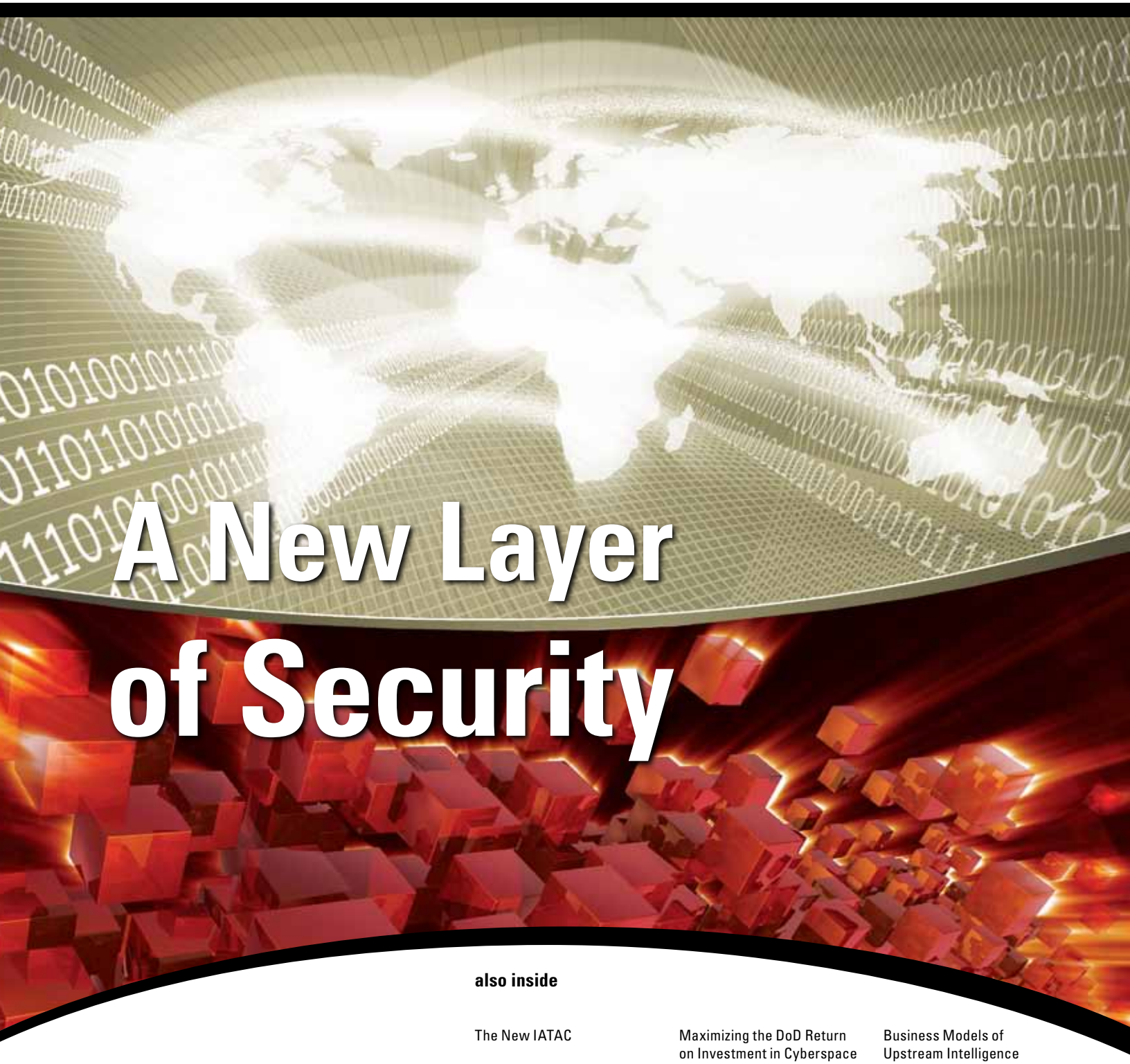
13/3

Volume 13 Number 3 • **Summer 2010**

IAnewsletter

The Newsletter for Information Assurance Technology Professionals



A New Layer of Security

also inside

The New IATAC

Open Specifications: An Enabler of UAV Operations

DoDTechipedia Happenings

Shall We Play a Game?

US Cyber Command is Activated

Maximizing the DoD Return on Investment in Cyberspace Professionals

Upstream Intelligence: A New Layer of Cybersecurity

Anatomy of Upstream Intelligence

Business Models of Upstream Intelligence Management and Distribution

State-of-the-Art Report on Information and Communications Technology Supply Chain Security Risk Management

IATAC

contents

The New IATAC

The current world situation places new strains on our combat forces, weapon systems, and supporting infrastructure. These strains put an increasing emphasis on the science and technology (S&T) community's rapid response capability to solve new issues as they arise.

8 Open Specifications: An Enabler of UAV Operations
As the number of unmanned systems increases, so too, will the overall cost and importance of information assurance (IA) within mission planning and execution.

11 DoDTechipedia Happenings
If you have been to DoDTechipedia before, you may notice a few changes.

12 Shall We Play a Game?
A board game can be a valuable technique to explore the benefits and consequences of different choices and strategies.

15 US Cyber Command is Activated
A command activation and promotion ceremony was held on 21 May 2010, at Ft. Meade, MD where the new command will be headquartered.

16 Maximizing the DoD Return on Investment in Cyberspace Professionals
This article focuses on the challenges our nation faces in developing an information assurance (IA)/cybersecurity workforce.

21 Subject Matter Expert
The SME profiled in this article is Dr. John Sokolowski, at Old Dominion University (ODU).

22 Upstream Intelligence: A New Layer of Cybersecurity
Upstream Intelligence (UI) is information about specific Internet protocol addresses (IPs), domains and Autonomous System Numbers (ASNs) behaving in manners indicative of threats.

26 Anatomy of Upstream Intelligence
This article reviews the anatomy of Upstream Intelligence (UI) and security. It provides a description of the major elements and activities within a carrier or service-provider network that generate UI.

32 Business Models of Upstream Intelligence Management and Distribution
Upstream Intelligence's (UI) ability to combat cyber threats is, in part, determined by the business model employed.

38 State-of-the-Art Report on Information and Communications Technology Supply Chain Security Risk Management
IATAC is developing a state-of-the-art report (SOAR) on managing security risks in the supply chain.

41 Old Dominion University
The Modeling and Simulation (M&S) program is a multi-disciplinary program supported by more than 35 faculty members from all six academic colleges.

42 Ask the Expert
In an era where more data flows into and out of organizations, the need for monitoring is high.

in every issue

3 IATAC Chat
37 Conference Feature
40 Letter to the Editor
43 Products Order Form
44 Calendar

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

If you are interested in contacting an author directly, please e-mail us at Iatac@dtic.mil.

***IAnewsletter* Staff**
Chief Editor: Gene Tyler
Assistant Editor: Kristin Evans
Art Director: Tammy Black
Copy Editor: Kali Wilson
Editorial Board: Al Arnold, Angela Orebaugh, Dr. Ronald Ritchey
Designers: Kacy Littlehale, Don Rowe

***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
Winter 2010 October 15, 2010

Cover design: Tammy Black
Newsletter design: Donald Rowe

IATAC Chat

Gene Tyler, IATAC Director

May 21st marked a significant milestone in our cyber defense; the standup of U.S. Cyber Command (USCYBERCOM). USCYBERCOM is a four-star level unified command headed by General Keith B. Alexander, located at Fort Meade, MD and is under United States Strategic Command (USSTRATCOM). The command will assume responsibility for several existing organizations: the Joint Task Force for Global Network Operations (JTF-GNO) and the Joint Functional Component Command for Network Warfare (JFCC-NW) will be dissolved by October 2010. The Defense Information Systems Agency, where JTF-GNO now operates, will provide technical assistance for network and information assurance to USCYBERCOM, and will move its headquarters to Ft. Meade. [1, 2] USCYBERCOM strengthens a new era of national defense strategies that incorporate cyber as a domain along with air, land, sea, and space. I am pleased that this edition of the IAnewsletter provides a brief snapshot of USCYBERCOM's inception, and that IATAC will provide products, services and capabilities to assist USCYBERCOM as it engages in its critical role in information assurance (IA) and the cyber domain. I know the IAnewsletter will continue to discuss USCYBERCOM and its role in the cyber domain in the months and years to come.

