12/4

Volume 12 Number 4 • **Fall 2009**

IAnewsletter

The Newsletter for Information Assurance Technology Professionals

Information Assurance Challenges in an International Environment

also inside

IATAC

contents

About IATAC and the *IAnewsletter*
The *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), and Director, Defense Research and Engineering (DDR&E).

Contents of the *IAnewsletter* are not necessarily the official views of or endorsed by the US Government, DoD, DTIC, or DDR&E. The mention of commercial products does not imply endorsement by DoD or DDR&E.

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

IATAC Director: Gene Tyler
Inquiry Services: Peggy O'Connor

***IAnewsletter* Staff**
Art Director: Don Rowe
Copy Editor: Lindsay Marti
Designers: Kathryn Littlehale, Lacey Olivares
Editorial Board: Dr. Ronald Ritchey, Angela Orebaugh, Al Arnold, Kristin Evans, 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 email address (soft-copy receipt), please contact us at—

IATAC
Attn: Peggy O'Connor
13200 Woodland Park Road
Suite 6031
Herndon, VA 20171

Phone: 703/984-0775
Fax: 703/984-0773

email: iatac@dtic.mil
URL: http://iac.dtic.mil/iatac

Deadlines for Future Issues
Spring 2010 February 5, 2010

Cover design: Kathryn Littlehale
Newsletter design: Donald Rowe

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

in every issue

IATAC Chat

Gene Tyler, IATAC Director

The Comprehensive National Cybersecurity Initiative (CNCI) started a trend that is exciting to watch. Every day, the general public becomes more engaged in cyber issues as it observes news reports about cybersecurity, its impact on our national defense, and technology developments that will improve our information assurance (IA) posture.

CNCI has added focus and visibility on how we protect Department of Defense (DoD) networks against attacks, and on protecting industry information as it circulates across corporate networks and migrates into government networks—truly a netcentric environment. After all, we do operate in a global environment.

Increasingly, there is more evidence that our forces operate alongside newly founded coalition and allies. Our response to the global war on terrorism has linked us with the Afghanistan Army, Iraqi forces, and in closer collaboration with the Pakistani Army. Just as our armed forces reach to new coalitions, our corporations interfacing with our government and its networks face similar security concerns with global international markets and many of our new coalition partners. Security is complex and must maneuver through many wickets.

This raises really difficult questions, including: where and how do we draw boundaries? Traditional borders and traditional boundaries often can make the solutions more complex. Who we share information with, how that information is shared, and the security of this information are paramount to netcentricity and globalization. In a world where we need to share information, we must examine how we share information—and how we protect it—beyond the national level to the broader international level. We have to be concerned with protection, not just with regard to national-level government and military information, but interoperable/secure protection of information as it flows from globalized industry.

Brian Bottesini, principal scientist within an IA team for the North Atlantic Treaty Organization (NATO), provides a unique snapshot of this dynamic in this edition's feature article, "Information Assurance Challenges in an International Environment." How do you facilitate information sharing across 28 nations, all with varying laws, policies, competing industries, and agendas? Better yet, how do you maintain cybersecurity at an international level for NATO members and their partner nations? This article describes the challenges NATO faces in securing its information resources, and the challenges we face as we become more interconnected among the global community. NATO has been around for over 60 years, and it struggles with IA. Imagine the hurdles that must be negotiated for not only a newly founded coalition, but also a dynamic coalition that has members filtering in and out.

Cybersecurity continues to grow in prominence and is becoming more mainstream here and abroad. This is good because the first step in solving complex problems is problem identification. We must solve these complex IA problems one step at a time by linking identification, policy, resources, training and education, and acceptance of people, processes, and technologies.

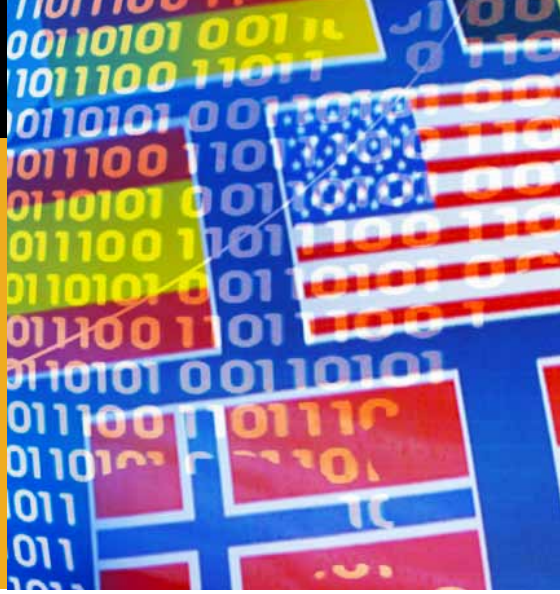
To help solve these complex IA problems, IATAC compiles updated information on important topics for our customers. That is why I am excited to tell you about the four IA Tools Reports IATAC published recently: *Vulnerability Analysis, Intrusion Detection Systems, Firewalls, and Malware*. We distribute these reports to our government customers and their contractors so that they can compare commercial off-the-shelf tools easily and identify which tool is best for their organization. These reports epitomize IATAC's mission to consolidate the information you need most to improve IA posture across your organization. The reports are available for public release, so just email us at *iatac@dtic.mil* to receive your free copy.

I am excited to see what happens as CNCI develops, and as the general public responds to cybersecurity issues. I encourage you to keep this dialogue going by sharing any insight you have with IATAC and the IA community.

In closing, please join me in congratulating Mr. Robert F. Lentz on his retirement 2 October 2009 with over 34 years of outstanding and faithful public service. In Mr. Lentz's final assignment, he served as Deputy Assistant Secretary of Defense for Information and Identity Assurance. He has been and will continue to be a leader in the greater IA community. ■

Information Assurance (IA) Challenges in an International Environment

by Brian Bottesini



Many *IAnewsletter* readers are probably aware of the challenges of coordination and interoperability among DoD activities. Establishing secure interoperability and coordination among the U.S. Army, Navy, Air Force, and Marine Corps is difficult indeed. Imagine the complexities of establishing secure interoperability among multiple nations' military services, and other governmental and non-governmental departments and agencies. Over the last several years, we have seen a transition from the "need-to-know" to the "need-to-share" information. Due to rapidly changing operational requirements, this information sharing needs to occur more quickly than ever before. The IA challenge is to promote this rapid information sharing in a controlled and secure way.

NATO Past and Present

The North Atlantic Treaty Organization (NATO) was formed in 1949 with a basic principle of collective defense—to safeguard the freedom and security of its member nations. While much has changed since the early beginnings of NATO, this basic principle remains unchanged. Today, NATO has 28 member nations, with Albania and Croatia joining the Alliance in April 2009. In addition to these member nations, NATO has established formal relationships with numerous "partner" nations. NATO provides the structure for political and military consultation on a variety of security issues, to include cyber defense. The senior political decision-making body at NATO is the North Atlantic Council, and the senior military decision-making body at NATO is the NATO Military Committee. In addition, there are many other committees and subcommittees at NATO, including an IA subcommittee.

One of the key challenges at NATO is getting the 28 NATO nations to agree to define, purchase, install, and operate IA technical solutions that are interoperable.

Technical Challenge or Political Challenge?

Most international IA challenges include technical issues, political issues, and operational and policy issues. One of the key challenges at NATO is getting the 28 NATO nations to agree to define, purchase, install, and operate IA technical solutions that are interoperable. It is easy for a senior U.S. military officer to recommend the use of a familiar U.S. crypto product for a NATO operation, for example; however, there are several NATO nations that produce NATO-approved crypto products. Each NATO nation has an interest in secure interoperability as well as ensuring that its national industry has a fair chance of receiving NATO contract awards. NATO promotes the development of common interoperable security protocols and algorithms; however, there are still many security products that are not interoperable. Near-term operational conditions often demand quick solutions and risk management decisions. NATO does its best to provide IA solutions in a timely manner to meet current operational demands. In parallel, NATO also participates in numerous international standards development activities to develop interoperable secure communications standards. Sometimes information sharing or equipment release can be a challenge, especially when national laws or regulations restrict technical data exchange or equipment sales to a foreign country. So, we see that the challenges are both technical and political, with the need to promote broad international interoperability standards and ensure a fair market for each nation's industry, and improved communications interoperability.

161st Chiefs of Defense Meeting at NATO HQ, Brussels, 6 May 09.

NATO and U.S. Expanding Operations in Afghanistan

The U.S. press has provided a lot of coverage of the U.S. operations in Afghanistan. In addition, NATO has a major role in stabilizing the security of the region. NATO's main role in Afghanistan is to assist the Afghan government in exercising and extending its authority and influence across the country, paving the way for reconstruction and effective governance. It does this predominately through its U.N.-mandated International Security Assistance Force (ISAF). [1]

NATO's operations in Afghanistan have gradually expanded to cover most of the regions of the country. There are now approximately 50,000 NATO troops from NATO member nations and NATO partner nations supporting the ISAF mission. Some of these troops are actually U.S. Forces under NATO command. To enhance support for overlapping U.S. and NATO forces in Afghanistan, the U.S.-NATO Information Sharing (UNIS) initiative was established, with the NATO C3 Agency (NC3A) working a variety of collaboration issues to include—

- Development of a common coalition network (Combined Enterprise Regional Information Exchange System [CENTRIXS]-ISAF) bridging U.S. and NATO networks
- Establishment of interfaces linking U.S. Global Command & Control System – Joint with NATO Joint Common Operational Picture
- Creation of a CENTRIXS – Global Counter Terrorist Force to ISAF Secret cross-domain chat capability
- Participation in periodic UNIS Technical Exchange Meetings.

IA is an important element of all these activities, and the NC3A provides important technical and policy support to ensure the accreditation of critical communications and information systems (CIS) installations and network interconnections.

So what's your definition of Coalition?

At the recent Defense Information Systems Agency (DISA) Customer Partnership Conference, the common definition of "coalition" was much narrower than I expected, often referring to a U.S.-led activity with a few select partner nations. Within NATO, a "coalition" can easily include 40 or 50 participating nations, with the lead nation varying within different regions of an area of operation. Imagine the challenges of planning and fielding the CIS and the associated IA security

NATO Secretary General Anders Fogh Rasmussen is welcomed by the Supreme Allied Commander Europe, Admiral James Stavridis.

services within this broader definition of "coalition." To further test modern IA technologies and secure interoperable solutions, NATO actively supports and participates in multinational exercises and demonstrations such as the Coalition Warrior Interoperability Demonstration. It is important that all military planners consider the broadest definition of "coalition" to include multinational military, governmental, and non-governmental organizations when preparing for future operations and exercises.

NATO and Cybersecurity

Among the many challenges faced by NATO, cybersecurity has received a lot of attention. Over the last few years, the NC3A and the NATO CIS Services Agency have been responsible for the development of the NATO Computer Incident Response Center, to include the fielding of a network-based intrusion detection system throughout NATO. In May 2008, NATO officially opened the Cooperative Cyber Defence Centre of Excellence in Estonia. NATO has also recently established a NATO Cyber Defence Management Authority. Heads of state and government recently reiterated their support for cybersecurity with the statement—

"We remain committed to strengthening communication and information systems that are of critical importance to the Alliance against cyber attacks, as state and non-state actors may try to exploit the Alliance's and Allies' growing reliance on these systems."

—NATO Strasbourg / Kehl Summit Declaration, 4 April 2009.

International cooperation in cybersecurity is critical because we know there are no borders in cyberspace. Due to different laws and regulations among NATO nations and partner nations, there are numerous challenges and legal issues to be resolved. Information sharing on cyber defense and cyber offense is especially important in a globally interconnected environment. NATO networks, national networks, and public networks such as the Internet are all interconnected, and all have potential risks. NATO IA experts are continually working to develop and deploy new IA technologies to counter the cyber threat.

The Job is Never Done

IA challenges are greater than ever before. While there has been considerable progress in secure interoperability and IA standards development, we need to ensure that all the traditional security services (*e.g.,* confidentiality, integrity, availability, non-repudiation and authentication) are considered at the earliest phases of a project. Foreign interoperability cannot be easily added on late in a project. It must be engineered in, and policies must be developed and agreed to support automated, yet controlled, information exchange. To address these IA challenges, NATO continues to provide a valuable forum for promoting IA and cybersecurity dialogue among NATO nations and partner nations. ■

References

1. *www.nato.int*

About the Author

Brian Bottesini, CISSP | has 25 years of experience in IA and is currently employed by the NATO C3 Agency in Brussels as a principal scientist within the IA Team. The NATO C3 Agency supports NATO's political and military objectives through the seamless provision of unbiased scientific support and common funded acquisition of Consultation, Command, Control, Communications, Intelligence, Surveillance, and Reconnaissance capabilities. Mr. Bottesini can be contacted at *Brian.Bottesini@nc3a.nato.int.*

Social Networking: Enabler, Drain, or Risk

by Allan Carey

Web sites such as Facebook, LinkedIn, MySpace, YouTube, and Twitter are all part of the social networking genre, which is often referred to as part of the Web 2.0 world. Employees of all ages are engaged in activities with social networking sites, especially the younger generation just entering the workforce. Organizations are struggling to balance employee expectations with workplace etiquette and acceptable behavior. Recently, clients in both the public and private sectors have asked the Institute for Applied Network Security (IANS) about how other organizations are dealing with this issue.

Drafting a social networking policy for your organization can be a political high-wire act. On one side of the equation, social networking sites can be leveraged for legitimate business purposes such as marketing, customer relations, and product development. If used effectively, an organization's public image and market messaging can be conveyed in a controlled fashion to very targeted audiences. Likewise, new product concepts or services can be tested with nearly instantaneous feedback. In these situations or ones similar, social networking sites can be an enabler to business progress.

