing any system-security degradation (*e.g.*, of integrity and availability), DID technologies usually introduce a certain level of system-security degradation. On the other hand, the advantage of DID technologies is that (a) they do not require that the system be redesigned and can be directly applied to legacy systems, and (b) their overhead is typically smaller than intrusion-masking technologies.

The key issues and problems in developing Defense-in-Depth technologies rest in how to implement the following:

- Quickly contain/isolate the intrusions so that their infection will not be too serious to operate through.
- Quickly distinguish the damaged part from the undamaged part of the system.
- Quickly repair the contaminated part of the system without bringing it off-line.
- Handle the impact of false alarms, undetected intrusions, and the detection latency.
- Make the intrusion-response facilities adaptive and proactive.
- Validate the cost effectiveness of DID technologies.

In the current literature, DID is usually referred to as Information Warfare-Defense (IW-D). IW-D does everything possible to prevent attacks from succeeding, but it also assumes at the outset that not all attacks will be averted. This places increased emphasis on the ability to live through and recover from successful attacks. IW-D must consider all phases of attack and recovery. These phases, and the activities that occur in each, are proposed as follows:

- **Prevention**—The defender puts protective measures in place.
- **Intelligence gathering**—The attacker observes the system to determine its vulnerabilities and find its most critical functions or data to target.
- **Attack**—The attacker carries out the resulting attack plan.
- **Detection**—The defender observes symptoms of a problem and determines that an attack may have taken place or be in progress.
- **Containment**—The defender takes immediate action to eliminate the attacker's access to the system and to isolate or contain the problem, preventing it from spreading further.
- **Damage assessment**—The defender determines the extent of the problem, including failed functions and corrupted data.
- **Reconfiguration**—The defender may reconfigure to allow continued operation in a degraded mode while recovery proceeds.
- **Repair**—The defender recovers corrupted or lost data and repairs or reinstalls failed system functions to re-establish normal operations.
- **Fault treatment**—To the greatest extent possible, the defender identifies weaknesses exploited in the attack and takes steps to prevent a recurrence.

Some operations—prevention, intelligence gathering, detection, containment, reconfiguration, and repair—lend themselves to automated mechanisms and support within the system being attacked. Others, such as fault treatment and some aspects of damage assessment, typically require human intervention.

The Information Warfare (IW) defender's goal is to keep the system operating to support as much critical processing as possible, even if the system is contaminated (or infected) by an attack. One way to ensure continued service is to explicitly address integrity losses caused to the systems in the presence of IW attacks. To some degree, real systems lack integrity most of the time. These integrity losses do not always prevent the systems from achieving their critical objectives. The challenge in IW is to anticipate acceptable integrity losses and design systems that operate in these degraded modes.

Survivability *vs.* fault tolerance

As a core concept of the third-generation IA technologies, survivability builds on several related fields of study (*e.g.*, security, fault tolerance, safety, reliability) and introduces new concepts and principles. In particular, because many survivability technologies are motivated by fault-tolerance technologies, questions arise concerning the differences between these two fields. Three major differences between survivability and fault-tolerance technologies are as follows:

- First, in fault tolerance, failures randomly happen; in security, attacks are typically intentional. Moreover, attacks are more intelligent and active (*i.e.*, more intentional and better planned) than failures; therefore, more proactive tolerance techniques are needed for survivability.
- Second, intrusion detection is typically much more complicated than failure detection. This is why there are so many new research challenges in intrusion detection.
- Third, in the literature of fault tolerance, intrusions in many cases are modeled and tolerated as Byzantine or arbitrary faults. Therefore, if a system is Byzantine-fault tolerant, it is able to tolerate intrusions to some degree. A practical Byzantine-fault-tolerant system can tolerate both faults and intrusions. However, it should be noted that not all damages to the system are caused by faults and not all intrusions can be modeled as Byzantine faults. For example, successful intrusions at the application level (*e.g.*, corrupted transactions of database systems) and data corruption usually do not appear as faults and cannot be handled by Byzantine-fault tolerance.

Conclusion

As society increasingly relies on digitally stored and accessed information, applications demand increasingly higher requirements to support the availability, integrity, and confidentiality of this information, and traditional information-security technologies are increasingly limited in satisfying the security requirements of applications because of their inability to survive successful attacks. As a result, IA technologies are introduced to not only prevent information from being disclosed, modified, or destroyed but also to detect intrusions and operate through attacks so as to ensure that a certain level of IS can be maintained in the presence of attacks. In this article, we surveyed the natural evolution of IA technologies. Three generations of IA technologies are summarized, and the newest generation of IA technologies is discussed in detail. In summary, this article takes the first steps toward providing a comprehensive overview of the scope of IA technologies; the relations among emerging survivability technologies and the more established IA technologies, such as IS and intrusion detection; the characteristics of survivability technologies; and the representative ideas, principles, and techniques of survivable systems development.