Ironically, on Thursday, May 6th, the day before the Senate confirmed General Alexander as the USCYBERCOM Commander, the New York Stock Exchange experienced intense fluctuations due in part to what the Securities and Exchange Commission labeled an "erroneous 'fat-finger' trade." [3] Allegedly, a typo impacted the volatility of the stock market, volatility that was compounded by the fast-pace at which market trades take place in today's digital age. Imagine how catastrophic the effects would have been if the cause was an effective cyber attack on our stock market. Contemplating this type of event stresses the importance of taking a proactive approach to implementing cybersecurity measures throughout all elements of power and the institutions that impact our daily lives. USCYBERCOM, in concert with elements of our Comprehensive National Cybersecurity Initiative (CNCI), and the authorization of a national Cybersecurity Coordinator, Mr. Howard Schmidt, was established to address these cyber threats. Additionally, this edition of the *IAnewsletter* provides some examples of the proactive tools and IA theories that could mitigate and help to prevent cyber events from occurring.

Terry Heston's article, "The New IATAC," highlights changes in the IAC program. The Defense Technical Information Center (DTIC) Information Analysis Center (IAC) program is making contract changes that will affect IATAC and other IACs by promoting greater market competition. As Terry Heston explains, this environment will give the government other tools and capabilities to implement creative cybersecurity solutions from a wider variety of skilled, successful companies in the IA field. Interestingly, this transition is occurring on the heels of USCYBERCOM's inception, which further demonstrates the significance our government places on addressing cybersecurity and stressing the need for cyber innovation.

Additionally, one of IATAC's subject matter experts, Tyson Macaulay, presents our readers with an overview of Upstream Intelligence (UI), which is a "new layer of cybersecurity." As Macaulay points out, "as a solution, UI consists of proactive and accurate identification of compromised devices and networks on large scales in real-time." This innovation and the other innovations highlighted in this edition of the *IAnewsletter* highlight capabilities IATAC tracks across IA and cyber topic areas.

We have a challenging future and IATAC has an important role; we clearly recognize the importance of IA and cybersecurity. As always, I am interested in your thoughts and perspectives, and I encourage you to enter into this discussion by submitting your own *IAnewsletter* articles at Iatac@dtic.mil. Visit our website and become familiar with our products, services, and capabilities, too.

References

1. *http://www.fcw.com/Articles/2009/06/24/DOD-launches-cyber-command.aspx*
2. *http://www.disa.mil/conferences/exposandfairs/disa_jtfgno_expo2010.html*
3. Goldfarb, Zachary A. "Wall St. firms blamed for plunge." The Washington Post, 12 May 2010.

The New IATAC

by Terry Heston

The current world situation is placing new strains on our combat forces, our weapon systems, and the supporting infrastructure. These strains are placing an increasing emphasis on rapid response for the science and technology (S&T) community to solve new issues as they arise. With a potential downturn in spending for new equipment, reuse of information makes sense and we expect the demand for innovative approaches to using and improving existing technology to increase.

Enter the Defense Technical Information Center (DTIC) and the Information Analysis Center (IAC) Program.

DTIC is responsible for collecting all scientific and technical reports for the Department of Defense (DoD) and is the Program Management Office (PMO) for various IACs established in accordance with DoD Instruction 3200.14. Today there are 10 DTIC-sponsored IACs focused in the following functional areas:

- Advanced Materials, Manufacturing, and Testing Information Analysis Center (AMMTIAC)
- Chemical, Biological, Radiological, Nuclear Defense Information Analysis Center (CBRNIAC)
- Chemical Propulsion Information Analysis Center (CPIAC)
- Data and Analysis Center for Software (DACS)
- Information Assurance Technology Analysis Center (IATAC)
- Modeling & Simulation Information Analysis Center (MSIAC)
- Reliability Information Analysis Center (RIAC)
- Military Sensing Information Analysis Center (SENSIAC)
- Survivability/Vulnerability Information Analysis Center (SURVIAC)
- Weapons Systems Technology Information Analysis Center (WSTIAC)

Each IAC has the mission to collect, analyze, evaluate, synthesize, store, publish, disseminate, and provide research, development, test, and evaluation (RDT&E) functionality concerning available worldwide scientific and technical information (STI) and engineering data. This function is known as the Core or Basic Center Operations (BCO) of the IAC. STI is obtained from a variety of electronic, paper, or other media sources and serves as a bridge across government, industry, and academia (figure 1). Additionally, each IAC leverages Core knowledge to perform additional work (known as "technical area tasks" [TATs]) to verify and validate the technical accuracy/reliability of existing data; evaluate and generate data collection and analysis techniques reported in literature; develop alternative approaches to collection and/or analysis related to their assigned technical area; identify and/or fill voids in existing data or knowledge base specific to user requirements; and advance the standardization of their functional area. TATs are actually task/delivery orders (*i.e.,* mini contracts) within the overall IAC contract. They are deliverable-based contracts, where the products are STI-focused and are made available for reuse by all authorized government, industry, and academic personnel through input into the Total Electronic Migration System (TEMS). TEMS provides instant access to the full online collection of IAC STI using easy-to-use tools to simplify searches by providing full text, abstracts, and bibliographies that further expand the researcher's world of knowledge *(https://tems-iac.dtic.mil)*.

IATAC—Today

In fall 1994, the Director, Defense Research and Engineering (DDR&E), tasked the IAC PMO to determine whether there was a role for the IAC Program in support of Defensive Information Warfare (DIW). As a result, the IAC PMO held a series of meetings with DoD organizations to develop initiatives in response to the threat of information warfare (IW) attacks. Those meetings revealed a significant need for support related to emerging technologies.

The IAC PMO established IATAC as a virtual IAC on 15 October 1996, and it operated in that capacity for 19 months. During this period, IATAC produced a Technical Report on Modeling and Simulation activities for information assurance (IA), a state of the art report (SOAR) on Malicious Code, and IA Tools Reports on Intrusion Detection and Vulnerability Analysis.

IATAC was formally established on 15 May 1998. A single award contract was competed and awarded for a base period of three years, with additional three- and four-year option periods. Currently, IATAC is operating in an option period. Integrated sponsorship for IATAC is provided by the DDR&E; Assistant Secretary of Defense for Networks and Information Integration (ASD(NII))/DoD Chief Information Officer (CIO); Joint Staff Command, Control, Communications and Computers Systems Directorate (J-6); the National Security Agency (NSA); and the Defense Information Systems Agency (DISA).

- **IACs collaborate with scientists and other SMEs around the globe**
  IACs collaborate with a diverse group of experts, including the Unified COCOMs, Defense research laboratories, U.S. Intelligence organizations, as well as engineers, physicists, biologists, medical professionals, and other experts from various government organizations (DHS, CDC, NASA) and private industry

- **IACs integrate with government program managers and technical experts to maintain awareness, relevance, and value to emerging issues**
  IAC Executive Steering Committees are co-chaired by IAC PM and senior technical lead

Figure 1 IACs Bridge Government, Industry, and Academia

IATAC—The Future

As a result of changes required by the FY08 National Defense Authorization Act (NDAA), a new acquisition/contracting strategy was required for the entire IAC Program. The current 10-year, single award IAC contracts needed to be changed due to limitations being placed on single award contracts and the need to enhance competition on task/delivery orders in excess of $5M. The resultant construct shows separate contracts for the TATs and the BCO.