On the other hand, these sites can be a productivity drain. Employees communicating with people such as friends, family, and online acquaintances for non-work related reasons take away valuable time from tasks and responsibilities that need to be accomplished while on the job. Twitter can be particularly distracting as people "tweet" their every move, thought, and action to their followers.

From a business perspective, social networking sites represent a significant risk that needs to be managed. Numerous vulnerability reports have cited malicious activity originating from places such as Facebook [1] and MySpace, [2] for example. Malicious code can be downloaded onto unsuspecting host machines by visiting certain popular profiles, including celebrities. They also represent an avenue for disclosing information that might be deemed sensitive or inappropriate by an organization. So, from an information leakage standpoint, who in your organization is monitoring your employees LinkedIn profiles or Twitter accounts for improper disclosure? Desktops may be considered locked down, but mobile devices are largely unmanaged.

At this point, most organizations do not have firm grasp of how to tackle this sensitive issue. The full spectrum of decisions has included blocking all sites from corporate resources to allowing all and everything in between. IANS conducted a survey of client organizations last fall.

Employees of all ages are engaged in activities with social networking sites, especially the younger generation just entering the workforce.

Approximately half of those surveyed gave unlimited access to social networking sites. One out of five organizations did not allow access to Facebook, MySpace, or Second Life. When asked about their efforts to make employees aware of Web 2.0-related risks, nearly 60 percent indicated they had no program or effort underway, while 20 percent said they did have a program. In the near future, more must be done by our community to raise the level of awareness of this rapidly growing risk. ■

References

1. *http://infosecurity.us/?p=4928*
2. *http://ftp.cerias.purdue.edu/pub/advisories/ciac/s-fy08/s-160.MySpace.txt*

Information Assurance Integration into U.S. Pacific Command Exercises

by William Romano and Leigh Bender

With the introduction of Cyber as a new military domain, combatant commands (COCOM) have begun to integrate IA in their exercises. The United States Pacific Command (PACOM) has the lead in integrating IA and cyber elements into its exercises. PACOM's tier-one exercise, Terminal Fury, sets the example as the preeminent COCOM exercise with integrated cyber elements within the DoD.

Terminal Fury and other PACOM exercises test and evaluate individual capabilities, multiple functions, and command performances. The exercise is focused on exercising plans, policies, personnel, and procedures on network operations, direction and control, and computer network defense (CND) response and recovery.

A successful training event involves a detailed and integrated scenario with injects and updates that drive decisions and activity. Its objective is to demonstrate capability under operational crisis conditions by presenting complex problems requiring rapid, effective responses by trained personnel in a stressful environment. This article discusses the key elements of successfully integrating IA into PACOM exercises.

Successful IA Integration in Exercises

The sophistication and complexity of IA integration in PACOM exercises started evolving in 2004. One of the keys to successful integration has been the development of the Cyber Cell. The Cyber Cell's focus is to ensure that the cyber events are realistic and credible. Keeping the events realistic provides the training audience with an enemy cyber threat that simulates—

- Worldwide presence
- Significant nation state resources
- Mature operational tradecraft
- Diverse networks of trusted partners
- Diverse networks of untrusted partners
- Worldwide secure communications and logistics
- Integration of human and technical operations
- Effective security programs
- Integration of offensive and defensive elements.

To make the exercise effective, the enemy cyber threat is continuously on the offense and has the ability to choose the time, place, and method of attack; it attacks the target's weakest point and seeks to exploit and maintain network presence.

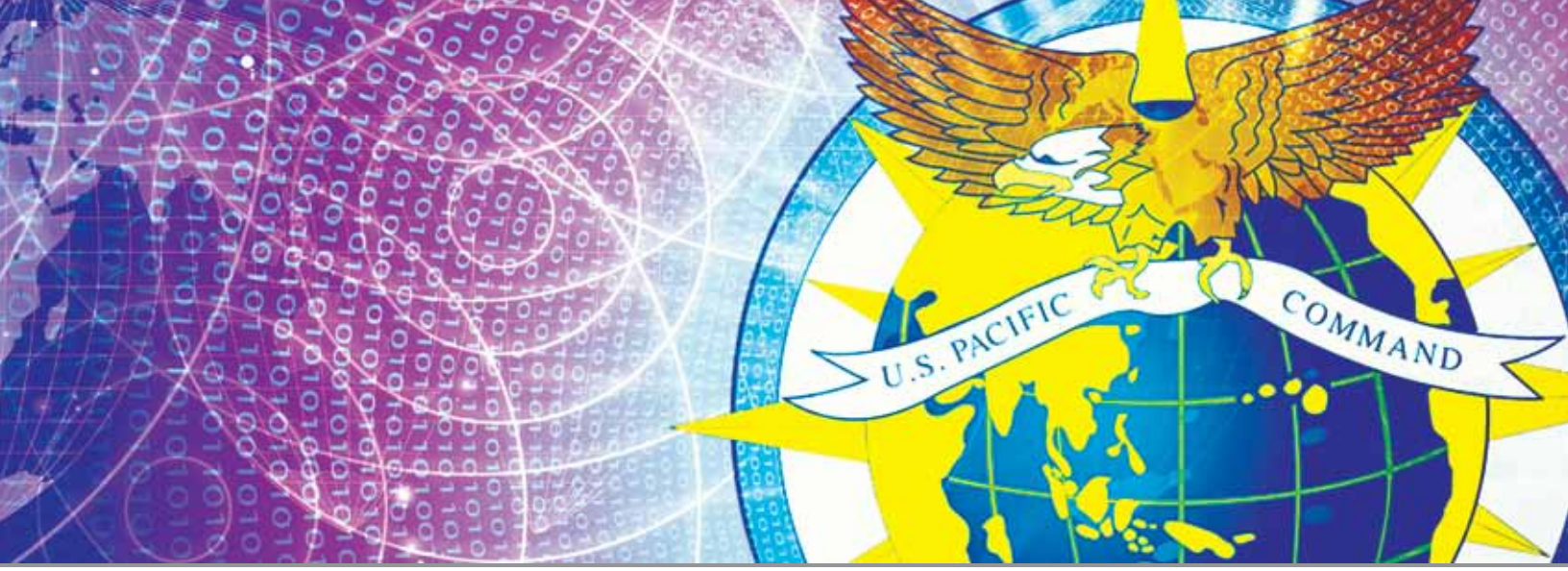
As the enemy cyber threat conducts its attack, the training audience's ultimate IA training objectives are to—

- Increase the probability of detecting a component behaving badly
- Increase the probability of attributing the bad behavior to the adversary
- Decrease the impact of a defensive failure
- Decrease inherent vulnerabilities within hardware and software
- Increase the ability to deeply evaluate and assess critical components and, using trends and analysis, predict future actions
- Increase the coupling of offensive and defensive elements
- Increase PACOM insight into the offensive information operations capabilities and intentions of our adversaries.

These enemy cyber threat simulations and training audience objectives are the essential elements to successfully integrating IA into COCOM exercises.

Successful Planning and Assessment of IA Exercises

The Joint Exercise Life Cycle (JELC) is a cyclical process that ensures all training objectives are accounted for during the planning process (Figure 1). It begins with the Concept Development Conference (CDC) and the Training Objective Workshop (TOW). At this stage, planners develop the initial ideas for the exercise and capture the relevant training objectives from the different elements of the training audience. The exercise scenario is then developed and refined through the Initial Planning Conference (IPC), Middle Planning



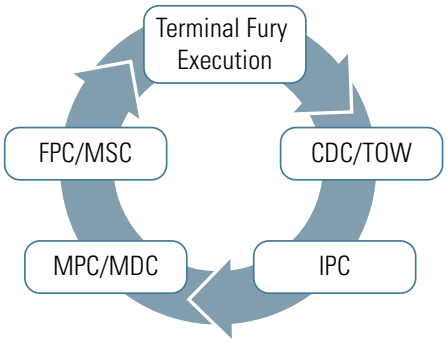


Figure 1 Joint Exercise Life Cycle Process

Conference (MPC), Master Scenario Events List (MSEL) Development Conference (MDC), MSEL Synch Conference (MSC), and Final Planning Conference (FPC).

Cyber planning starts at the CDC, during which the type and tempo of cyber activity is discussed. Then specific events are constructed to support the overall storyline at the IPC and MPC. By the end of the MPC, the cyber storyline is defined and the detail work begins. Table 1 breaks down the different elements of the JELC and lists some of the key information required and developed at each stage.

An IA assessment runs concurrently with the JELC. The assessment team visits the COCOM and conducts an IA assessment with the exercise. Its goal is to collect all relevant data on the training audience's responses to the Cyber MSELs so that the COCOM can improve upon its IA weaknesses.

Exercise Conference	Description	Timing	Key Participants
Concept Development Conference	▸ Develop Conceptual Framework (including purpose, duration) ▸ Develop key exercise assumptions, artificialities, and simulations ▸ Develop scenario narrative, provide initial exercise objectives	10 To 11 Months Prior To Exercise	Cyber Cell Lead and PACOM Training Audience Lead
Training Objective Workshop	▸ Draft exercise objectives and scenario ▸ Identify the scope and concept of play for the training audience ▸ Coordinate levels of training audience participation	9 To 10 Months Prior To Exercise	Cyber Cell Lead, And Training Audience Leads
Initial Planning Conference	▸ Confirm exercise dates ▸ Review of Training objectives ▸ Development of Cyber scenario ▸ Initial identification of resources	8 Months Prior To Exercise	Cyber Cell Lead, Training Audience Leads, National Intel Leads
Middle Planning Conference	▸ Conduct in-progress review of planning actions ▸ Make course corrections to ensure objectives are attained	4 To 5 Months Prior To Exercise	Cyber Cell Lead, Training Audience Leads, National Intel Leads
MSEL Development Conference	▸ Develop chronological list of scenario events and injects ▸ Synopsis of key events and expected responses ▸ Generate activity in specific functional areas to drive demonstration of objectives ▸ Draft Cyber Master Scenario Events Lists (MSEL)	Immediately Following Middle Planning Conference	Cyber Cell Lead, National Intel Leads
Final Planning Conference	▸ Review all planning actions ▸ Final cross cell coordination ▸ Selection of Joint Exercise Control Group white cell members ▸ Development of Joint Exercise Control Group (JECG) organization, structure and Process and Procedures ▸ Review of all MSELs	3 Months Prior To Exercise	Cyber Cell Lead, National Intel Leads
MSEL Synch Conference	▸ Final Synchronization of all MSELs	Immediately Following Final Planning Conference	Cyber Cell Lead, National Intel Leads

Table 1 Joint Exercise Life Cycle Stages

Key Components of a Successful IA Exercise

The Joint Exercise Control Group (JECG) is the exercise control and coordination group, and it is responsible for the orchestration of the entire event. The group consists of subject matter experts in the political, military, and civil components represented in the exercise. The modeling and simulation control for the exercise is controlled by the JECG. The Cyber Cell is also part of the greater

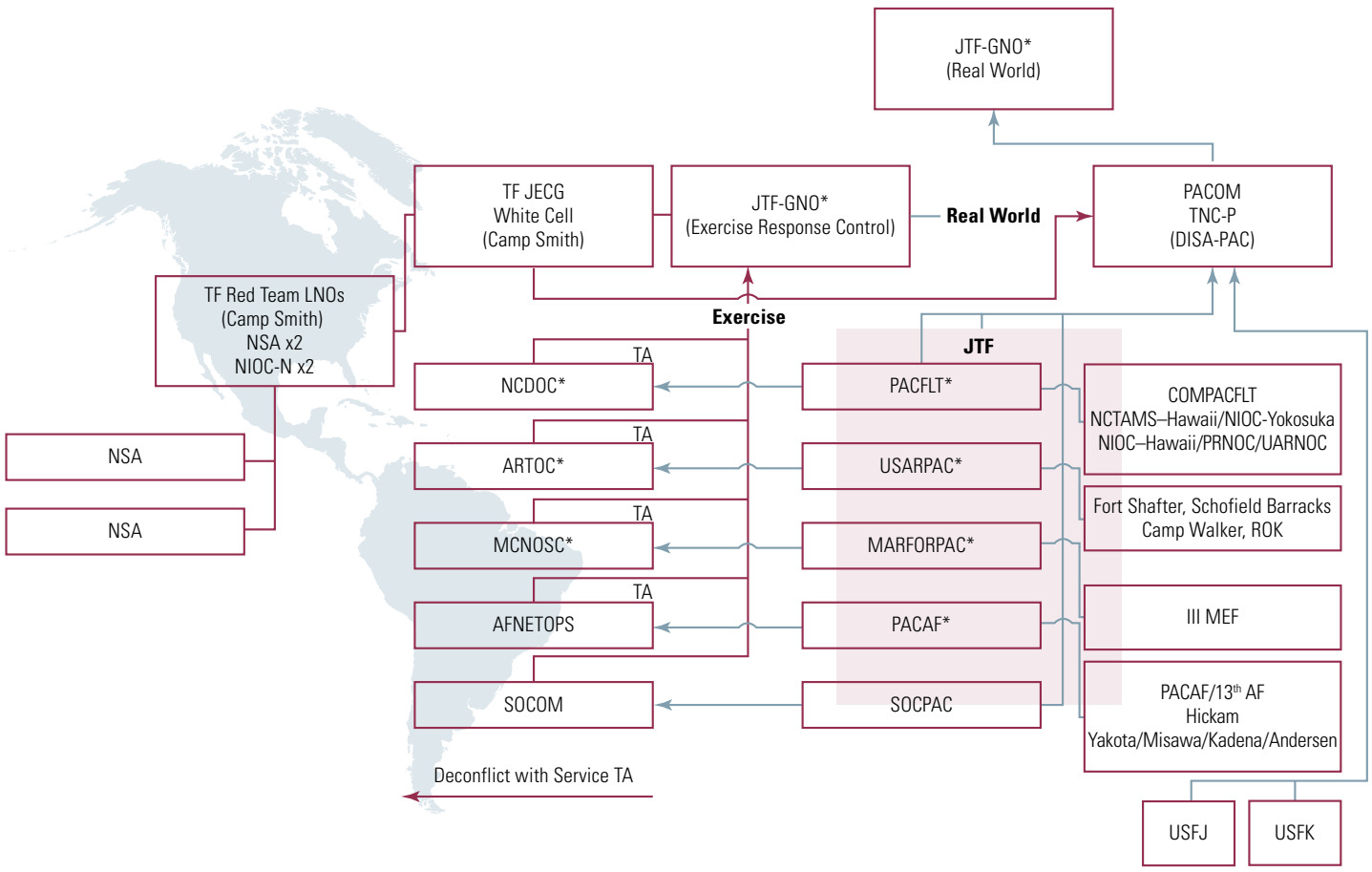


Figure 2 Terminal Fury Cyber De-Confliction Information Flow

JECG. It is this cell that controls all the planned cyber activity during the exercise.