Although various emerging IA technologies have been recently developed to ensure a certain level of IS for applications in the presence of attacks, existing IA technologies are still in their earliest stages and are limited in many aspects, and advanced IA technologies have not yet been widely deployed. Hence many existing new IA technologies and practices are yet to emerge, including the following:

- **The threat aspect of survivability**—Without a tangible and accurate threat model, a highly assured information system cannot be developed. To build a good threat model, both system vulnerabilities and attack characteristics (*e.g.*, intent) are crucial. Some preliminary research has been done in analyzing an attacker's intent and strategies, but more research is certainly required.
- **Survivability requirements analysis**—Without a clear specification of a user's survivability requirements, a survivable system may either overreact to attacks (and threats) or not be proactive enough, and therefore the effectiveness of survivability mechanisms may not be well evaluated. Survivability-requirements analysis is a challenging problem, especially when quantitative requirement specifications are expected.
- **Survivability metrics and measurements**—IA metrics are scarce and qualitative. Given the need to determine the IA posture for a given organization under given conditions, users in the field require a means to determine the relative degree of assurance associated with the information assets under their control. Likewise, developers of survivable systems require metrics to measure the degree to which they are employing engineering practices during system development. The use of IA metrics would establish trust in a system built from untrusted components, determine sufficient levels of security for the specific tactical situation and condition, and assess system vulnerabilities. IA metrics enable quantitative trade-offs between security and performance (degradation).
- **Service survivability**—Existing IA technologies largely focus on system survivability, but, in many cases, system survivability does not imply service survivability, and additional service survivability facilities and controls are required. Service survivability facilities are application oriented and function at a higher level than system survivability.
- **Wireless IA**—A key piece of the large-scale information enterprise is the wireless IA segment. Wireless networks must exhibit the same functional and IA attributes as wired networks. These networks must be protected, attacks against them must be detected, specifics of successful attacks must be assessed, and, finally, appropriate responses must be carried out. As more and more wireless components become a part of the larger network and as wireless networks proliferate, we need to be aware that these networks, if improperly understood and configured, could provide a "back door" into our protected wired enterprise. Intrusion detection for wireless networks must be addressed as well as recovery of wireless services after adversarial disruption/denial/destruction of friendly networks. ■

About the Author

Peng Liu

Peng Liu, assistant professor of Information Sciences and Technology at Pennsylvania State University and Director of its Cyber Security Lab (http://ist.psu.edu/s2/), is interested in all areas of computer and network security. He has published a monograph and approximately 50 referred technical papers. He is the founding program co-chair of the Association for Computing Machinery (ACM) Workshop on Survivable and Self-Regenerative Systems, the proceedings chair of the 2003 and 2004 ACM Conference on Computer and Communications Security (CCS), and a program committee member of approximately 20 international conferences. His laboratory has developed two major prototypes: ITDB, a self-healing database system prototype (40,000+ lines of code), and ESVT, an Internet security Experiment Specification and Visualization Toolkit (25,000+ lines of code).

Bibliography

P. Ammann, S. Jajodia, C.D. McCollum, B.T. Blaustein, "Surviving Information Warfare Attacks on Databases", Proc. IEEE Symposium on Research in Security and Privacy, Oakland CA, May 1997, pages 164–174.

P. Ammann, S. Jajodia, P. Liu, "Recovery from Malicious Transactions", IEEE Transactions on Knowledge and Data Engineering, Vol. 15, No. 5, September 2002, pages 1167–1185.

D. G. Anderson, H. Balakrishnan, M. F. Kaashoek, R. Morris, "Resilient Overlay Networks", Proc. 18th ACM Symposium on Operating Systems Principles, 2001.

M. Castro and B. Liskov, "Practical Byzatine Fault Tolerance", Proc. OSDI, 1999.

P. Liu, W. Zang, "Incentive-Based Modeling and Inference of Attacker Intent, Objectives and Strategies", Proc. ACM CCS 2003, Oct. 28–31, Washington DC, 2003.

P. Liu, S. Jajodia, "Multi-Phase Damage Confinement in Database Systems for Intrusion Tolerance", Proc. 14th IEEE Computer Security Foundations Workshop, June 11–13, 2001, Nova Scotia, Canada. Pages 191–205.

T.F. Lunt, "A Survey of Intrusion Detection Techniques", Computers & Security, 12(4):405–418, June, 1993.

P. Luenam, P. Liu, "The Design of an Adaptive Intrusion Tolerant Database System", Proc. IEEE Workshop on Intrusion Tolerant Systems, June 2002.

B. Mukherjee, L. T. Heberlein, K.N. Levitt, "Network Intrusion Detection", IEEE Network, June 1994, pages 26–41.

S. Singh, M. Cukier, W. H. Sanders, "Probabilistic Validation of an Intrusion-Tolerant Replication System", Proceedings of the 2003 International Conference on Dependable Systems and Networks (DSN-2003), San Francisco, CA, June 22–25, 2003, pp. 615–624.