Figure 2 provides a comparison of the current and future constructs. The way ahead section of this figure shows each IAC BCO will be a single award contract to provide information collection (including obtaining information from open sources, conferences/symposiums, and other media), information management and internal information processing (including maintaining various libraries, interface with TEMS, and maintaining a subject matter expert [SME] network), information analysis (including maintenance of existing and development of new analytic tools and techniques and synthesis of information from defense sources resulting in new knowledge), and information dissemination (including response to technical [user] inquiries, maintaining an awareness program [newsletter, web site, *etc.*], and maintaining relevant models, software, and databases).

SNIM serves as an efficient contracting vehicle to quickly get IA, software data and analysis, modeling and simulation, knowledge management and information sharing services into the hands of DoD components, other government agencies, industry, and academia.

Three multiple-award, indefinite delivery, indefinite quantity (IDIQ) contracts will be awarded to perform contract work (TATs), combining the functionality of various IACs. The first of these was just awarded in May 2010 and

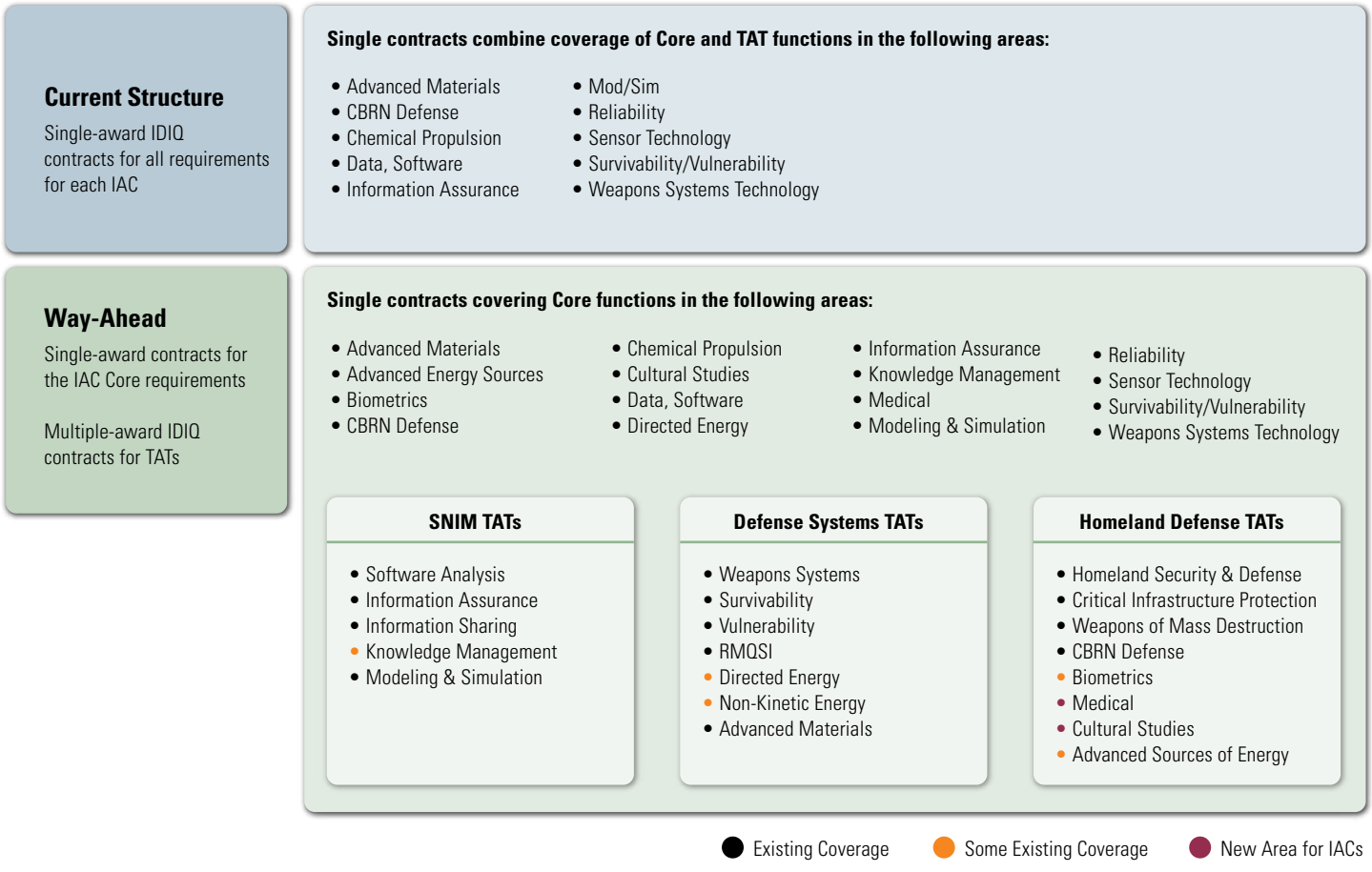


Figure 2 Current and Future IAC Contracts

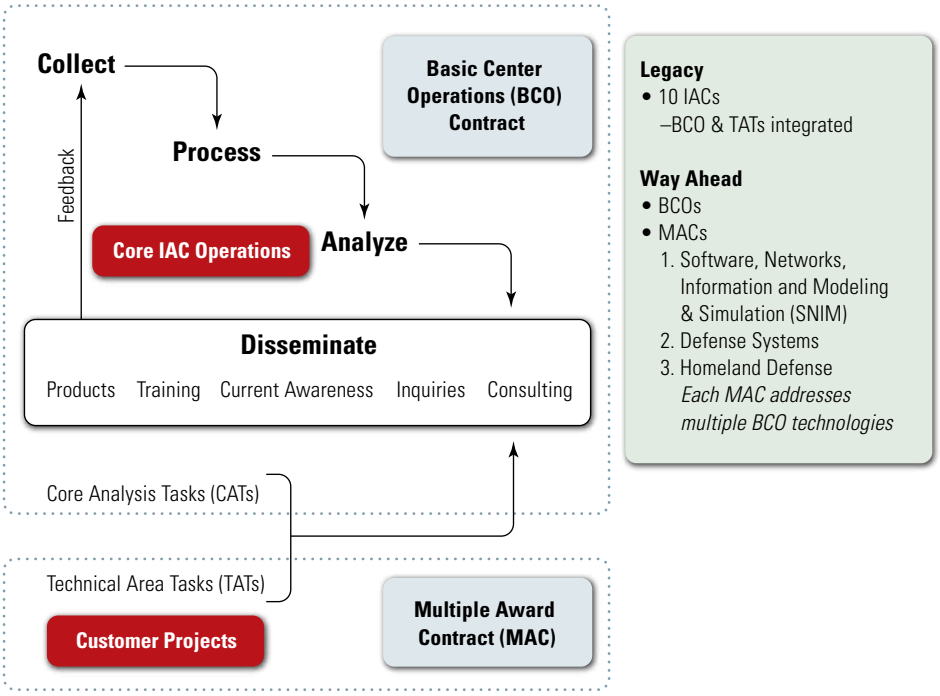


Figure 3 IAC Processes: Same Mission, New Construct

covers Software, Networks, Information, and Modeling & Simulation (SNIM). It combines the TAT effort associated with DACS, IATAC, and MSIAC. With a maximum value of $2 billion over the next 5 years, SNIM serves as an efficient contracting vehicle to quickly get information assurance, software data and analysis, modeling and simulation, knowledge management and information sharing services into the hands of DoD components, other Government agencies, industry and academia. For more information on SNIM, visit the IAC Program Web site at *http://iac.dtic.mil/*.

In spite of the separation in IAC contracts, the mission of the IACs remains the same (figure 3). The IAC PMO has worked extensively with our partners in government, industry, and academia to design a new construct that carries forward the integration of BCO and TAT functions. Core IAC Operations (BCO) depend on STI generated by customer-funded projects (TATs), and vice versa. What sets the IAC Program apart is the focus on investing up front in developing a comprehensive knowledge base (IAC BCO), then leveraging that knowledge base to expeditiously and effectively solve specific challenges requiring research and technical analysis. While operating under separate contracts, BCO and TAT contractors are integrated under a unified approach built on information sharing, and focused on building the technical community across government, industry, and academia.