The Cyber Cell is headed by the cell lead whose role is to serve as the subject matter expert and single point of contact on all matters relating to cyber play. The cell also has a number of other support personnel to assist the cell lead. Primarily, these are CND and IA experts. In Terminal Fury, for example, there are several CND/IA experts representing several different CND/IA organizations, such as Defense Information Systems Agency, Joint Task Force–Global Network Operations (JTF-GNO), and Joint Functional Component Command–Network Warfare (JFCC-NW).

Other cell personnel in the Cyber Cell include an enemy cyber threat representative whose responsibility is to coordinate the use of information gathered during the execution of Cyber MSELs. An assessment team data collector is also embedded in the Cyber Cell to collect information for the exercise assessment report.

Successful IA Processes and Procedures

The Cyber Cell chief must act as the nucleus of information flow to the training audience. He facilitates all communication between the Cyber Cell chief and cyber role players. Effective communication between related cells requires all role players to keep the Cyber Cell chief informed of all actions.

Another key process in the Cyber Cell is measuring effects of the Master Scenario Events on the training audience. This is handled primarily by the role players who communicate with their trusted agents embedded with the training audience or by shadowing the training audience daily meetings. Because cyber effects cannot be gauged by any modeling and simulation tools, it is crucial for the Cyber Cell chief and the role players to constantly keep track of training audience actions *via* all means available.

De-confliction, or the resolution of whether cyber activity is actual activity or exercise-related, is a crucial role of the Red Team, which is also a part of the Cyber Cell. Figure 2 illustrates the de-confliction lines of communication used during the exercise. It is important that exercise information is conveyed to the correct reporting node and de-conflicted as exercise play. It is just as important to ensure that real-world incidents are not mistakenly attributed as exercise activity and are reported through the correct channels.

MSEL synchronization is equally important to Red Team de-confliction procedures. This process occurs two times daily in the JECG. Representatives from every response cell come together to review all the upcoming events in the exercise for the next 12 to 24 hours. This allows the entire control group to maintain awareness of the activities that all the other response cells are planning. This ensures that one cell's planned activities will not have an adverse effect on another cell's planned activities. It also provides an opportunity for activities planned by one cell to be used by another.

During this process, the group painstakingly reviews each planned event. The group ensures all the required information is present and is aligned with the overall exercise scenario. Furthermore, the group follows the guidance put forth by the exercise director. The MSEL sync sessions are the key component to making sure the exercise does not go awry. It is also a good venue to gather feedback on the effects of certain cyber aspects of the exercise. Based on previously executed cyber events, the number and types of MSELs planned by other cells can change. A robust training environment for the training audience is the overarching goal of MSEL synchronization.

Throughout the exercise life cycle, cyber planners also interact with a number of external agencies, including JTF-GNO, JFCC-NW, Defense Intelligence Agency, and National Security Agency Threat Operations Center. The objectives are to create plans that replicate the organizations' missions, and provide the training audience with realistic responses.

Providing Constructive Feedback

When the exercise is complete, the training audience needs feedback on its performance. This is conducted through several venues.

The first is the post-exercise cyber hot wash. Held immediately following an exercise, a hot wash is a facilitated discussion among exercise players from each functional area. It is designed to capture feedback about any issues, concerns, or proposed improvements. The hot wash is an opportunity for players to voice their opinions about the exercise and their own performance. This facilitated meeting allows players to participate in a self-assessment of the exercise play and provides a general assessment of how the entity performed in the exercise. At this time, evaluators can also seek clarification on certain actions and what prompted players to take them. PACOM typically conducts hot washes within four hours of the end of the exercise to maximize its training value.

The hot wash allows the training audience to envision how disparate events were, in fact, part of a holistic picture. This often has the effect of an "Aha" moment among members of the training audience. During the hot wash, the IA assessment team provides a short summary of the findings and correlations of the data gathered though the exercise. This is in the form of DoD 8500 metrics, observed reactions to cyber events, and information on network status gained from technical vulnerability assessments. This also reviews the specific exercise findings and provides recommendations for IA improvements.

Conclusion

Integrating information assurance into COCOM exercises is essential to ensuring our warfighters know how to respond to cyber attacks. Though the planning and coordination processes are extensive, providing training audiences with the constructive criticism necessary to improve their responses to cyber events is critical to national security. PACOM, through Terminal Fury and other IA exercises, is proof that well-conducted IA exercises improve mission-essential skills, processes, and procedures for cyber warfare. ■

About the Authors

William Romano | received a BA degree in sociology from the University of San Francisco, and an MA degree in management from Central Michigan University. He is currently the team lead for the DoDIIS/DS International Information Systems Office Coalition Network Communications Architecture Survey and Validation task and is providing exercise planning analysis to USPACOM J63 for Exercise Planning. He is also the team lead for the USPACOM J6, which supports its Information Assurance, Certification and Accreditation, and Cyber Fusion programs. He has also supported the USPACOM J1 and J05 Critical Infrastructure Protection Program. Mr. Romano can be reached at *iatac@dtic.mil.*

Leigh Bender | received a BS degree in electrical engineering from Old Dominion University and received MBA and MS degrees in information systems from Hawaii Pacific University. He is the cyber exercise planner for PACOM, supporting the J6 Communications Directorate and the J39 Information Operations Division. Mr. Bender also coordinates the IA and Interoperability assessment for the Office of the Secretary of Defense at PACOM. Prior to this role, Mr. Bender served as the team lead for the PACOM Modeling, Simulation, and C4I exercise support team. Mr. Bender can be reached at *iatac@dtic.mil.*

DoD Certifies the Power of Partnership

by W. Hord Tipton

Five years ago, the DoD officially unveiled Directive 8570.1, Information Assurance Workforce Improvement Program, a program that requires every one of its information security employees to receive a professional certification that is accredited under the global American National Standards Institute (ANSI)/ Industry Standards Organization (ISO)/ International Electrotechnical Commission (IEC) Standard 17024. This mandate was undertaken in pursuit of one clear goal: to ensure that the right people with the right skills are matched to the right job in the right environment.

The DoD's action and goals were quickly lauded by both the defense and information security communities because, among other things, it validated the need for a well-trained, professionalized information security workforce to guard effectively against emerging threats and identified it as a critical and distinct profession.

The program, however, presented an immediate logistical challenge because, as planned, the Directive required that nearly 100,000 personnel had to be identified and trained and then successfully pass a commercial certification exam—all during an ambitious four-year implementation phase. In addition, the DoD needed a way to effectively keep track of who received what certification and whether those personnel were adhering to their credential's maintenance conditions, including continuing education requirements.

Fortunately, those challenges are being met, and the 8570.1 program implementation is making steady progress. This is due in large part to a unique relationship that exists between officials within the Defense-wide Information Assurance Program (DIAP) and the commercial (*i.e.,* non-government) certification industry, including my organization, (ISC)².

This cooperative arrangement is not just a standalone exercise. It offers plenty of lessons for other federal agencies and even foreign governments that are considering implementing their own enterprise-wide mandates for a professionalized information security workforce.

A Cooperative Effort

The DoD's decision to rely on commercial ANSI-approved certifications was a real breakthrough in public/private collaboration. DoD officials could have developed their own unique certification program, as the agency has historically done in other job categories. Ultimately, they chose a very different—and much more effective and efficient—course.

By leveraging existing accredited information security credentials, the DoD could not only save time, money, and administrative headaches, but it could also piggyback off years of benchmarking, research, curriculum, and standards development already performed by certification organizations who are widely respected by private companies and governments around the world.

Moreover, the decision gives DoD employees a highly recognized professional credential that belongs to them. They can take it with them if they retire or transfer to another agency, and they can enjoy the networking and professional benefits that come with being part of an elite community of information security professionals. In (ISC)²'s case, there are more than 63,000 information security professionals that hold our Certified Information Systems Security Professional (CISSP®) credential, and thousands more who have obtained our other certifications.

Cooperation between DIAP, (ISC)², and the information security certification industry occurred from the very beginning, when DoD officials first began laying the groundwork for its initiative. They hosted a series of meetings with certification organizations, including (ISC)², to gather input on how to structure the program; to identify which certifications should be included in the program and by what criteria; and to identify what kind of assurance the certification organizations could provide to ensure the certifications would meet DoD's unique and long-term needs.

One major discussion centered around which independent third-party

should review and validate the certifications. (ISC)² strongly supported the requirement that all certifications be accredited under the global ANSI/ISO/IEC Standard 17024, a then brand-new international accreditation that was designed to provide a way to assess the quality of certifications provided to personnel who perform a service—a certification for the certifier, if you will. The evaluation and accreditation process involved with Standard 17024 is particularly rigorous. It can take months to complete and requires an organization to answer hard questions about its certification process, practice, and ethics. Organizations then have to undergo an annual audit and reapply every five years.

By using certifications accredited under the ISO Standard 17024, DoD officials could rest assured their program was backed by a rigorous standard that would—

- Eliminate consistency issues and problems caused by too many unregulated, unrecognized qualifications
- Provide a metric that can be easily and reliably measured
- Reduce the language disparity between those who determine and write information security policy and those who implement it
- Create professional pride through the recognition of an accepted global standard
- Provide intangible benefits, such as renewed motivation, diligence, and leadership.

The evaluation and accreditation process involved with Standard 17024 is particularly rigorous. It can take months to complete and requires an organization to answer hard questions about its certification process, practice, and ethics.

Certification organizations also benefited when DoD agreed to utilize the ISO Standard 17024. The decision ensured that the large investment certification organizations would have to make to certify their credentials was for a widely recognized international standard, thereby strengthening the professionalism of the information security industry.

Shortly thereafter, (ISC)² submitted the CISSP certification for ISO Standard 17024 evaluation and accreditation. In 2004, it became the first information security credential to be accredited under the global ISO Standard 17024, and in 2006, the first credential to be approved by the DoD for use under Directive 8570.1.

Since then, several more of our certifications have successfully gone through the accreditation process and now qualify under the 8570.1 program. They are the Systems Security Certified Professional (SSCP®); the Information Security Systems Management Professional (ISSMP®); the Information Systems Security Architecture Professional (ISSAP®); and the Information Systems Security Engineering Professional (ISSEP®), a credential developed with the National Security Agency to establish an additional level of knowledge and expertise unique to U.S. national security employees and contractors. This summer, our Certification and Accreditation Professional (CAP®) credential will also be an approved credential for DoD personnel.

The DoD later added to its program a matrix of different categories, each outlining different roles and

responsibilities and qualifying credentials. Managers, for example, must obtain a certification that meets the requirements outlined under the three levels of the Information Assurance Management category and level 3 of the Information Assurance Technical (IAT) category. Pursuing the CISSP certification, in that case, would enable the manager to meet the 8570.1 requirement. An information security technician could obtain the SSCP, which satisfies IAT levels 1 and 2.

Moving Forward

After DoD released its 8570.1 manual, (ISC)² developed educational materials that summed up and explained the goals and requirements of the program to DoD personnel, including a Frequently Asked Questions document and a fact sheet. We also created programs that help the DoD meet its ambitious goals.

We created and launched the (ISC)² eLearning educational program, which offers self-paced lectures and exercises. This is especially important for DoD employees, who sometimes have irregular schedules or are stationed in remote areas. We have also just begun offering Web-based seminars with live instructors, which is the same instruction offered in our five-day, full-time, classroom-based CBK® Review Seminars, but spread out over 10 weeks. Both of these programs enable candidates to partake in a review session—whether they are on a Navy ship or work extra-long hours at the Pentagon.

A key best practice that the DoD has recognized in this process is the need for self-assessment tools. Officials first asked us about the possibility of a self-assessment program after some of the earliest certification candidates under the 8570.1 program experienced a higher failure rate.

DoD did not need to incur the higher costs associated with paying for numerous exam tries and re-tries, so we came up with the StudISCope Self Assessment. This online tool allows candidates to experience a simulation of the official CISSP and SSCP certification exams. Afterward, the program not only scores the exam but analyzes the answers for knowledge gaps and prepares a personalized study plan that highlights the areas in which a candidate performs well—and where they need to closely target their studies.

The program also provides a Readiness Gauge to give candidates a sense of their knowledge status for sitting for the full exam. In the case of the Navy, candidates must pass their self-assessment before they are allowed to take an official certification exam.

In addition to our online efforts, (ISC)² tries to be as flexible as possible in providing instructor-led reviews and examinations for DoD personnel. Pools of at least 12 candidates can arrange for (ISC)² to provide a dedicated CBK Review Seminar or exam at their location, for example. And, of course, we always work to help any DoD employee who is ready to move forward with certification locate the closest public exam.