Jay Wylie, Michael Bigrigg, John Strunk, Gregory Ganger, Han Kiliccote, Pradeep Khosla, "Survivable Information Storage Systems", IEEE Computer, August 2000.

R. J. Ellison, D. A. Fisher, R. C. Linger, H. F. Lipson, T. A. Longstaff, N. R. Mead, "Survivability: protecting your critical systems", IEEE Internet Computing, Volume 3, Issue 6, 1999, pages:55–63.

http://www.maftia.org/ (MAFTIA project)

http://www.darpa.mil/ipto/programs/oasis_demval/

product order form

Instructions: All IATAC **LIMITED DISTRIBUTION** reports 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/registration.
The *IAnewsletter* is **UNLIMITED DISTRIBUTION** and may be requested directly from IATAC.

Name _____ DTIC User Code _____

Organization _____ Ofc. Symbol _____

Address _____ Phone _____

_____ E-mail _____

_____ Fax _____

Please check one: ❑ USA ❑ USMC ❑ USN ❑ USAF ❑ DoD
❑ Industry ❑ Academia ❑ Gov't ❑ Other

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

_____

LIMITED DISTRIBUTION

IA Tools Reports (softcopy only)

❑ Firewalls ❑ Intrusion Detection ❑ Vulnerability Analysis

Critical Review and Technology Assessment (CR/TA) Reports

❑ Biometrics (soft copy only) ❑ Computer Forensics* (soft copy only) ❑ Configuration Management
❑ Defense in Depth (soft copy only) ❑ Data Mining (soft copy only)
❑ IA Metrics (soft copy only) ❑ Network Centric Warfare
❑ Wireless Wide Area Network (WWAN) Security ❑ Exploring Biotechnology (soft copy only)

State-of-the-Art Reports (SOARs)

❑ Data Embedding for IA (soft copy only) ❑ IO/IA Visualization Technologies (soft copy only)
❑ Modeling & Simulation for IA ❑ Malicious Code

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

UNLIMITED DISTRIBUTION

Hardcopy *IAnewsletters* available

Volumes 4		❑ No. 2	❑ No. 3	❑ No. 4
Volumes 5	❑ No. 1	❑ No. 2	❑ No. 3	❑ No. 4
Volumes 6	❑ No. 1	❑ No. 2	❑ No. 3	❑ No. 4
Volumes 7	❑ No. 1	❑ No. 2	❑ No. 3	❑ No. 4
Volumes 8	❑ No. 1			

Softcopy *IAnewsletters* back issues are available for download at http://iac.dtic.mil/iatac/IA_newsletter.html

Fax completed form to IATAC at 703/289-5467

May

Net-Centric Architecture Conference
May 3–5, 2005
Crystal City, VA
shanr@marcusevanssd.com

Information Security Decisions
May 9–11, 2005
Hilton Chicago, Chicago, IL
http://searchsecurity.techtarget.com/eventsFrame/1,289197,sid14,00.html?passedURL=http%3A%2F%2Finfosecurityconference%2Etechtarget%2Ecom%2F

Information Security Professionals Conference
May 18–20, 2005
Adams Mark Hotel, Dallas, TX
http://www.cissp.com/ispc/

4th Annual PKI R&D Workshop—Multiple Paths to Trust
May 19–21, 2005
http://middleware.internet2.edu/pki05/

Defense Procurement and Acquisition Policy, E-Business Conference
May 23–26, 2005
http://www.acq.osd.mil/dpap/ebiz/ebconference2005.htm

National OPSEC Conference and Exhibition
May 23–27, 2005
Town and Country Resort and Conference Center San Diego, CA
http://www.ioss.gov/conf/noce.html

Information Assurance Conference Pacific—Enabling IA: Why IA Matters
May 24–26, 2005

June

Federal Information Security Conference (FISC)
June 15–16, 2005
Antler's Hilton, Colorado Springs, CO
http://www.fbcinc.com/fisc/

6th IEEE IA Workshop
June 15–17, 2005
USMA, West Point, NY
http://www.itoc.usma.edu/workshop/2005/index.htm

Military Operations Research Society (MORS) 73rd Symposium—Balancing Risk for an Uncertain Future
June 21–23, 2005
USMA, West Point, NY
http://www.mors.org/upcoming_events.htm

Force Tracking 2005
June 27–29, 2005
Ronald Reagan Building and International Trade Center, Washington, DC
http://idga.org/cgi-bin/templates/singlecell.html?topic=221&event=6533

4th Annual Symposium on Information Sharing Homeland Security
June 27–29, 2005
New Orleans, LA
http://www.ncsi.com/ishs05/index.shtml

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

To change, add, or delete your mailing or E-mail address (soft-copy receipt), please contact us at the address above or call us at: 703/289-5454, fax us at: 703/289-5467, or send us a message at: iatac@dtic.mil