Until the new BCO contract is awarded, the legacy IATAC contractor will be providing all Core services. For example, this newsletter will continue to be published by the legacy IATAC until the new BCO contract is awarded. Similarly, other Core services will continue in the same quality manner customers have been used to. Four hours of free technical assistance will continue to be provided. STI will continue to be captured and made available *via* TEMS and through other means such as the IADigest and IA/IO Events Scheduler, the latter two vehicles available for email subscription. The IATAC Web site *(http://iac.dtic.mil/iatac/)* will continue to be maintained with free products still being able to be downloaded or ordered. The central IATAC inquiry telephone line (703-984-0775) remains available for assistance until transition is complete to the new BCO. Under the new BCO contract, core historical services will be maintained; upon award, new contact information will be disseminated to the user community.

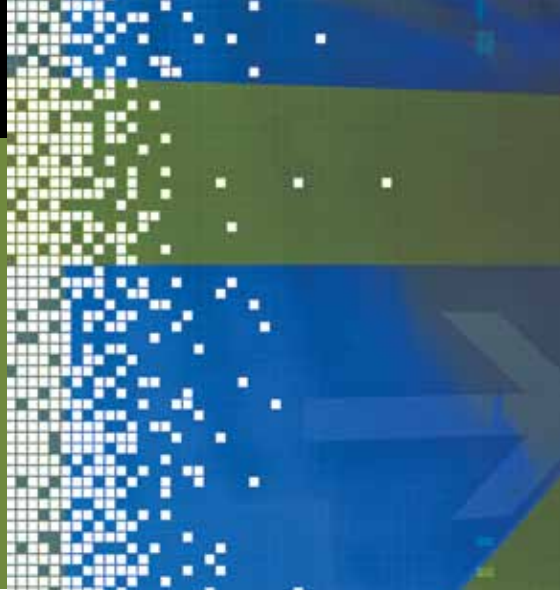
IATAC is providing significantly worthwhile services in support of our nation's warfighters and first responders, the acquisition community, and the entire R&D community. The new way ahead for IATAC and the overall IAC Program will not only meet the mandates from the FY08 NDAA, but will provide continued focus on solving our customers' toughest challenges.

About the Author

Terry M. Heston | is the Program Manager of the DoD Information Analysis Centers at the Defense Technical Information Center (DTIC), where he has served in various management roles over the past 17 years. In his current position, Mr. Heston works closely with the Office of the Director, Defense Research and Engineering to ensure the IACs are positioned to best meet the research and analysis needs of the DoD both today and in preparing for an uncertain future.

Open Specifications: An Enabler of UAV Operations

by Andrew Boyle



Background

During 2009, the United States Air Force (USAF) trained more pilots on unmanned aerial vehicles (UAVs) than on conventional fighters, bombers, and transport aircraft. From 2004 to 2010, overseas high and medium altitude UAV missions increased by over 600%. In late 2009, it was reported that Iraqi militants were using software programs like SkyGrabber ($26 retail price) to intercept real-time unencrypted video feeds from USAF UAVs. The US military knew about the use of unencrypted video feeds, but the highly proprietary and closed system architecture hampered their ability to update the system's security mechanisms. It is clear that current and future conflicts will see an increasing number of unmanned systems. As the number of systems increases, so too, will the overall cost and importance of information assurance (IA) within mission planning and execution.

Current Environment and Deficiencies

Nearly all current unmanned systems use closed and proprietary ground control stations (GCS) to control the unmanned platform. In addition to the control stations being proprietary and associated with a specific vehicle type, a common set of external interfaces allowing standardized integration and facilitating IA testing does not yet exist. The lack of a standard plug on these control stations presents a high integration barrier requiring an external program to customize the integration for each type of control station, with an increased potential of inadvertent security weaknesses. The result is that today's GCSs are monolithic, tightly coupled, and costly solutions. They lack the flexibility to rapidly address security issues, and are available from a limited set of vendors. There could be a better approach to resolving this challenge.

From 2004 to 2010, overseas high and medium altitude UAV missions increased by over 600%.

Prospective Solution

One solution to the interoperability challenge is a set of government-owned, common interface specifications for all control stations that would be freely available to any solution provider.

In general, an interface specification dictates what rules must be followed for discrete systems (or processes) to intercommunicate. Rules would exist for things such as message or data format for a software interface and signal voltages for a hardware interface. "Common," in the context of "common interface specifications," means the interface specification is standardized for a specific type of solution and utilized by many diverse solution providers.

A set of government-owned and controlled specifications would allow for all control station interfaces to be open and published, simplifying integration and reducing cost while increasing the rate of innovation. This approach would increase the solution providers' ability to deliver differentiated solutions, and would engender innovative approaches for controlling multiple platforms, distributed control, and fusing sensor feeds. Opening up the interface specifications would help reduce existing vendor dependencies and commoditize capabilities thereby reducing costs and increasing the number of solution providers and compatible systems. The use of common specifications would facilitate automated information assurance testing.

Real World Application of Open Interface Specifications

Open common interface specifications have been successfully implemented within both industry and government programs. Universal Serial Bus (USB) is an example of a hardware interface specification that has been widely adopted by both manufacturers and consumers. On the software side,

Hypertext Transfer Protocol (HTTP) and Hypertext Markup Language (HTML) have enabled the rapid growth of the Internet and web-related technologies. The widespread adoption of these specifications has benefited both parties. Consumers have an efficient, easy-to-use solution, and manufacturers are able to provide solutions at a price point, increasing sales and enabling them to continue investing in the development of dramatic product innovation.

A common argument against open standards and specifications is that the openness provides potential adversaries with information about the information system; alas, security through increased awareness (*e.g.,* open-source such as Linux) has overwhelmingly shown to be more secure than security through obfuscation (*e.g.,* Microsoft Windows).

The combination of HTTP and HTML has engendered an environment where one web browser works with all websites regardless of its location. This was possible due to the early convergence and stability of the HTTP protocol, essentially creating a common "plug" for all websites to seamlessly integrate with any HTTP compliant browser. No individual website designer owns the HTTP specification, and all site consumers and providers benefit from its existence. The common specification enables the development of common security mechanisms that work across a broad user base.

Applying Open Interface Specifications to Ground Control Stations and UAVs

Similarly, an external consumer would develop a solution that works with all specification-compliant ground control stations avoiding risky and costly configuration changes, integration costs, and most information assurance security issues. The Internet would not have succeeded if each website required a different type of browser. Similarly, the widespread adoption of unmanned systems would be unsuccessful if the data could be easily acquired in a common manner.

A prevalent misconception about open common interface specifications is that vendors would no longer be willing to invest in solutions since the result would be open to all. This is an incorrect assumption. Even though the USB specification is open and widely known, manufacturers are still able to develop compatible proprietary products (*e.g.,* cameras, music devices, storage devices). The use of open specifications means that the external interface must be compliant with the specification. The internal processes, however, may be proprietary and typically are. The existence of the USB specification reduces the risk and cost associated with the integration of new devices to virtually nil. The development of a new USB compatible device does not require testing against every individual computer model to verify compliance. The new device simply needs to adhere to USB specifications.

The adoption of open common interface specifications by unmanned systems control stations would seem an obvious choice. In fact, some recent systems are already moving in this direction with the adoption of various Standardization Agreements (STANAGs), such as the North Atlantic Treaty Organization's (NATO's) STANAG 4586 Standard Interfaces of UAV Control

A set of government-owned and controlled specifications would allow for all control station interfaces to be open and published, simplifying integration and reducing cost while increasing the rate of innovation.

System (UCS) for NATO UAV Interoperability. To maximize its potential, the open specification approach should be extended for internal ground control station consumption in addition to the external consumption of data.