On the administrative side, (ISC)² personnel are in daily contact with the DIAP office to answer their questions or meet whatever needs they have. Through a mutually developed, automated process, we validate the certifications of about 50 personnel submitted twice a week by the DoD and can directly indicate in a DoD database whether or not each candidate on the list is (or is not) certified. We are also a participant in the U.S. Defense Activity for Non Traditional Education Support (DANTES) Program, which reimburses DoD personnel in the Army National Guard, Army Reserve, and Air Force Reserve for certification exam costs. Many of our exams, in fact, are offered at DANTES testing centers.

In summary, this unique relationship is working, and it has a larger significance for the information security community. At a minimum, DoD's attention to this effort—and its decision to collaborate with the commercial certification industry—has helped government organizations around the world recognize that they, too, need to invest in their information security workforce. The question remains as to whether or not the rest of government will mandate its information security personnel to obtain a professional certification. As the 8570.1 program continues to successfully move forward, the rest of the information security world will be waiting to hear the answer. ■

At a minimum, DoD's attention to this effort—and its decision to collaborate with the commercial certification industry—has helped government organizations around the world recognize that they, too, need to invest in their information security workforce.

About the Author

W. Hord Tipton | is currently the executive director for (ISC)², the not-for-profit global leader in information security education and certification. Tipton previously served as chief information officer for the U.S. Department of the Interior for over five years. He is CISSP-ISSEP, CAP, and CISA certified. Mr. Tipton can be reached at *hord.tipton@isc2.org*.

The University of Washington

by Angela Orebaugh

Founded in 1861, the University of Washington (UW) is one of the oldest state-supported institutions of higher education on the West Coast and is one of the preeminent research universities in the world. The University offers over 250 degrees within 150 departments programs across 18 colleges and schools. UW currently employs over 4,100 full-time faculty members and has over 47,000 students.

UW's Information School (iSchool) offers a BS in informatics, MS in information management, and PhD in information science. [1] Each of these programs offers studies in information assurance and security (IA&S).

As a National Security Agency-designated Center of Academic Excellence (CAE) in IA education, UW offers certificates, courses, and programs in IA&S, including the following—

- IA & cybersecurity [*2*]
- IT security [*3*]
- Information systems security [*4*]
- Digital forensics [*5*]
- Electronic discover management. [6]

Faculty and staff working in the area of IA&S collaborate with stakeholders from industry, government agencies, and academia to conduct basic research and develop cross-campus undergraduate and graduate educational programs. UW IA&S research strives to identify, address, and promote interdisciplinary solutions and act as a catalyst for innovation and increased public awareness.

UW's Center for Information Assurance and Cybersecurity (CIAC) provides a Pacific Northwest forum for the collaboration of professors, professionals, industries, and students. The mission of the center is to identify, address, and promote visions and solutions for IA and cybersecurity issues. The center will produce and be a catalyst for research, invention, innovation, education, public awareness, entrepreneurship, and economic growth in the state of Washington. [7]

CIAC hosts the annual Pacific Rim Regional Collegiate Cyber Defense Competition (CCDC), which provides institutions with an IA or computer security curriculum—a controlled competitive environment to assess their students' depth of understanding and operational competency in managing the challenges inherent in protecting an enterprise network infrastructure and business information systems. In this competition, student teams are presented with pre-configured systems of a fictitious company that they are tasked to operate. A red team attempts to vandalize and break into this network, while student teams need to defend against the attacks of this red team. The team with the most points at the end of the two-day event will be the winner of the Pacific Rim Regional CCDC and will proceed to the national competition.

UW's Institute for National Security Education and Research (INSER) provides a forum for independent research and cutting-edge scholarships in areas with broad relevance to public safety and national security issues, including distributed collaboration in virtual organizations and knowledge management and decision making. [8] INSER is one of the nation's 10 Intelligence Community (IC) CAEs established by the Office of the Director of National Intelligence. The IC CAEs were established to promote the alignment of curricula (*e.g.*, scientific and technical programs of study, international relations) necessary to develop core skills relevant to the intelligence community. In its role as an IC CAE, INSER coordinates research and education for more than a dozen well-recognized experts, including UW faculty in a number of disciplines. ■

References

1. *http://www.ischool.washington.edu/*
2. *http://www.outreach.washington.edu/ext/certificates/inf/inf_gen.asp*
3. *http://www.tacoma.washington.edu/pdc/schedule/IT_security.html*
4. *http://www.extension.washington.edu/ext/certificates/iss/iss_gen.asp*
5. *http://www.extension.washington.edu/ext/certificates/cpf/cpf_gen.asp*
6. *http://www.extension.washington.edu/ext/certificates/edm/edm_gen.asp*
7. *http://ciac.ischool.washington.edu/*
8. *http://cluster.ischool.washington.edu/caenser/*

Developing an Effective Data Breach Response Program

by Kathryn Maginnis

"The person who stole my identity did not know me. She did not know my age or mother's maiden name. She did not know my driver's license number. She did not even know what I looked like. (In fact, she changed all these statistics to match her own.) All this person knew who stole my identity was my Social Security number. Having my identity stolen and recovering my identity was traumatic, scary, and surreal. I felt like I was victimized once by the perpetrator and again by the system."

"Selene" delivered this testimony in June 2000 to the California State Assembly. Such incidents were relatively new then, but with the growing proliferation of Internet users and hackers, data breaches are now far too common. And the computers themselves are vulnerable to loss or theft.

The government keeps electronic records of millions of people, including their Social Security numbers, across multiple agencies. This data is potentially subject to breaches due to loss or theft. Although the U.S. Department of Veterans Affairs (VA) makes information protection a high priority, data breaches can still occur, either accidentally or intentionally.

Data security and privacy challenges are becoming more complex. VA is partnering with the Department of Defense (DoD) and has established the VA/DoD Health Information Sharing Directorate to directly support the VA mission and efforts to promote quality health care for Veterans and eligible service members, including National Guard soldiers and reservists.

The VA/DoD Health Information Sharing effort was launched in 2000 and elevated to full Directorate status in May 2004. The Directorate recently announced its continuing efforts to pursue a joint lifetime electronic heath and benefits record for service members, Veterans, and their families. That's because many soldiers, sailors, and airmen returning from overseas seek treatment at both VA and DoD facilities after serving their country. For more information, visit: *http://www1.va.gov/VADoDHealthITSharing/*

VA by the Numbers

- 278,000+ employees
- 23.4 million Veterans
- 1,600+ facilities—such as medical centers, outpatient clinics, benefits offices, and data centers

Incident Response Data

VA is proud of the robust Incident Response Program it has established.
Here are data showing the sheer volume of incidents managed—

- Data security and privacy incidents—More than 5,000 incidents were dealt with in 2008.
- Approximately 20,000 offers for credit protection services to mitigate possible data exposure.

What Happened in 2006

Many will remember the well-publicized incident in 2006 of a stolen VA laptop. In response to this occurrence, VA formally organized a dedicated Incident Resolution Team (IRT). The VA Office of Risk Management and Incident Response (RMIR) now uses a four-step incident response process as part of the program—

1. **Report**—VA employee reports incident to appropriate VA personnel –Information Security Officers (ISO) and Privacy Officers (PO), who enter them into VA's national reporting systems for tracking.
2. **Assess**—VA's IRT triages incidents based upon accepted severity criteria and escalates significant occurrences to the Chief Information Officer and VA senior management, including the VA Secretary.
3. **Resolve**—VA determines the severity of the breach and coordinates the resolution among VA business partners. This may include an offer of credit monitoring or the escalation of remediation efforts that are affecting patient care.
4. **Communicate**—Significant incidents are reported daily to the VA Secretary and a monthly and quarterly summary are provided to Congress.

The Office of Information Protection and Risk Management, of which RMIR is a part, has a mission to serve Veterans by ensuring the confidentiality, integrity, and availability of VA sensitive information and information systems.

VA focused its efforts on securing data at rest and in transit by mandating the encryption of all data on laptops and VA-issued thumb drives that retained VA data.

VA also developed an identity safety program to provide prompt and accurate notification and remediation to Veterans and their families whose personally identifiable information (PII) or personal health information (PHI) is compromised. Credit monitoring and protection service contracts have been in use since 2006. This allows VA to quickly remediate the potential adverse effects of data breaches by offering affected individuals the opportunity to opt-in to this service.

In the case of the 2006 laptop theft, notification letters were sent to Veterans and their spouses whose information was on the missing computer. Fortunately, when the laptop was recovered, the Federal Bureau of Investigation's computer forensics revealed that the data had not been compromised.

VA wants to achieve the "gold standard" in information protection for those who served our country. VA has aggressively and effectively developed processes to manage, monitor, mitigate suspected or verified data breaches.

Lessons Learned

- **Situational Awareness is Key**—Tools and technologies for incident monitoring and conducting analysis are essential to understanding the causal factors.
- **Put Business Processes in Place**—All data breaches cannot be prevented, but they can be anticipated. Having policies, processes, and personnel in place to report and respond to the breach enables the organization to respond optimally.
- **Hire Diverse Skill Sets**—Incident response teams need to have a broad organizational understanding and a variety of expertise to response to a wide range of data breach incidents and to creatively meet challenges. At VA, this means expertise in health care, information technology, information security, privacy laws, and project management.
- **Communicate with Employees** — Everyone in VA plays a role in information protection. Keeping employees informed about new developments in information protection helps everyone, especially Veterans. Talking to people one-on-one is the most effective communication method.
- **Train and Re-train Employees**—Cultural shifts and awareness do not happen overnight. Stay committed to providing training to end users and encourage information sharing.

  For example, one VA training initiative is a DVD titled *Incident Response and What You Need to Know*. Another training method VA uses with employees is the annual Information Protection (IP) Awareness Week, with the recent theme of "Information Protection Starts with 'I'."

  ISOs and POs across VA participated by conducting interactive events, creating displays, and managing booths at local facilities. Not only does this raise overall information protection awareness, but it serves to introduce ISOs and POs to local staff. IP Awareness Week also highlights the role ISOs and POs play every day in protecting information.

- **Notify Leaders Promptly**—Local VA facilities are required to report data breaches to the security operations centers within an hour of discovery. Operation centers are staffed 24 hours per day.

Figure 1 The VA Incident Response Tracking System (VIRTS) is a situational awareness dashboard that incorporates the use of a geographical information system to visually represent reported incidents.

- **Build Effective Relationships**—Trust and mutual understanding with those in the field comes in handy during a crisis.

Implementing Technologies

Our "Lessons Learned" list includes developing and implementing the technology tools that will foster better incident responses. One tool now in use is the VA-developed Formal Event Review and Evaluation Tool (FERET) that assigns one of three level-of-risk scores to incidents based on responses to an automated questionnaire. The FERET risk assessment tool, and other determining factors, assist VA's IRT in determining the appropriate mitigation response for the risk level.

The VA Incident Response Tracking System (VIRTS) is a situational awareness dashboard that incorporates the use of a geographical information system to visually represent reported incidents (see Figure 1). This capability will provide key management stakeholders with near real-time awareness of events.

VIRTS is composed of two parts: a case management tool and an executive dashboard. The case management tool will support the day-to-day triaging, tracking, and reporting of incidents, while the dashboard will provide situational awareness and performance reporting to VA's Chief Information Officer and executives.

Looking Forward

VA's 2006 stolen laptop incident was a definite wake-up call. Because of it, VA is now in a much stronger information protection position and ready to share our lessons learned with others. I told a recent audience at the Federal Office Systems Exposition (FOSE) that through collecting and sharing "lessons learned," VA is able to continuously improve its own programs and help other organizations with similar missions.

In April 2009, President Barack Obama, Veterans Affairs Secretary Eric Shinseki, and Defense Secretary Robert Gates announced they had taken the first step in creating a Joint Virtual Lifetime Electronic Record—a comprehensive system that allows the streamlined transition of health care records between the DoD and VA.

With the two largest health care providers in the nation setting standards of interoperability as a model for all of American healthcare information technology, the implications for information protection are immense. Security and privacy issues are becoming more complicated as we move forward with sharing medical information electronically.

VA is proud to be on the leading edge of information protection, as the need for privacy and security is extremely important to protect the medical information of Veterans and ultimately all Americans. We are geared up for the challenge and excited to be an integral part of this effort by sharing what we have learned. ■

About the Authors

Kathryn Maginnis | became the first VA Associate Deputy Assistant Secretary for Risk Management and Incident Response (RMIR) in the Office of Information and Technology in April 2007. Prior to taking on this new role, she had a long and successful career in the Veterans Health Administration. Ms. Maginnis is credited with creating VA's first IRT to continuously monitor and assess all privacy and security breaches throughout VA. She became a member of the Senior Executive Service in 2001. Ms. Maginnis holds an MBA, and is a Certified Information Privacy Professional and a Fellow of the American College of Healthcare Executives. She may be reached at *kathryn.maginnis@va.gov.*

DoDTechipedia Happenings

by Rogelio Raymond

A computer scientist working for the Department of Justice is completing a three-year research project on the effects of malware on government computer networks. On the other side of the country, an IA analyst at the United States Northern Command is contemplating conducting a similar study. How can two individuals within two government organizations that traditionally do not cross-communicate share their intentions and knowledge? DoDTechipedia is the solution!

DoDTechipedia can help the computer scientist and the IA analyst connect for a common cause. Browse the recently updated DoDTechipedia pages on malware and Conficker under the Information Assurance technology focus area. They are both excellent starting points for not only understanding what the current malware threats are in cyberspace, but also to connect with other IT professionals. The Malware page reviews the history and lists the most common recognized types of malware. The page features external links to malware removal guides and tutorials that assist with removal of specific malware types by name and description. There is also an external link to an exclusive malware wiki for those who are passionate about understanding and discussing vulnerability issues.