A service-oriented architecture (SOA) provides just such an approach. Simply put, an SOA is a distributed architecture composed of discrete components, each of which provides a particular business functionality that can be reused by different applications. Flight planning would be one such internal "business" component exposed as a service in an SOA. Externally available services would be made accessible to share weather information or data received from the vehicle sensor feeds [*e.g.,* Imagery Intelligence (IMINT) and Signals Intelligence (SIGINT)]. A key point is that all components providing weather information would implement the same, common interface specification, so that information consumers are not affected when one solution provider's weather component is swapped out for another vendor's solution.

Effective use of interface specifications within government programs requires that the government own and control the specification, ensuring the result is truly an open specification (*i.e.,* non-proprietary and license-free). Although the specification should be owned and controlled by the government, specification best practices are that they must be developed and enhanced *via* substantial inputs from industry, academia, and others. A solid and sustainable specification governance process is critical to ensure that the process for submitting and tracking inputs is structured and transparent to all interested and participating organizations. Above all, government organizations must refrain from getting into a battle of the standards, similar to what occurred between BetaMax and VHS, and more recently between Blu-ray and HD-DVD.

For unmanned systems with Intelligence, Surveillance, and Reconnaissance (ISR)-oriented sensors, the Distributed Common Ground System (DCGS) program has already defined a set of ISR specifications along with a structured and transparent governance process for updating the specification. The unmanned systems community would quickly adopt these specifications and, where additional specifications are needed, communicate those needs to the DCGS governance board so the specifications can be updated and then adopted by both communities. This approach is more cost-effective than each community/program/project creating and maintaining its own open specifications and enables low risk interoperability between the sensors carried on the platform and all downstream consumers.

Future Benefits

The emerging use of open common interface specifications will enable solutions to transition to a modular approach that in turn enables the system to improve through incremental continuous changes, instead of the current big bang system upgrades with stove-piped solutions. In today's consumer market, a consumer can plug a new digital camera into their existing computer without waiting for the next model year of the computer so long as both are USB compliant. Similarly, it will become possible for control stations to upgrade components, such as flight planning, as new and improved versions are released.

Aside from incremental technological advances, the use of open common interface specifications benefit the government through lower per-control station cost, increased solution innovation, improved security, and reduced external solution provider dependencies. The use of open specifications benefits solution providers by increasing the available market for future capabilities. Most importantly, the use of open common interface specifications benefits the warfighter and their command by enabling battlefield capabilities more quickly *via* incremental technological advances, throughout all platforms and at a lower cost. ■

About the Author

Andrew Boyle | received a BA degree in Economics from the University of Maryland College Park. He is currently the Service Oriented Architecture subject matter expert for a US government project focused on integrating existing and emerging unmanned aerial vehicle (UAV) capabilities into a large highly distributed enterprise. He is also a subject matter expert for a DoD project, which supports the development and governance of service specification packages for use across the Intelligence, Surveillance, and Reconnaissance (ISR) community. He has supported DoD, intelligence community, and commercial clients in achieving complex enterprise integrations. Mr. Boyle can be reached at iatac@dtic.mil

DoDTechipedia Happenings

by Albert Arnold III

Have you been to DoDTechipedia lately? Several new features enhance usability and navigation, and more content is available to meet your research needs.

DoDTechipedia, is DoD's science and technology (S&T) wiki. Users can share information with other S&T professionals; it expands our collective brainpower to rapidly respond to technological needs. DoDTechipedia's Suite of Services earned the 22nd Annual *Government Computer News* (GCN) Award for "Outstanding Information Technology Achievement in Government."

How DoDTechipedia works:

- **Sharing Knowledge**—The more users contribute, the more the collective knowledge base expands. DoDTechipedia is looking for subject matter expert "gardeners" who edit pages to improve content and maintain information integrity.
- **Connect Across Walls**—By reading or creating technical blogs, users can reach across organizations to brainstorm ideas, develop solutions, discuss hot topics, and learn about new technological trends.
- **Collaborating**—Today's wars require immediate solutions. DoDTechipedia enables collaboration across the Department of Defense (DoD), increasing our ability to identify challenges and rapidly deliver solutions.

If you have been to DoDTechipedia before, you may notice a few changes. *Technology Challenges* discusses technical challenges facing DoD about maintaining military readiness and effective mission capabilities. Any user with specific, immediate or emerging technological interests or needs, can post questions to the community for input.

Technology Discovery contains top-level articles focusing on particular S&T investment areas or enabling technologies. Resources, such as the *information assurance portal,* cover topics ranging from common criteria to important information assurance event meeting minutes, to the latest information on controlled unclassified information.

The *macro browser tool* makes editing pages easier and less time consuming. It allows users to add footnotes, embed presentations, or upload documents, which eliminates the need to use HTML code, or "notations."

The *homepage* now includes upcoming events, a featured article, a wiki tip of the week, and community spaces. These additions highlight new information and are updated on a regular basis. For example, one of the organizations featured within the Combatant Command S&T Community space is the Defense Science and Technology Advisory Group (DSTAG). This group provides executive-level oversight for Reliance 21 and holds monthly meetings to discuss strategic issues impacting DoD-wide S&T activities.

Getting started on DoDTechipedia is easy: Register with the Defense Technical Information Center (DTIC) to obtain a user id and password by visiting *https://register.dtic.mil,* then visit *https://www.DoDTechipedia.mil* and log in with your DTIC user id and password or your Common Access Card (CAC).

Once you are logged on, sign up for a free webinar or view the tutorials to learn how to add or edit information. "New Tools on DoDTechipedia" walk you through recent enhancements, helping you understand their benefits.

Users can also visit the *Sandbox* to practice adding and editing content, and uploading files to DoDTechipedia.

With over 2,800 blog entries, and more than 21,000 updated pages, DoDTechipedia is where the best minds collaborate to develop cutting-edge solutions. ■

DoDTechipedia is a project of the Under Secretary of Defense for Acquisition, Technology and Logistics; Director of Defense Research and Engineering; Defense Technical Information Center; and Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer.

Shall We Play a Game?

by Gregory Dupier

An environmental specialist working in a federal agency is studying the effects of irrigation on watersheds and is looking for data describing public water lines in farming communities across the United States. In a small county in Iowa, a public works engineer, who relies on federal grants for funding, is surveying the new installation of a public water main. How can these two individuals within two government organizations that traditionally do not work together share their information? Playing a board game may help provide the answer!

Recently a group of federal, state, local, and industry geospatial stakeholders got together to play a board game to analyze and develop strategies for scenarios like this one, as well as others that commonly confront the geospatial community. Specifically, the objective of the game was to help the players determine whether certain solutions such as Service Oriented Architecture (SOA), cloud computing, and web 2.0 technologies should be part of the geospatial community's overall strategy.

Developing Security Strategies Using Board Games

Today's information technology (IT) organizations and security specialists are constantly asked to rapidly support changing mission needs with fewer resources. As a result, both security specialists and IT decision-makers must carefully develop strategies that provide the data and agility required to develop needed capabilities, while managing costs, allocating resources, and mitigating risk.

A board game can be a valuable technique to explore the benefits and consequences of different choices and strategies. When most people hear the phrase "board game" they might think of Monopoly©, Scrabble©, or Risk©. However, consider what each of these games has in common:

- **A defined set of goals and objectives**—Players may play as individuals or as teams, however each are trying to accomplish the goals or objectives of the game by accumulating the most points, accumulating resources, or by eliminating other players from the game.
- **Limited resources**—Resources in a board game can be represented in numerous ways including: money, people, letters of the alphabet, land, *etc*. However, in nearly all cases players must maximize the use of the limited resources they have to do well and win the game.
- **Changing conditions**—As players or teams play the game, the choices available to players change. What was once a choice may no longer be an option as the result of other players' or teams' actions.
- **Multiple choices**—Players or teams may make different choices or decisions throughout the course of the game to affect the outcome.
- **Risk versus reward**—Does a player go for the big "payout" even though they may risk losing considerable resources or points needed to win the game? This is a key question players must incorporate into their game playing strategy.

Each of these elements is similar to the elements needed to form an effective IT security strategy. While there are numerous frameworks and methodologies for developing an organization's security strategy, at a minimum, an effective security strategy should address four areas:

- **People**—An effective security strategy identifies the stakeholders that will benefit from the goals and objectives of the strategy, as well as the stakeholders needed to implement the strategy.
- **Processes**—The strategy should describe the processes needed to perform or support the goals and objectives of the security strategy.
- **Data**—The strategy should identify the data and information needed to perform or implement the goals and objectives of the security strategy.
- **Technology**—A key component of an effective security strategy is the identification of the technologies

that need to be acquired and implemented to support the goals and objectives of the organization.

Let us look at how several different government leaders have used board games to inform and formulate their strategies.

Fostering Collaboration

Board games can be a very effective technique to help foster and encourage collaboration. One of the common challenges across the geospatial community is encouraging collaboration between geospatial stakeholders. Frequently one geospatial user may have a data set that has details or information that could be useful to others.

In the geospatial community example, a board game was designed so that teams of geospatial stakeholders competed against each other, with each team trying to accumulate the most points by the end of the game. To earn points, each team was assigned multiple "tasks" representing real-world geospatial activities, analysis or programs. Within each team, players received different amounts of resources (*e.g.,* money to spend), as well as access to different data sets and geospatial applications or services.

Figure 1 Cloud Computing Board Game at FOSE 2009

As each team played the game, the teams that earned more points collaborated and developed a strategy to share their resources to complete their assigned tasks. This collaboration did not come without risk, though. For example, if a team collaborated, shared, and pooled its resources but failed to invest in certain security controls, they might be penalized as their geospatial data sets were "hacked."

So how did the board game help inform the players' strategies for securing geospatial information? When collaboration and geospatial data sharing occurs in the real world, a primary concern of both geospatial data providers and analysts is to ensure the security and integrity of the geospatial data sets. Throughout the game, players were able to explore the different levels of security and risk associated with sharing different types of data sets. Specifically, in the game, different data sets had different levels of risk or "risk profiles." Players were able to specify which data sets they were sharing, the technologies they used to share the data sets, and who had access to each data set. As the game progressed, players were penalized or rewarded based on their choices and the risk profile of each data set. This feedback allowed players to identify key considerations needed when developing real-world information sharing security strategies.

Maximizing Resources

Today, there are many organizations ranging from large federal agencies to small towns and counties that use geospatial data for different purposes. In reality, it is common for larger organizations to have significantly greater resources in the form of budgets and staff. However, just because an organization has a larger amount of resources does not always mean they have the same level of detailed geospatial data as smaller organizations.

In the same geospatial board game mentioned above, players were also able to experiment by applying different amounts of money, people, and technology towards the completion of specific tasks. These choices allowed players to experiment and identify the levels of resources needed to mitigate security risks and prevent the compromise of different types of geospatial data. If players allocated sufficient amounts of resources to secure the data set, they received their points for completing the task successfully. However, spend too few resources and players risk losing points; or spend too many resources and

players risk running out of resources before the end of the game. This experimentation helped the players identify the key resource considerations needed when developing a geospatial data security strategy.

Other Board Games

The "Geospatial Board Game" is one of three board games recently played by federal organizations to develop their IT security strategies and capabilities. Other recent board gaming events included a game designed for Chief Information Officers (CIOs) and a game designed to help players understand IT security governance processes.

The term "CIO" can have different meanings to different people and as such, the "CIO Board Game" was developed to facilitate a common understanding of the authorities and responsibilities of an Office of the Chief Information Officer (OCIO), as well as some of the risks and challenges CIOs face. Recently, a group of IT leaders played the CIO board game looking to understand how various Information Assurance (IA) activities should be integrated with investments, projects, and programs managed in cooperation with the OCIO.

Another term that commonly has different meanings to different people is "governance." A group of current and future CIOs recently played the "IT Security Governance Board Game" as part of a CIO IA and IT security certification program. During the course of the game, players were exposed to different governance processes, decisions and governance documents to understand how and when to implement the appropriate IA controls within an organization.

The goal of both games was to create a learning tool that was interactive and full of energy while also helping the players learn about the functions of a CIO or to learn how IT security governance processes can be applied within an organization.

Board Game Results

Actively applying modeling and simulation to IT security decision making can make all the difference for an organization. The "Geospatial Board Game," the "CIO Board Game," and the "IT Security Governance Board Game" have helped players and organizations:

- Illustrate the interaction between different activities occurring within an IT organization to implement and support IT security strategies and capabilities
- Use data and game-play to model an organization's specific needs
- Reveal how different strategies maximize impact and value
- Understand how to optimize resource distribution (people and dollars) across multiple functions and activities to maximize value
- Promote team building and communication by providing an entertaining and educational tool
- Build awareness of how different roles work with business and IT security partners throughout the organization.

In the end, a board game can be a fun, informative alternative to editing lengthy documents and presentations when developing a security strategy for an organization. By increasing collaboration and helping organizations maximize efficiency, board games may even free up more time for employees' game of "life!" ■

About the Author

Gregory Dupier | has been involved in modeling and simulation for more than 13 years. He has helped over 50 government organizations and over 300 players use these techniques to shape and support IT strategic planning, architecture, and IA processes within their respective organizations. Mr. Dupier has extensive professional experience in strategic and organizational planning, business change management, enterprise architecture, systems development, security, financial consulting, cloud computing, and technical consulting in both the public and private sectors. In this role, he works closely with CIOs and senior leaders in the development and execution of strategies, architectures, and systems that enable business processes within an organization. Mr. Dupier has also spoken at numerous conferences and professional events including Federal Office Systems Exposition (FOSE) 2009, International Association of Privacy Professionals (IAPP) 2009, FOSE 2006, the DCI Enterprise Architecture Conference 2005, Federal Computer Week's Wireless & Mobility Conference 2004, Billing World 2002, and eBill Exchange 2001. Mr. Dupier can be reached at iatac@dtic.mil.

US Cyber Command is Activated

On 7 May 2010, the United States Senate presented General Keith B. Alexander, US Army, with a fourth star and confirmed him as the head the Department of Defense's (DoD) newly formed United States Cyber Command (USCYBERCOM), a sub-unified command subordinate to the United States Strategic Command. A command activation and promotion ceremony was held on 21 May 2010, at Ft. Meade, MD where the new command will be headquartered. At the ceremony, Secretary of Defense Robert Gates remarked, "this new command will bring together the resources of the Department to address vulnerabilities and meet the ever-growing array of cyber threats to our military systems." The new command will combine the former Joint Functional Component Command - Network Warfare (JFCC-NW) and the Joint Task Force - Global Network Operations (JTF-GNO), focusing on offensive and defensive computer network operation missions.

IATAC has provided research and development for the JFCC-NW and JTF-GNO since their Initial Operating Capability. Such work has included providing the commands with cyber planning, strategy, policy, and cyber intelligence analysis, computer forensic research, knowledge management, and analysis for the development of standard operating procedures. IATAC was recently awarded two new contracts that will provide US Cyber Command analysis to achieve Full Operational Capability and beyond. Specifically, the work IATAC will perform will focus on the following areas:

"This new command will bring together the resources [to]…meet the ever-growing array of cyber threats to our military systems."

- **Evaluated level of assurance analysis and risk assessment**—As USCYBERCOM matures its cyber mission, it will rely heavily upon both technical assurance analysis and risk assessment to determine cyber capabilities, and to quantify the level of risk present. The results of this work directly impact Defensive Information Operations planning, and cyber capabilities analysis in response to cyber events.
- **Computer Network Operations capability development**—IATAC is now positioned to develop computer network operations capabilities with direct impact to countering terrorism. This work includes researching vulnerabilities, and reverse engineering technologies.
- **Cyberspace Operational Analysis**—IATAC will be positioned to assit USCYBERCOM's cyberspace operations and policy to ensure the nation is able to protect the cyber domain. This includes development of new cyberspace strategies and plans.
- **Cyberspace Intelligence**—IATAC will provide USCYBERCOM information assurance analysis to shape and serve as a focal point fusing time-sensitive cyber intelligence data, developing indications and warning methodologies, characterizing threat data, and developing processes to create actionable information allowing the US to attain cyberspace decision superiority.