There is a recently added Conficker subpage attached to the Malware page. As most IT professionals know, the Conficker worm gained international notoriety for infecting an estimated 8.9 million computers worldwide. The subpage identifies the primary known variations as well as profiles of each. There are several external links to additional resources in understanding and combating Conficker. Both pages are still wide open for expansion through content or subpages. Users who are part of organizations that deal with IA are encouraged to link their organization pages to these two pages.

Be sure to browse though the Information Assurance and Information Warfare Technology blog areas for blurbs on malware and Conficker in current events. Feel free to add comments and links to other current events articles online. Don't hesitate to contact IATAC about acquiring blogger administration rights if you are a subject matter expert.

With the addition of blog and Common Access Card login capability, DoDTechipedia is an excellent place to share both unclassified and For Official Use Only scientific and technology program information/data both safely and securely. The sky is the limit regarding where sharing and collaboration can take us. After all, no one organization is above the knowledge of all organizations together. Connect with the scientific community to share information and ideas. Let's make the IA and Research & Development communities stronger! ■

DoDTechipedia can help the computer scientist and the IA analyst connect for a common cause.

There are other pages, such as the Information Assurance Technology Focus area page on the National Vulnerability Database, that can augment the research and knowledge base of malware with its link to lists of known government computer network system and hardware flaws that could render them vulnerable to known malware, or the Information Security Automation Program page that focuses on government standards of implementing uniform information systems security protocols that can protect systems from known malware.

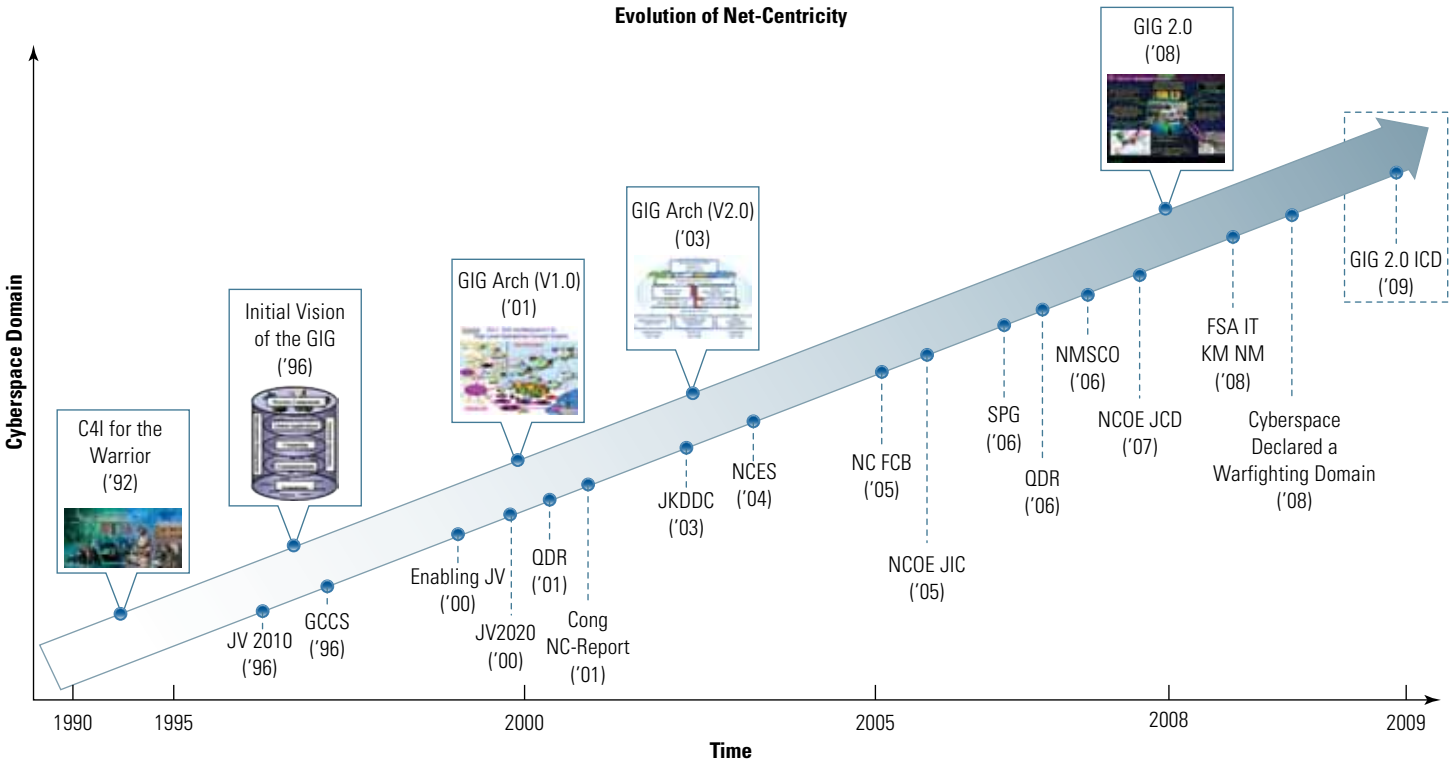
Global Information Grid 2.0: An Enabler of Joint/Coalition Warfighting

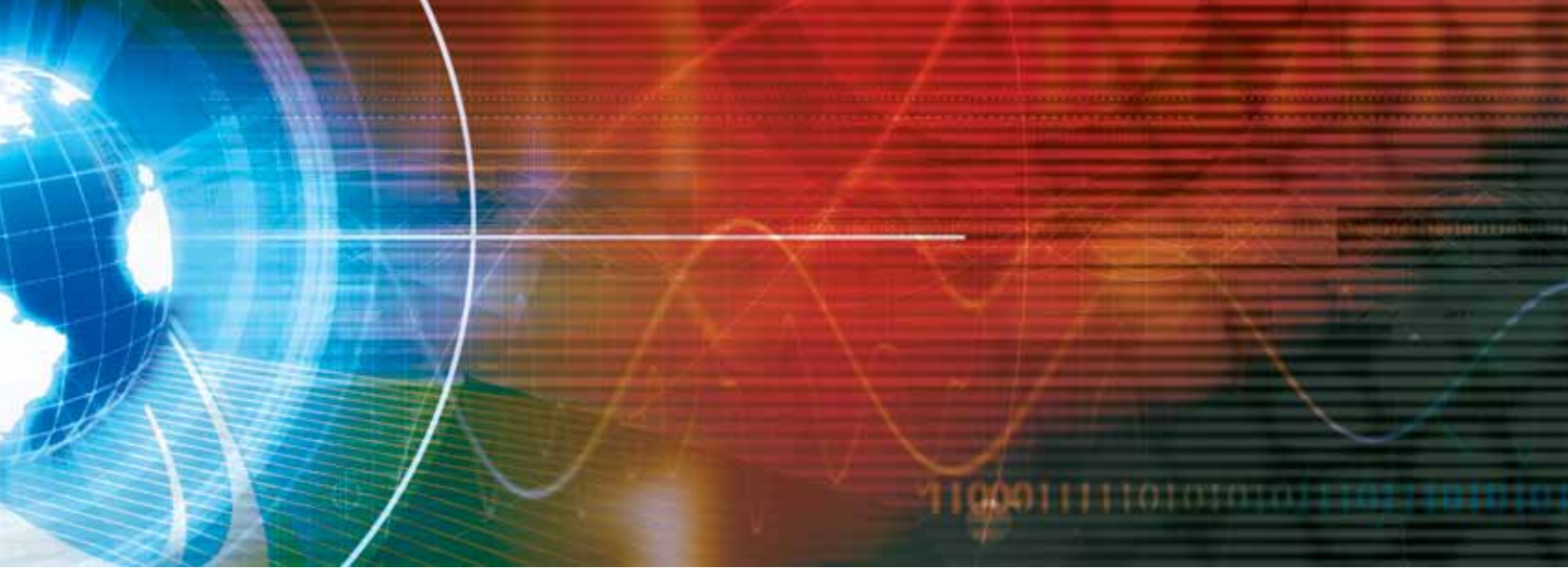
by VADM Nancy Brown

Background/Vision

In the early 1990s, there was an effort to develop information superiority in order to enable combat power across the spectrum of operations. As shown in the accompanying picture, netcentricity has evolved through numerous iterations to include Command, Control, Communications, Computers, & Intelligence targeted for the battlefield, through Global Information Grid (GIG) architectures, to today's framework. Through an evolutionary process that included the Quadrennial Defense Review and the acknowledgement that cyberspace is a warfighting domain, we have developed a framework we refer to as GIG 2.0.

While we have been on the path to net-centric operations for almost 20 years and have made some progress, we continue to run into some of the same barricades to information sharing that we did in 1990. With this said, why do we think that in 2009 we will have more success in breaking down these barricades than we have had to date? A major reason is that absent an overarching framework, those who have the dollars will spend it to optimize their priorities. Since the Services have significant funding, they have designed their networks to support their specific service business process. This leaves the warfighter in the gaps between these service intranets. To start breaking down the Service intranets, we need an overarching framework that dries us to a true, single information environment





focused on supporting warfighting. For the first time, we have delivered such an overarching framework, constructed by the Command, Control, Communications, and Computer Systems Directorate of the Joint Chiefs of Staff (J6) and kick-started to provide global access to information so the warfighter can achieve and maintain the information advantage. Throughout the DoD, it is widely acknowledged that supporting the deployed warfighter in a Joint, interagency, and coalition environment creates complex operational issues where unity of command and effort are vital to mission success. Recent operational experiences in Iraq and Afghanistan highlight the necessity to eliminate barriers to a Joint and coalition network environment that currently exist on our multiple networks. The GIG 2.0 effort, striving to unify the diverse interagency garrison and tactical networks into a single, robust, and secure information environment, will provide increased network agility to commanders and thereby improve command and control, operational capabilities, and mission execution.

The overarching capabilities of the GIG 2.0 vision are taken from a number of sources, including the *Net-Centric Operational Environment Joint Capabilities Document* and *Joint Net-Centric Operations Strategy.* Providing an IT infrastructure that is accessible anywhere, anytime, to anyone is central to ensuring that the DoD achieves and maintains the information advantage. In turn, the enterprise services and infrastructure of the GIG must be designed and optimized to support warfighting functions of both advantaged and disadvantaged users across the full range of military operations in any operational environment. The GIG 2.0 effort strives to achieve and maintain the information advantage as a critical element of national power. The intent is to make DoD operations seamless and secure over a single information environment that provides the necessary capabilities to project power and protect our assets, bringing the fruits of information sharing to bear for the warfighter. The task is daunting: currently, DoD's GIG consists of more than 15,000 separate networks and roughly seven million IT devices in a global network that includes wired and wireless connectivity [1] over a variety of mediums. The challenges to seamlessly integrate this loosely coupled network are obvious, but the goal is the same: move the DoD toward an integrated architecture that provides all DoD components and mission partners enhanced and integrated elements of command and control at any place, at any time, without fail.

Global Information Grid 2.0 Characteristics

- Unity of Command
- Common Policy and Standards
- Global Authentication, Access Control, and Directory Services
- Information Services "From the Edge"
- Joint Infrastructure

Global Information Grid 2.0 Characteristics

When achieved, the GIG 2.0 vision will ensure seamless network interoperability between Joint, coalition, and ultimately interagency and non-governmental organization partners through universal services and protocols. Additionally, it will provide a scalable network common operating picture from the tactical to the strategic level.

GIG 2.0 will ensure availability of assured information to achieve decision superiority and drive resources, policy, and procedural changes to achieve net-centric operations, ultimately transforming the GIG into a single, unified information environment with standardized interfaces and singular governance processes. The enhanced GIG 2.0 capabilities will reduce our vulnerabilities through standardized, controlled access to the information environment.

The following characteristics are the foundation of GIG 2.0 and relate directly to the Joint Operational Concept— [2]

- **Unity of Command**—This characteristic defines the necessary coordination and cooperation of supported commanders for operating and defending the GIG. United States Strategic Command has the mission to operate and defend the GIG and will direct actions to ensure the GIG is protected. The geographic combatant commanders will employ and operate GIG assets to ensure execution of their operational missions. GIG 2.0 success requires supporting and supported commanders (*e.g.,* combatant commanders, military services, agencies, joint task forces), Joint infrastructure, policies, and standards defined to achieve global authentication, access control, directory services, and information and services from the tactical edge. This characteristic ensures support for the command and control relationships as identified in the Unified Command Plan.
- **Common Policies and Standards**—The GIG 2.0 will be built upon common policies and standards that ensure all DoD networks and IT systems are integrated to provide seamless, end-to-end information services. Such common standards will ensure systems are developed, tested, certified, and deployed with enterprise commonality. This concept does not imply a "one size fits all" approach to IT systems, but rather one set of technical reference standards to ensure seamless interoperability of IT systems across the force. As a result, this characteristic provides effective enterprise direction for data standards, information service standards, acquisition, certification, and enforcement to ensure seamless flow of information between all DoD and mission partner users and systems. GIG 2.0 components, including user access and display devices and sensors, networking and processing applications and services, and related transport and management services will be governed by common policies and standards.
- **Global Authentication, Access Control, and Directory Services**—This characteristic ensures that any authorized user can access the global network infrastructure from any location with common and portable identity credentials that enable visibility of, and access to, all appropriate warfighting, business, or intelligence-related information, services, and applications related to their mission and communities of interest. This characteristic includes single sign-on anytime, anywhere to gain access to the network, IT services, and a true global address list. The property tag on the device you use should not dictate what you have access to; rather, your identity and mission requirements must be the driver.
- **Information and Services "From the Edge"**—This characteristic ensures that the warfighter is provided timely, assured access to required data and services at the edge of the battlespace to fully leverage the information advantage in direct support of the mission. The warfighter network must be designed and optimized to support warfighting functions of advantaged (robust environment) and disadvantaged (austere environment) users, to include mission partners across the full spectrum of military operations in any operational environment.
- **Joint Infrastructure**—This characteristic provides a single, unified information environment that interconnects GIG 2.0 users securely, reliably, and seamlessly. The infrastructure enables shared information services for Joint, coalition, and unanticipated mission partners, business support and intelligence personnel, and systems from the tactical edge to any global location. This characteristic includes present and future military and commercial communications capabilities, such as the aerial layer relay and gateway capabilities to expand communications coverage, communications network distribution services (*e.g.,* routing, switching), data center facilities, and transmission systems.