These technical contributions will directly advance USCYBERCOM's larger mission to plan, integrate, and coordinate effective cyberspace operations across the DoD. This will provide strategic deterrence and security to US networks, infrastructure, information systems, and computer-based capabilities. ■

Maximizing the DoD Return on Investment in Cyberspace Professionals

by Juan Lopez, Jr. and Dr. Richard A. Raines

This article focuses on the challenges our nation faces in developing an information assurance (IA)/ cybersecurity workforce. Among these challenges is the trade-off between investing in human capital development versus accepting the resulting risks should this investment not be made. As with any investment, a profitable return is sought. This article sheds light on how the federal government is seeking to create and sustain the IA/cyber workforce it needs. Through examples, we show how the government is enjoying a high return on investment (ROI) from relatively small investments in the National Science Foundation's (NSF) Scholarship for Service (SFS) and the Department of Defense (DoD) Information Assurance Scholarship Program (IASP). [1, 2]

President Obama's declaration that cybersecurity is, "one of the most serious economic and national security challenges we face as a nation," asserts the importance of cultivating an IA workforce that can meet the cyberspace challenges facing our nation.

National Focus on Developing the IA/Cyber Workforce

The ability of any organization to create a high performance IA/cyber workforce and sustain a cyberspace skill set is challenging. Cultivating such a talent pool of IA professionals is even more difficult for the DoD given the additional constraints of security clearance requirements, age limits for military service, availability for worldwide service, and increased competition from the private sector. These challenges amplify the need for the DoD to improve the process to discover, select, develop, train, educate, and retain world-class cyberspace professionals. Several indicators have identified this shortfall as a major concern, but an effective plan to mitigate the problem has only received marginal attention. Highlighting this concern, President Obama's declaration that cybersecurity is, "one of the most serious economic and national security challenges we face as a nation," [3] asserts the importance of cultivating an IA workforce that can meet the cyberspace challenges facing our nation.

Since 1996, the Association for Federal Information Resources Management (AFFIRM) Emerging Issues Forum has conducted an annual survey of the senior federal information technology (IT) community to ascertain the most critical challenges facing the federal chief information officer (CIO). The survey respondents represent a good sample of the federal sector. In 2008, 15% of the responses were from the DoD or the Intelligence Agency category and 85% were from a civilian department/agency/bureau. [4] From a longitudinal perspective, the survey consistently indicates that security is by far the largest skill/knowledge gap of the IT workforce. [5] Furthermore, the year-to-year trend indicates that progress to close the gap is marginal. Accentuating this point, participants in the survey continue to rank "hiring and retaining skilled professionals" in the top five of the federal CIO "top ten challenges" portion of the survey (out of 25 challenges in 2008). This particular CIO challenge has been one of the top five challenges for the last 10 years. Of those 10 years, it has occupied the number one spot four times—twice within the last two years. No other challenge remaining in the current survey can claim the same distinction. [6]

Also, since the late 1990s, there has been an increased emphasis in understanding and developing capabilities in the cyberspace domain. National-level initiatives such as the National Strategy to Secure Cyberspace (2003), the National Security Presidential Directive 54/Homeland

Security Presidential Directive 23 (2008), and the Comprehensive National Cybersecurity Initiative (2008) have identified critical shortcomings and challenges our nation faces when operating in the cyberspace domain. The DoD, in turn, has also focused its efforts towards improving its capabilities in this domain (*e.g.,* formation of the US Fleet Cyber Command, US Air Force 24th Air Force, and most recently, the US Cyber Command). These actions and initiatives have been wide reaching, covering organizational policy, technology, processes, and people.

In July 2009, the Partnership for Public Service and Booz Allen Hamilton studied the current state of the federal cybersecurity workforce. The study found that the federal cybersecurity workforce continues to face serious shortages of highly skilled cybersecurity specialists and an absence of coordinated leadership on cybersecurity workforce issues. [7] According to the study, there exist four key challenges that threaten the quality and quantity of the federal cybersecurity workforce. They are:

1. The pipeline of potential new talent is inadequate;
2. Fragmented governance and uncoordinated leadership hinder the ability to meet federal cybersecurity workforce needs;
3. Complicated processes and rules hamper recruitment and retention efforts; and
4. There is a disconnect between front-line hiring managers and the government's human resource specialists.

Of the four key challenges, the inadequate pipeline of potential new talent continues to be persistent in light of its increasing importance. This article intends to direct the attention of enterprise leadership on two programs that are well funded, present no barriers to entry, have a robust process in place for candidate selection, have educational programs specifically designed to meet DoD cyberspace requirements, but are potentially underutilized to help allay part of the talent pool issue.

One of the most difficult areas to measure effectiveness is related to investment in developing human capital. It is difficult to quantify the value of education and/or training with respect to an individual. Given fiscal constraints, there will always be open discussions on a return on investment (ROI) with regard to education and training (E&T) versus the risk that will be assumed if E&T is marginalized. All too often, when budgets must be cut, one of the first areas examined for cuts is E&T. Many consider this decision to be detrimental to the long-term success of our nation. A current national E&T challenge is to produce and sustain the IA/cyber workforce in the face of restricted budgets and generational aversions to Science, Technology, Engineering, and Mathematics (STEM) education. Now, more than ever, a cultural change is needed to attract our nation's brightest young talent into the STEM disciplines.

Education should not be confused with training. In simple terms, training prepares an individual for the known (*i.e.,* checklists based on mature techniques, tactics, and procedures) while education prepares an individual for the unknown (*i.e.,* develops critical thinking and problem-solving skills). Advanced or graduate-level education cultivates an in-depth understanding of theories and applications not generally provided at the undergraduate level. This is particularly important as the nation and the DoD seek to develop the cyberspace professions.

Our Reliance on Cyberspace and Security Challenges Faced

As a nation, we rely heavily on cyberspace and its underlying infrastructure. This reliance ranges from entertainment to social networking, to commerce, and ultimately, to warfighting. Operations in the cyberspace domain pose new and interesting challenges for the nation and the DoD. First, it is a domain that has a very low cost of entry for participation. An extremely small investment allows a potentially disruptive source to operate

virtually uncontested within the domain. In this domain, the asymmetrical advantage nations possess resulting from large investments in technologies does not exist. Second, the domain is highly dynamic with new threats and vulnerabilities appearing daily. And third, because this domain is so dynamic, it is difficult for professionals to obtain and maintain the currency of knowledge needed for proficiency. Until the cyberspace domain evolves to a level of recognizable maturity, education will continue to play a key role in developing the human capital needed to successfully operate within the domain.

National-Level IA/Cyber Educational Investments

Recognizing the importance of education in developing cyberspace professionals, two federal government programs have been established to grow the number of professionals focusing on IA. These programs are the NSF SFS program and the DoD IASP. The NSF SFS seeks to recruit US citizens into IA-related education program (at the undergraduate and graduate levels) with an employment payback to the government equal to the time spent in school. The DoD IASP program consists of two subprograms: Recruitment and Retention. Similar to the NSF SFS program, the Recruitment portion of the IASP seeks non-DoD civilians through educational scholarships with post-graduation employment within the US government. The Retention portion of the IASP provides cross-educational opportunities to DoD civilians and military members for IA specializations. Graduates of the IASP Retention program incur service commitments in return for the educational scholarships. The SFS and IASP have served as the predominant sources for producing the IA professionals needed by the federal government. Beginning in 2001 and through 2008, 1,001 students have received IA scholarships and have graduated *via* sponsorship from the aforementioned programs. Roughly, 93% of these graduates have found employment with the federal government. While these numbers appear to be substantial, they reflect only a small percentage of the roughly 8,000 projected new IA/cyber hires by the federal government over the next four years. Additional demand will come from industry as IA/cyber-related initiatives drive the need for expansion. A key challenge in the near future will be to find enough qualified applicants to meet the growing needs for IA/cyber professionals. As programs such as the SFS and IASP seek to expand the number of scholarships they support due to increased funding, the national shortage of STEM-prepared students will make this expansion difficult.