Ultimately, GIG 2.0 will support the full range of military operations, which vary in size, purpose, and combat intensity, from limited contingency operations to major operations and campaigns. The GIG 2.0 framework places the warfighter as the focal point, and each of the five characteristics support, enhance, and enable the warfighters whether they are operating in hostile environments far from support elements, in inter-service and coalition operations, or in an interagency mission.

In light of the warfighters' increased dependencies on networking technologies, the GIG 2.0 vision directly supports combatant and Joint Force Commanders in all Joint Capability

Global Information Grid 2.0 Goals [3]

- Provide for a unified information environment optimized for the warfighter to facilitate force integration
- Deliver the information advantage that facilitates freedom of action
- Enable access to required information anytime and anywhere, shortening decision cycles
- Ensure agility and versatility of the information environment to support operational reach and synergy of the force

Areas across the full range of military operations. The following enabling capabilities are derived from the five fundamental characteristics of GIG 2.0 [4]—

- Improve the DoD governance structure for the GIG (Unity of Command, Common Policies and Standards)
- Strict, unequivocal enforcement of common policies and standards across the DoD (Unity of Command, Common Policies and Standards)
- Availability of global, secure, interoperable communications and networks for the DoD (Global Authentication, Access Control and Directory Services, Information Services "From the Edge")
- Availability of usable and reliable Enterprise Services in a unified environment to all authorized users at all locations worldwide (Information Services "From the Edge")
- Establishment of a common Joint infrastructure that enables information sharing across a diverse spectrum of operational requirements (Joint Infrastructure)
- Ability to ensure that the DoD's primary mission-essential functions can be completed regardless of the condition of the GIG or information environment through means such as enterprise resilience, continuity of operations planning, and network diversity initiatives (Global Authentication, Access Control and Directory Services, Information Services "From the Edge," Joint Infrastructure, Unity of Command, and Common Policies and Standards)
- Survivability against cyberspace and physical threats (Global Authentication, Access Control and Directory Services, Information Services "From the Edge").

Challenges

Current challenges to achieving a single, interoperable information environment include a need for updated policies and procedures, a standard baseline for network security, and a unified governance structure for validating and approving communication capability acquisitions. Interoperability with coalition allies remains a key issue, particularly when expanding beyond our core alliances and into other nationalities where language translation is necessary. The GIG 2.0 vision challenges the DoD to deliver results that are timely, relevant, and focused on the needs of the warfighter. Together, the DoD must do what is necessary to ensure the information advantage.

The GIG 2.0 vision transforms the current GIG from multiple stove-piped intranets, processes, governance, and control to a single, net-centric environment, thereby allowing the GIG 2.0 to support all DoD missions and functions in war and peace, and with interagency, coalition, state, local, and non-governmental organizations. When the GIG 2.0 vision is realized, it will integrate DoD IT resources to support the United States national interests and national strategies. Combatant commanders will have situational awareness of the entire network and can tailor their view. Warfighters will have access to the information and services that they need, wherever they are, whatever their task, and it will be independent of the device they use to connect. State, local, other federal agencies, and allied and coalition partners will be able to communicate and collaborate with the DoD to carry out the mission.

In the end, creating a framework for assured system and network availability, assured information protection, and assured information delivery is central to providing the IT services required to implement the GIG 2.0 vision, ensuring the warfighter can achieve the information advantage at the right place, at the right time, without fail. If the entire DoD concentrates efforts to provide a single, seamless environment—optimized for the warfighter—then the U.S. will be able to achieve and maintain the information advantage as a critical element of national power. ■

References

1. Association for Enterprise Integration, CYBER: The New Warfighting Domain, *http://www.afei.org/brochure/9a04/,* 2009.
2. Chairman, Joint Chiefs of Staff J6, *Initial Capabilities Document for Global Information Grid 2.0,* Joint Requirements Oversight Council, Pentagon, 2009.
3. Chairman, Joint Chiefs of Staff J6, *Global Information Grid 2.0 Operational Reference Architecture,* Pentagon, 2008.
4. Ibid

About the Author

Nancy Brown, VADM | is the former director of the Joint Staff's Command, Control, Communications, and Computer (C4) Systems Directorate (J6) and the principal advisor to the Chairman of the Joint Chiefs of Staff on DoD C4 systems matters. Under her leadership, the GIG 2.0 framework has become a reality and been approved as an initial capabilities document. VADM Brown can be reached at *nancy.brown@js.pentagon.mil.*

IATAC Develops Malware Tools Report

by Theodore Winograd

IATAC has developed a new IA tools report on malware tools. This report provides a brief background on what malware is, the types of malware and how they operate, and information about recent trends in malware capabilities, behaviors, and incidents as well as what makes systems vulnerable to malware infections. The introductory portion of the report also discusses technical and non-technical countermeasures that can be incorporated into information security programs to fight malware.

The IATAC IA Tools Database is intended to act as a central compendium of publicly available information about IA tools, including anti-malware tools.

The bulk of the report is an annotated index of data contained in the IATAC IA Tools Database on malware analysis, detection, prevention, blocking, removal, and analysis tools.

This report defines anti-malware tools as software programs that perform one or more of the following functions to address malware that has entered a system or network—

- **Detection**—identifying specific malware, indicators or anomalies
- **Blocking**—preventing malware from installing or running
- **Isolation and constraint**—preventing malware from interacting with the system
- **Removal and eradication**—completely removing all traces of malware from the system and reversing any changes the malware has caused.

The tool descriptions in the report are organized according to the tool's function and, in the case of detection and removal tools, the category of malware threat (as taxonomized in the introduction) the tool is intended to address. Tools include—

- Malware detection and removal tools, including—
  - "Broad spectrum" anti-malware: addresses more than one category of threat
  - Anti-virus: addresses viruses, worms, and "delivered" (rather than embedded) Trojans (excludes spyware Trojans)
  - Anti-spyware
  - Anti-rootkit
  - Anti-bot (excluding spy bots, which are considered spyware)
- Installation blocking, execution termination, and isolation and constraint tools
- Malware analysis tools
- Other anti-malware tools (outside the categories above).

Despite the fact that the report limits itself to "dedicated" anti-malware tools and excludes multi-function security tools that include anti-malware as only one of multiple capabilities (*e.g.,* Internet security gateways that perform firewall, intrusion prevention, anti-malware, content filtering, and encryption functions), it still describes over 150 tools. This reflects an extensive investigation to discover as many available tools as possible, though the authors admit that it is likely that some tools were overlooked; for this reason, the list of tools should be seen as extensive, but not exhaustive.

For each tool, the report provides an abstract—a brief descriptive overview of the tool's capabilities, based in most cases on information provided by the tool's developer or vendor (in a small number of cases in which the supplier did not provide sufficient information, third-party descriptions from other reliable sources were used). Following the abstract, standard data points about the tool are captured, including the tool's main function (*e.g.,* "virus detection and removal"); the operating system(s) under which it runs;

The report's main purpose is to expose the reader to the numerous tools available in the anti-malware arena.

the hardware requirements of its host; whether the tool has undergone evaluation by the National Information Assurance Partnership or received a Common Criteria Evaluation Assurance Level rating (unsurprisingly, no tools had either, as there is no government certification or Common Criteria protection profile for anti-malware tools); the type of license under which it is distributed (commercial, open source, or freeware—no distinction was made between commercial and shareware, as both are paid licenses); the developer, vendor, or supplier name; and the Uniform Resource Locator for the Web page from which the tool can be obtained (downloaded or purchased).

The IATAC IA Tools Database is intended to act as a central compendium of publicly available information about IA tools, including anti-malware tools. The anti-malware tools landscape is constantly changing—new tools are always emerging and old tools and tool suppliers frequently disappear or are acquired. As the anti-malware tools landscape changes, the tools entries in the Tools Database are updated to reflect those changes. In addition, this tools report, as a "snapshot in time" of the Database's content, will also be updated periodically.

To keep up with the volatile tools landscape, IATAC performs very little analysis on the open-source information it captures about the hundreds of tools described in the IA Tools Database. While every effort is made to eliminate all marketing-type claims from the tools descriptions, there is no independent verification of those descriptions, nor any hands-on testing of the tools themselves. IATAC's role is not that of a tool evaluator. The authors of the tools report have made no qualitative judgments of any of the tools described therein, nor expressed any opinion about their apparent quality, capabilities, or supplier competence or integrity. The report's main purpose is to expose the reader to the numerous tools available in the anti-malware arena. It is up to the reader to perform the further investigation necessary to determine a tool's true capabilities and ability to satisfy his/her requirements.

For instructions on obtaining the Malware Tools Report, please visit the IATAC Web site at *http://iac.dtic.mil/iatac*. Technical questions concerning this report may be addressed to *iatac@dtic.mil*. ■

About the Author

Theodore Winograd CISSP | has been involved in software security assurance and information assurance for over five years, particularly service-oriented architecture security and application security. He has supported the DHS Software Assurance Program, the DISA Application Security Program, and the DISA Net-Centric Enterprise Services project. Mr. Winograd has also supported security engineering efforts for multiple government organizations. Mr. Winograd has served as lead author for multiple National Institute of Standards and Technology Special Publications (SP), including SP 800-95, Guide to Secure Web Services, and has served as a contributing author for State-of-the-Art Reports for DTIC's IATAC. Mr. Winograd can be reached at *iatac@dtic.mil*.

CyberWatch's Pipeline for the Cybersecurity Workforce

by Dr. Bob Spear and Dr. Vera Zdravkovich

Through the advent of the Comprehensive National Cybersecurity Initiative, President Obama's administration has put cybersecurity in the spotlight of mainstream media. What that spotlight has revealed is that, more than ever, the U.S. needs a well-trained workforce that can meet tomorrow's cybersecurity needs.

Building this workforce requires developing a pipeline that will funnel the right people with the right skills into the right jobs. CyberWatch has been building this pipeline and is increasing its efforts to help tomorrow's cybersecurity professionals thrive.

Funded by the National Science Foundation, CyberWatch is one of only three regional Advanced Technological Education Centers devoted to information security. Led by Prince George's Community College in Maryland, the CyberWatch consortium consists of 16 community colleges and 12 universities that share best practices, training methodologies, and resources to improve the quantity and quality of the IA workforce. CyberWatch accomplishes its mission using a four-pronged approach focusing on curriculum and infrastructure, faculty development, students, and community outreach.

In order to develop an infrastructure that supports cybersecurity, CyberWatch focuses a lot of its efforts developing the curriculum and resources offered at its member institutions. It is involved in developing computer laboratories, cybersecurity and IA courses, and model A.S. and A.A.S. degree programs that meet national security standards. Recognizing that there are limited resources to meet growing student demands, CyberWatch developed a state-of-the-art Virtual Laboratory that its members use to provide students with practical application exercises either from a computer lab or from home. It also has helped its schools develop online courses, and it advocates use of a course-sharing model so that its members can share educational resources to train their respective students.

Faculty development is a priority concern at many member institutions who wish to initiate or expand IA programs, but lack a sufficient number of faculty qualified to teach IA. CyberWatch conducts many seminars and workshops for faculty, and also provides tuition assistance to individual faculty members through its Faculty Graduate Program.

CyberWatch takes an innovative approach to developing students for the IA field. At every level of educational development, CyberWatch is conducting outreach programs to stimulate interest in cybersecurity. Its K-12 Cybersecurity Education Program is a new initiative, for example, that reaches kids in elementary schools by providing summer camps and afterschool programs. Kids in these programs develop technological skills, as well as critical thinking, collaboration, and teamwork skills essential for the computer security workforce.
To augment this initiative, CyberWatch offers training and outreach programs to high school faculties and guidance counselors, ensuring kids' interests are cultivated throughout school.

CyberWatch offers various resources for college students.
It promotes, publicizes, and coordinates internship opportunities, scholarship opportunities, and job postings. It also sponsors three student competitions: the Regional Collegiate Cyber Defense Competition, the Security Awareness Contest (in conjunction with Educause), and the Digital Forensics Cup.

Funneling highly trained students into the right jobs is the end-goal of CyberWatch's efforts. To make sure its pipeline is properly constructed, the center works hand-in-hand with government, industry, and academic leaders in the IA field. Some of CyberWatch's supporters include Cisco Systems, Inc.; CompTIA; Lockheed Martin; SAIC; and Northrop Grumman. Additionally, the Department of Homeland Security and the Maryland State Department of Education support CyberWatch in its initiatives. This support ensures CyberWatch's efforts

will produce the IA workforce needed to meet future cybersecurity demands.

All of CyberWatch's initiatives are designed to inform the general public about the importance of cybersecurity, and clearly, its message is spreading. Perhaps the greatest testament to CyberWatch's success is that it has developed into a national organization. CyberWatch began as a Maryland, Virginia, and District of Columbia regional organization, but now CyberWatch encompasses institutions also in Delaware, North Carolina, Louisiana, New York, Massachusetts, and Washington State. With its continued success, CyberWatch expects its footprint to grow significantly over the next few years.

For more information about CyberWatch and its initiatives, please visit *www.cyberwatchcenter.org*, or join the CyberWatch group on LinkedIN.

About the Author

Dr. Bob Spear | is the director of the CyberWatch Center, succeeding the center's first director, **Dr. Vera Zdravkovich**, who remains heavily involved in the center. Dr. Spear and Dr. Zdravkovich are both retired from Prince George's Community College. Dr. Spear was a professor of computer information systems, and Dr. Zdravkovich was a chemistry professor and college administrator, ending her career as vice president for academic affairs. Dr. Spear can be reached at *robert.spear@cyberwatch.org*. Dr. Zdrakovich can be reached at *vzdrakovich@pgcc.edu*. ■

Letter to the Editor

Q ***I always enjoy reading your column, IATAC Spotlight on Education. I think it's important for institutions of higher learning to offer programs that will better train future IA experts. Is there a list of the top-ranked academic institutions for IA?***

A Yes, there is a list of America's top institutions for IA programs. The NSA and DHS work in conjunction with one another to evaluate IA programs at various academic institutions. Schools are measured against stringent criteria to determine whether they classify as National Centers of Academic Excellence in IA Education (CAEIAE) or Centers of Academic Excellence in Research (CAE-R). The schools that classify as CAEIAE have strong academic programs that offer students extensive IA resources and programs of study to become IA experts in the field. The CAE-R are schools recognized for their IA research initiatives and their contribution to IA literature.

NSA and DHS recognize the importance of producing IA professionals with a broad range of technical skills. As a result, students from schools designated as CAEIAE or CAE-R are eligible to apply for various DoD and federal scholarship programs.

If you are interested in learning which schools qualify as Centers of Excellence, please visit: *http://www.nsa.gov/ia/academic_outreach/nat_cae/index.shtml* ■

Dr. Endicott-Popovsky

by Angela Orebaugh

This article continues our profile series of members of the IATAC Subject Matter Expert (SME) program. The SME profiled in this article is Dr. Barbara Endicott-Popovsky at the University of Washington (UW).

Dr. Endicott-Popovsky is the director for the Center of Information Assurance and Cybersecurity at UW, designated by the National Security Agency (NSA) as a Center for Academic Excellence in Information Assurance Education. She holds a faculty appointment as senior lecturer with the UW Information School (iSchool), following a 20-year industry career marked by executive and consulting positions in information technology architecture and project management. Her research interests include calibration of low-layer network devices, forensic-ready networks, and integrating secure coding practices into development efforts.

In 2007, Dr. Endicott-Popovsky earned her PhD in computer science/computer security from the University of Idaho after completing her dissertation titled *A Methodology for Calibrating Forensic-Ready Low Layer Network Devices*. She holds an MS degree in information systems engineering from Seattle Pacific University (1987), an MBA from the University of Washington (1985), and a BA degree from the University of Pittsburgh (1967).

Dr. Endicott-Popovsky has created a variety of university courses, including Information Ethics, Security, and Privacy; Information Assurance Risk Assessment and Management; Computer Forensics; and Cyberterrorism.

Her recent research papers include—

- "Identification of Malicious Web Pages through Analysis of Underlying DNS and Web Server Relationships"
- "Digital Forensics and Records Management: What We Can Learn from the Discipline of Archiving"
- "Justifying the Need for Forensically Ready Protocols: A Case Study of Identifying Malicious Web Servers Using Client Honeypots"
- "An Operational Framework for Service Oriented Architecture Network Security."

Dr. Endicott-Popovsky has made a number of contributions to IA and education, including establishing the Northwest Regional Collegiate Cyber Defense Contest, creating the IA certificate program for the UW Educational Outreach and the iSchool, and leading the creation of an NSA/Department of Homeland Security-designated Northwest Regional Center of Excellence for IA research in collaboration with Pacific Northwest National Laboratory and Microsoft. She has earned a number of honors and awards, including the University of Washington Educational Outreach 2008 Excellence in Teaching Award. ■

Dr. Endicott-Popovsky has created a variety of university courses, including Information Ethics, Security, and Privacy; Information Assurance Risk Assessment and Management; Computer Forensics; and Cyberterrorism.

Information Assurance (IA) Conference of the Pacific

The IA Conference of the Pacific (IACP) was held in Honolulu, Hawaii, from 16 to 19 June 2009 and provided a venue for IA professionals from across the entire Pacific theater to focus on improving their IA security posture of information networks and systems. In addition to briefings and panel discussions, attendees were able to share ideas, exchange information, and engage in discussions related to strengthening their organization's security posture.

Keynote addresses were provided by Mr. Robert Lentz, Deputy Assistant Secretary of Defense Cyber, Identity, and IA, Office of the Secretary of Defense; BG Ronald Bouchard, U.S. Pacific Command J6; COL Jim Barrineau, Joint Task Force–Global Network Operations (JTF-GNO); Mr. Bill Marshall, National Security Agency (NSA) Information Assurance Directorate (IAD); Mr. Richard Hale, Defense Information Systems Agency (DISA) chief IA engineer; and Ms. Mary Ann Davidson, Oracle chief security officer. In addition to the keynotes, presentations were provided in the following areas: Cyberspace Architecture; Cyberspace Operational Proactive Steps; Cyberspace Strategies; Cyberspace Monitoring, Analysis & Investigation; IA/Computer Network Defense Tools and Initiatives; Cyberspace Deep Dives; Cyberspace Defense Strategy; and Cyberspace Research and Development. There were panel discussions on Cyber Operations with the United States Army Pacific G6, United States Forces Japan G6, United States Forces Korea J6, Pacific Air Forces A6, and DISA Pacific Field Command, and on the New Normal in Cyberspace with the JTF-GNO, NSA IAD, and DISA. Attendees included IA professionals from across the entire DoD as well as representatives from Singapore, Japan, and New Zealand.

This annual conference is a very important facet for our nation's way ahead in cyberspace operations in support of the Administration's Comprehensive National Cybersecurity Initiative. A key focus throughout the conference was "change"; the environment is different now than even 12 months ago (*e.g.,* the DoD is now seeing an average of 360 million probes each day to its systems and assets, and implementations are taking on a focus of "everything over Internet protocol"). We need a cultural change to embrace today's environment. If a military member lost his/her weapon in a field training exercise, no resources would be spared to find it. We need the same intensity for IA. We need a "new normal." Briefings from this year's IACP can be found at the following links: *https://www.us.army.mil/suite/page/555136* or *http://psp.hq.pacom.smil.mil/orgareas/j6/j63/j632* (document library, conferences). ■

The 2010 Information Assurance Exposition

The next IAE will be held in Nashville, Tennessee, 2–5 February 2010. This well-attended conference is expected to fill up early. Watch the web site *(http://www.informationassuranceexpo.com/)* for registration and agenda information.

Intrusion Tolerance—Getting from Security to Survivability

by Karen Mercedes Goertzel

Security for Department of Defense (DoD) information systems and networks needs to be addressed at two levels: the system level and the information level. At both levels, there are threats to availability (for systems, this is often expressed in terms of "quality of service") and to integrity. At the information level, the threat to confidentiality of the information is added. The threats to which DoD systems and networks are subject include—

- Denial of service (intentionally caused failure)
- Corruption of or tampering with the system's executable software or hardware logic, or the configuration files, control files, or data files that govern how that logic executes. This corruption or tampering may occur during the system's development, distribution, installation, operation, or maintenance.
- Embedding or insertion of malicious logic into the system's software or hardware components (again, at any time during its life cycle).

The threats to which DoD information (which includes inputs to and outputs from the system) is subject include—

- Leakage to or sharing with inappropriate parties (unauthorized disclosure)
- Corruption or tampering (unauthorized modification)
- When privacy is a concern, unintended use.

The traditional strategy for information security, cybersecurity, and computer network defense has been protect-detect-react (PDR)—

1. Detect the manifestations of threats as intrusions and attacks
2. Protect against those threats through use of a variety of "defense in depth" and "defense in breadth" security controls and countermeasures that in some (but certainly not all) cases have had their effectiveness proactively verified and validated prior to use (*e.g.,* through certification and accreditation)
3. Respond to intrusions and attacks in ways that minimize—
   - The extent, intensity, and duration of their impact on the targeted system or network
   - The likelihood of their recurrence.

Following this strategy, security controls in DoD environments tend to focus on (1) monitoring and controlling the interaction of systems and networks with external entities (humans, software processes, hardware devices) in ways that mitigate the exposure of those systems/networks to hostile activities by those entities; (2) minimizing the intensity, extent, and duration of, and rapidly recovering from, the damage that results from security compromises that cannot be prevented. The complementary disciplines of system assurance and software assurance augment this operational security strategy by attempting to eliminate or mitigate any vulnerabilities and malicious logic introduced into system components during their development.

Why PDR is a Losing Proposition

Recently, practitioners of information assurance, computer network defense, and cybersecurity have begun to admit that their long-pursued strategy of PDR to secure information systems is essentially flawed. The systems to be secured are growing too complex, diffuse, and in many ways uncontrollable, the adversaries too skilled and expert, and the emergence and proliferation of new threats too rapid for any security strategy based on avoidance, deterrence, and defense to ever succeed. The information war, as currently being waged, is not only being lost, it cannot be won.

So, if PDR is failing, what can succeed? Inside and outside the DoD, it is increasingly hoped that the answer is *survivability.* Survivability has been defined as "the degree to which a system is able to withstand attack and still function at a certain level." [1]

Survivability as a strategy for dealing with threats against security

expands the focus from preventing, detecting, and reacting to attacks to include surviving them.

Earlier (and in many cases even now) security practitioners used the term "resilience" or "resiliency" to express this idea. The trouble is that outside the security community, resilience does not explicitly incorporate the idea of intentional and malevolent threats to the continued ability to operate. Resilience outside of a security context refers to the ability to continue to provide service following any change or attempted change to that ability, whether such a change is intentional or accidental.

The need for resilience is, in fact, an area of common ground among all high-confidence systems, including mission-critical, safety-critical, and security-critical systems. Indeed, a significant amount of research has been undertaken to adapt fault tolerance, diversity, and assurance techniques from other high-confidence engineering communities to transform security engineering into survivability engineering.

Resilience in the broad sense also differs from survivability in its emphasis on graceful degradation and recovery from unanticipated service interruption, with full restoration of service to its pre-interruption state. Survivability, by contrast, not only emphasizes the malevolent causality of the service interruptions, it shifts the focus to careful calibration of service degradation to ensure continued availability of critical services and information throughout sustained high-intensity attacks.

Survivability, by contrast, not only emphasizes the malevolent causality of the service interruptions, it shifts the focus to careful calibration of service degradation to ensure continued availability of critical services and information throughout sustained high-intensity attacks.

"Intrusion Tolerance" as an Engineering Objective

High-confidence engineering has long focused on providing the means by which systems and software can continue operating despite the presence of errors and faults. High-confidence systems are designed and implemented to achieve this ability, in large part, through fault tolerance techniques.

Two of the means by which fault tolerance is achieved are redundancy and diversity. Critical system functions are multiply instantiated and distributed throughout the system; each instantiation is implemented to be functionally identical to all the others, but physically different from them, so that a fault that could cause one instantiation to fail will not necessarily affect the others in the same way. As individual instantiations fail, the remaining instantiations continue to operate, thus enabling the system as a whole to continue operating, albeit at a gradually degrading level of service. Increasingly, the specific approaches for achieving diversity are based on biological models. [2]

In fault-tolerant systems, redundancy and diversity are augmented by very specific, complete software error and exception handling logic that takes exceptional measures to avoid the escalation of any error or fault into a failure.

For security critical systems, fault tolerance might be seen as "intrusion tolerance." The number one imperative of survivability is to prevent the failure of critical system functions regardless of the stress imposed on those functions by intentional malicious attacks—or

intrusions. The means by which system failures in the face of intrusions can be prevented are similar to the means by which failures are prevented in the face of unintentional faults or safety hazards. In either case, there are various analyses, design principles, implementation practices, and testing regimes that will enable the system engineer, the software developer, and the hardware manufacturer to—

1. Recognize and understand the security threats to which the system and its individual components are likely to be subjected, how those threats are likely to manifest in the real world, and how the system is likely to behave when subjected to those threats
2. Recognize the nature and exposure of the defects, flaws, bugs, *etc.,* in the system components that make them vulnerable to compromise by those threats
3. Design, code, integrate, and test the individual components and the system as a whole to minimize both the number of overall vulnerabilities, as well as to reduce the external exposure ("the attack surface") of any residual vulnerabilities that could not be eliminated or otherwise mitigated.

Even if all these measures are taken, there may be conditions under which complete failure is ultimately unavoidable. In such (one hopes very) rare circumstances, the system should be designed to fail securely, *i.e.,* to fail in a way that does not leave any critical information or other assets exposed to compromise.

Challenges to Achieving Survivability

"The complexity of systems and the vast deployment of global data networks have put both the public and private sectors in a new situation. So far we have not seen proof of deliberate, coordinated terrorist-initiated attacks on data systems. Should terrorists exploit these abundant vulnerabilities—and it seems likely that they may soon—our society will find itself in a new, challenging situation." [3]

In DoD, there is often no direct correlation between the criticality of the mission and, by extension, the information used in performing that mission, and the redundancy of the information systems and services that enable that mission. The DoD increasingly tends to follow common commercial practices, using the fewest physical servers and devices possible, and physically centralizing a number of critical services (*e.g.,* cross-domain information sharing) to enable ease of operation and administration. This reduced proliferation and centralization of servers/devices is particularly notable in forward-deployed environments. Tactical units tend to place all of their command and control elements in close physical proximity to each other so as to simplify physical connectivity.

Increasing use of virtualization is enabling the DoD to further reduce the multiplicity of physical servers, by enabling disparate applications and services to be co-hosted on the same physical platform. What this does, of course, is increase the criticality of each virtualized platform by recasting "redundancy" as a function of multiple virtual instantiations on a single physical host rather than multiplying physical backup systems. The result is an increased number of "single points of hardware failure." In short, any redundancy advantages gained through virtualization are eliminated in the case of hardware failure. Not only does a server's failure bring down one service or application; it now has the potential to bring down numerous services/applications co-hosted on the same platform.

Budgetary constraints have long encouraged the DoD to insist upon standardization and uniformity rather than diversity of systems and the robustness that accompanies it. Asked about this, several DoD IA practitioners have claimed that redundancy of uniform components in sufficient numbers will be enough to provide such robustness. The problem is that when redundant components are uniform, if one of those components has a particular vulnerability, they all will, and they will all, therefore, be susceptible to any attack that exploits that common vulnerability. Moreover, reliance on published standards, while it provides numerous advantages, also makes DoD systems easier to understand by attackers, who can then exploit known vulnerabilities in those systems' standard protocols and interfaces. Security through obscurity alone should never be relied upon. But security through obscurity as a first line of deterrence, in addition to all the other countermeasures, should not be dismissed either.

Budgetary constraints have long encouraged the DoD to insist upon standardization and uniformity rather than diversity of systems and the robustness that accompanies it.

Increasing DoD reliance on civilian (commercial and public) telecommunication and satellite communication facilities and services as well as the Internet renders DoD networks more exposed and more likely to harbor known vulnerabilities than the dedicated military communications of previous years that they have replaced.

Increased DoD dependence on commercial off-the-shelf (COTS) products, while such products can minimize development risk and acquisition costs, also means that many vulnerabilities in DoD systems will be

familiar to any attacker who understands the commercial products from which those systems are built. Rapid commercial development cycles, seen as an advantage because they reduce time to deployment, seldom include disciplined structured development methods, security testing, or robust configuration control practices that can minimize inclusion of vulnerabilities and detect and prevent attempts to embed malicious code (Trojan horses, trap doors, rootkits, *etc.*).

Furthermore, competition among suppliers of COTS products increases pressure for them to outsource their product development to inexpensive off-shore contractors in countries with problematic relationships with the U.S. In such countries, developers may have political loyalties and ideological leanings that predispose them to subvert or sabotage products they believe to be intended for the U.S., and particularly the U.S. government market. Nor are the backgrounds of such non-U.S. developers likely to be investigated or even considered in the commercial supplier's choice of contractor. These issues exist whether the COTS product is software or hardware (*e.g.*, semiconductors, microprocessors).

DoD's transition to complex, global Web service-based applications operating in service-oriented architectures, and the anticipated future migration to even more problematical cloud computing architectures, is causing an exponential growth in the sheer volume of data to be transmitted and processed over the networks that comprise the Global Information Grid (GIG). The size and complexity of distributed GIG networks, with their large numbers of nodes and significant exposure, have increased their susceptibility to penetration, exploitation, and compromise by creative yet unsophisticated adversaries, as well as to intentional abuse by insiders, to naturally occurring failures, and to physical capture or destruction of nodes. Another problem is created by the increasing complexity of inter-node, inter-component, and inter-service: it is making it extremely difficult to adequately model, simulate, and understand DoD's net-centric systems in order to specify effective security protections and controls prior to deployment, or to establish and maintain situational awareness once those systems are deployed.

DoD's transition to complex, global Web service-based applications operating in service-oriented architectures, and the anticipated future migration to even more problematical cloud computing architectures, is causing an exponential growth in the sheer volume of data to be transmitted and processed over the networks that comprise the Global Information Grid.

These new computing paradigms and the increasingly widespread use of COTS products and, with the imminent adoption of cloud-based "as-a-service" computing, outsourced computing and network infrastructure, platforms, and/or applications, have greatly increased the complexity and reduced the controllability and comprehensibility of DoD systems. COTS increases complexity because many COTS products include a multiplicity of features and functions intended to appeal to and accommodate the broadest possible customer base. Complexity and controllability and survivability are closely related: as complexity increases, survivability decreases because analysts and engineers lose the ability to recognize potential faults and failures, vulnerabilities, and access paths. As controllability decreases, so does survivability because it leaves survivability engineers with few, if any, options for increasing the "attack tolerance" of systems and networks. You cannot (re)engineer what you do not own or control.

Unfortunately, their advantages—real or perceived—mean that not one of these factors is likely to be changed by the DoD anytime soon. Instead, the security practitioners must continue to do their best to protect and defend this vastly complex, increasingly distributed, and decreasingly controllable beast called net-centric computing. But, as we've already seen, these practitioners are readily admitting that their task as currently defined is impossible to achieve.

While long asserting that risk management should be the driver for its information security strategy, in reality the DoD's security approach has been and remains heavily weighted toward specification, implementation, operation, and monitoring of technical security controls and countermeasures, most of which are concentrated at the boundaries of the system architecture. These controls and countermeasures are intended to—

1. Protect the confidentiality, integrity, and availability of information and, by extension, the network and network-based system components and mechanisms that store, process, and transfer that information
2. Detect and react to any attempts to intentionally compromise or bypass that protection. The problem with

Survivability, then, is not just an "add-on" to security. Rather, security now becomes a key objective in achieving the larger goal of survivability. In this way, protect-detect-react is recognized as insufficient on its own. Instead, PDR must become an element of a larger survivability strategy that also includes *intrusion tolerance.*

protect-detect-react is that it becomes a goal in itself. Security practitioners have lost sight of the purpose security has in the first place, which is as an enabler for the success of the mission.

Survivability entails moving past protect-detect-react toward a strategy in which practitioners never lose sight of the "survival of the mission" goal, and drives every strategic and tactical decision. And survivability itself is pragmatic; it not only assumes that perfect security cannot be achieved, it recasts acceptance of risk as acknowledgement that protection will fail, detection and response will be inadequate, and that other strategies must be employed to ensure the survival of the mission. This survival depends on the ability for the systems, services, networks, *etc.,* that support the mission to provide continuity of service, if at a degraded level, "in the presence of attacks, failures, or accidents." [4] For the DoD, such attacks may, in fact, be incursions in a high-intensity, nation state-sponsored information war.

Survivability, then, is not just an "add-on" to security. Rather, security now becomes a key objective in achieving the larger goal of survivability. In this way, protect-detect-react is recognized as insufficient on its own. Instead, PDR must become an element of a larger survivability strategy that also includes *intrusion tolerance.* ■

Endnotes

1. Cashell, Brian, William D. Jackson, Mark Jickling, and Baird Webel. "The Economic Impact of Cyber Attacks," Congressional Research Service Report for Congress RL32331, 1 April 2004, page 28.
2. The security engineer may further benefit from biological models in designing mechanisms for isolating and destroying attack vectors or malicious code traces, specifically through use of computer immunology techniques.
3. Ilmonen, Urho. "Survival planning for business: a view from Nokia," Chapter 15 in *Business and Security: Public-Private Sector Relationships in a New Security Environment* (Alyson J.K. Bailes and Isabel Frommelt, editors) (Oxford, England: Oxford University Press, 2004), page 184.
4. Allen, Julia H. and Carol A. Sledge, CMU SEI. "Information Survivability: Required Shifts in Perspective," in *CrossTalk: The Journal of Defense Software Engineering,* July 2002.

References

Goertzel, Karen Mercedes and Larry Feldman. "Software Survivability: Where Safety and Security Converge," in *Proceedings of the American Institute of Aeronautics and Astronautics Infotech @ Aerospace Conference,* Seattle, Washington, 6-9 April 2009.

Gansler, Jacques S. and William Lucyshyn. "Trends in Vulnerabilities, Threats, and Technologies," in *Information Assurance: Trends in Vulnerabilities, Threats, and Technologies* (Jacques S. Gansler and Hans Binnendijk, editors) (Washington, DC: National Defense University Center for Technology and National Security Policy, January 2005).

Steinberg, Laura J. "A Brief Note on Resilience in Engineering," in *Workshop Report: Resilience in Post-Conflict Reconstruction and Natural Disasters,* (Patricia Longstaff, Ines Mergel, and Nicholas Armstrong, editors) (Syracuse, New York: Syracuse University Institute for National Security and Counterterrorism, 9 March 2009).

Ellison, Robert J., David A. Fisher, Richard C. Linger, Howard F. Lipson, Thomas Longstaff, and Nancy R. Mead. "Survivable Network Systems: An Emerging Discipline," Carnegie Mellon University Software Engineering Institute (CMU SEI) Technical Report CMU/SEI-97-TR-013, ADA341963, 1997.

CMU SEI Computer Emergency Response Team (CERT) Survivable Systems Engineering Research Projects. Accessed 20 June 2009 at *http://www.cert.org/nav/index_purple.html/*

Henning, Ronda R. "Designing for Disaster: Building Survivable Information Systems," in *CrossTalk: The Journal of Defense Software Engineering, October 2005*

About the Author

Karen Mercedes Goertzel, CISSP | leads IATAC's Security Research Service. She is a subject matter expert in software assurance, cybersecurity, and information assurance. She was lead author of *Software Security Assurance: A State-of-the-Art Report* (July 2007) and *The Insider Threat to Information Systems* (October 2008), published by the Defense Technical Information Center. Ms. Goertzel has advised NAVSEA and the Department of Homeland Security Software Assurance Program; for the latter, she was lead author of *Enhancing the Development Life Cycle to Produce Secure Software* (October 2008). Ms. Goertzel was also a contributing author of the National Security Agency's *Guidance for Addressing Malicious Code Risk,* and chief technologist of the Defense Information Systems Agency Application Security Program, for which she co-authored a number of secure application developer guides. She contributed to several National Institute of Standards & Technology Special Publications (SP), including SP 800-95, *Guide to Secure Web Services.* She also tracks emerging technologies, trends, and research in information assurance, cybersecurity, software assurance, information quality, and privacy. Before joining IATAC, Ms. Goertzel was a requirements analyst and architect of high-assurance trusted systems and cross-domain solutions for defense and civilian establishments in the U.S., North Atlantic Treaty Organization, Canada, and Australia. Ms. Goertzel can be reached at *iatac@dtic.mil.*

FREE Products 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 online: *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 _____

_____ Email _____

_____ Fax _____

Please check one: ☐ USA ☐ USMC ☐ USN ☐ USAF ☐ DoD ☐ Industry ☐ Academia ☐ Government ☐ 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** ☐ **Malware** ☐ **Anti-Malware**

Critical Review and Technology Assessment (CR/TA) Reports
☐ Biometrics (soft copy only) ☐ Configuration Management (soft copy only) ☐ Defense in Depth (soft copy only)
☐ Data Mining (soft copy only) ☐ IA Metrics (soft copy only) ☐ Network Centric Warfare (soft copy only)
☐ Wireless Wide Area Network (WWAN) Security ☐ Exploring Biotechnology (soft copy only)
☐ Computer Forensics* (soft copy only. DTIC user code MUST be supplied before these reports will be shipped)

State-of-the-Art Reports (SOARs)
☐ Measuring Cyber Security and Information Assurance
☐ The Insider Threat to Information Systems (soft copy only. DTIC user code MUST be supplied before these reports will be shipped)
☐ Software Security Assurance
☐ A Comprehensive Review of Common Needs and Capability Gaps
☐ IO/IA Visualization Technologies (soft copy only)
☐ Modeling & Simulation for IA (soft copy only)
☐ Malicious Code (soft copy only)
☐ Data Embedding for IA (soft copy only)

UNLIMITED DISTRIBUTION

IAnewsletters Hardcopies are available to order. The list below represents current stock.
Softcopy back issues are available for download at *http://iac.dtic.mil/iatac/IA_newsletter.html*

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	☐ No. 2	☐ No. 3	☐ No. 4
Volumes 9	☐ No. 1	☐ No. 2	☐ No. 3	☐ No. 4
Volumes 10	☐ No. 1	☐ No. 2	☐ No. 3	☐ No. 4
Volumes 11	☐ No. 1	☐ No. 2	☐ No. 3	☐ No. 4
Volumes 12	☐ No. 1	☐ No. 2`	☐ No. 3	☐ No. 4

Fax completed form to IATAC at 703/984-0773

Calendar

November

Combatant Commanders Workshop
3–4 November 2009
Tampa, FL
http://www.dtic.mil/

2009 Eastern Conference on IA for DoD and DHS
16–17 November 2009
Washington, DC
http://www.ttcus.com/view-conference.cfm

Interservice/Industry Training, Simulation and Education Conference
30 November–3 December 2009
Orlando, FL
http://www.iitsec.org/about.cfm

December

Configuration Management Seminar
7–8 December 2009
Las Vegas, NV
http://www.asdevents.com/event.asp?ID=623

2009 Annual Computer Security Applications Conference
7–11 December 2009
Honolulu, HI
http://www.acsac.org/

January

2010 Cyber Crime Conference
22–29 January 2010
St. Louis, MO
http://www.dodcybercrime.com/10CC/

DC 2010 Black Hat Briefings & Training
31 January–3 February 2010
Arlington, VA
http://www.blackhat.com/index.html

February

2010 Information Assurance Exposition
2–5 February 2010
Nashville, TN
http://www.informationassuranceexpo.com/

The Network and Distributed System Security Symposium (NDSS) 2010
28 Feburary–3 March 2010
San Diego, CA
http://www.isoc.org/isoc/conferences/

To change, add, or delete your mailing or email address (soft copy receipt), please contact us at the address below or call us at: 703/984-0775, fax us at: 703/984-0773, or send us a message at: iatac@dtic.mil

IATAC
Information Assurance Technology Analysis Center
13200 Woodland Park Road, Suite 6031
Herndon, VA 20171