IA/Cyber Educational Return on Investment (ROI)

Of the students mentioned previously, approximately 931 graduates from the SFS and IASP scholarship programs have been employed by the federal government. Here, we focus on a small sample of these graduates to demonstrate the ROI being realized by these programs. Specifically, we examine the impact of the Retention portion of the IASP *via* a small sample set of its graduates. The Retention portion of the IASP provides IA/cyber educational specialization opportunities to DoD military and civilian employees. These opportunities for long-term education span the military rank structure from mid-grade enlisted to senior officer with similar ranges across the DoD civilian ranks. The DoD has the potential to see an ROI from the education by placing the graduates into critical IA/cyber positions that will utilize their talents. The reason for the emphasis on "potential" in the preceding sentence is that operational and career advancement requirements do not always allow for the ideal placement of these graduates. However, ideal placement after graduation does not mean that cyber talent is wasted and that the programs fail to yield a beneficial ROI. In fact, the selected samples provide credibility that an adequate ROI can be realized even though the overall programmatic process can introduce delays in assignments to IA/cyber positions.

The below examples focus on a set of IASP graduates who were, and in many cases still are, applying the learning and honed problem-solving skills in post-graduate positions within the DoD. We specifically focus on a set of IASP graduates who received their graduate education from the Air Force Institute of Technology (AFIT) over the past seven years. In 2002, the United States Marine Corps (USMC) began an initiative to educate a portion of its IA workforce through the IASP Retention program. Since that time, seven senior USMC enlisted personnel and one naval officer, among others, have received Masters Degrees focusing on IA from AFIT. The below chronicles their post-graduate contributions to the USMC, the US Navy (USN), and the DoD as a result of this educational opportunity. While the number of personnel receiving this education is small, it should be considered a superb foundational corporate investment when considering the increased operational tempo the USMC and the USN have experienced since 2001.

- **Master Sergeant Brian K. Hamilton, USMC (ret)** came to AFIT with the first enlisted group in July 2002. After graduation, he was assigned as the Information Assurance Chief for the 3rd Marine Division in Okinawa, Japan. While in Japan, he deployed as the Information Assurance Officer for the Communications Detachment in support of the Tsunami relief effort in Banda Aceh, Indonesia. For his follow-on assignment, he served as the Information Assurance Officer for the 8th Communications Battalion

at Camp Lejeune, NC. After retirement, he became a civil service employee with an INFOSEC specialty as the Information Assurance Manager in the Management Information Department of the US Naval Hospital in Camp Lejeune, NC. He is a Certified Information Systems Security Professional (CISSP®). [8]

- **Master Sergeant Juan Lopez Jr, USMC (ret)** came to AFIT with the first enlisted group in July 2002. MSgt Lopez received the "Excellence in Research Award" sponsored by the Armed Forces Communications and Electronics Association (AFCEA) for research contributions characterizing electromagnetic interference of emerging 4th generation (4G) wireless technologies. After graduation, he was assigned as the Information Assurance Chief for US Marine Corps Forces, Atlantic (redesignated as US Marine Corps Forces Command in 2004) located in Norfolk, VA. During his payback tour, he served as a member of the newly established Marine Corps Information Assurance Assessment Team. Additionally, he is an adjunct faculty member for Saint Leo University teaching Computer Information Systems and participated as a SME to develop the question pool for the CompTIA Security+ examination. After retirement, he was hired as a Research Engineer at the Center for Cyberspace Research, AFIT at Wright Patterson AFB, OH. He is currently pursuing a PhD in Computer Science at AFIT. He is a Certified Information Systems Security Professional (CISSP®).
- **Master Gunnery Sergeant James Orlovsky, USMC (ret)** came to AFIT with the first enlisted group in July 2002. After graduation, he was assigned as the Information Assurance Chief for the First Marine Expeditionary Force (I MEF) in Camp Pendleton, CA. He also served forward deployed as the Information Assurance Chief for the Multi-National Force in Iraq. After retirement, he became a civil service employee with an INFOSEC specialty as the Information Assurance Manager for I MEF.
- **Master Sergeant Kelvin B. Scott, USMC (ret)** came to AFIT with the first enlisted group in July 2002. After graduation, he was assigned as the Information Assurance Manager for the 3rd Marine Expeditionary Force (III MEF) in Okinawa, Japan. He also served as the Information Assurance Chief for the 7th Communications Battalion at the same location. After retirement he worked as a Senior IA analyst for General Dynamics in Huntsville, AL and is currently employed with Mantech International as an IA Manager for US SOUTHCOM in Miami, FL.
- **Master Gunnery Sergeant Arthur Crawford, USMC** came to AFIT with the second enlisted group in July 2004. He is currently serving his payback tour as the Senior Information Assurance Chief at Headquarters, US Marine Corps. He is a Certified Information Systems Security Professional (CISSP®) and a Certified Information Security Manager (CISM®). [9]
- **Master Sergeant William King, USMC** came to AFIT with the second enlisted group in July 2004. He is currently serving his payback tour as a replacement for MSgt Scott as the Information Assurance Manager for the Third Marine Expeditionary Force (III MEF) in Okinawa, Japan. He is a Certified Information Systems Security Professional (CISSP®).
- **Master Gunnery Sergeant Terry Levoy, USMC (ret)** came to AFIT with the second enlisted group in July 2004. He served his payback tour as the lead for Network Defense Plans at the Marine Corps Network Operations and Security Command in Quantico, VA. Additionally, he is an adjunct faculty member at Germanna Community College teaching undergraduate courses in Computer Information Systems. After retirement, he was hired as an IA Future Operations Planner with Northup Grumman working at the Marine Corps Network Operations and Security Center in Quantico, VA. He is a Certified Information Systems Security Professional (CISSP®).
- **Lieutenant Commander Antonio T. Scurlock, USN** came to AFIT in 2005. After graduation, he served as the Component Information Assurance Officer and Computer Network Defense Lead for the Commander of Naval Forces Europe and Africa. He also served as the liaison officer to the United States European Command for Information Assurance and Interoperability testing. He holds a GIAC Security Essentials Certification (GSEC). [10] He is currently serving as both a Cyber Battle Captain in the Joint Operations Center (JOC) and a COCOM Tactical Capabilities Integrations Officer at the newly established United States Cyber Command (USCYBERCOM).

Where Do We Go From Here?

The above individuals represent only a small sample of graduates from the IA scholarship program. Although a list of specific individual contributions—which were many—are not enumerated here in detail, the intent is to demonstrate that it is essential for IASP graduates to be placed in critical IA/cyber positions to maximize the ROI. If the trend continues, such a strategy will undoubtedly provide a tangible contribution to the IA/cyber workforce shortfall and stabilize the IA/cyber expertise across the DoD. It is this type of investment in our cyber talent that

should be recognized and harnessed by those in a position of leadership. While undergraduate and graduate educations are important to develop the knowledge, skills, and abilities the nation needs with respect to IA/cyber, it is only one piece of the variety of actions that must take place to strengthen our cyber human capital. Initiatives to professionalize the IA cyber workforce as outlined in the IA Workforce Improvement Program will continue to be essential as it touches a larger population than possible with education. [11] Proper employment placement and career advancement opportunities for personnel with key IA/cyber skill sets are additional challenges. Above all, maintaining currency of expertise in the highly dynamic cyberspace operating environment will be challenging both fiscally and from a manpower viewpoint. To do so will take a long-term commitment by the nation to invest in the future. Long-term investments in STEM education and harvesting promising talent from within our own labor force must begin early. We must foster sustained commitments for years to come if we are to be a world leader in the cyber environment. ■

About the Authors

Master Sergeant Juan Lopez, Jr., CISSP, USMC (ret) | is a research engineer at the Air Force Institute of Technology (AFIT). He conducts cybersecurity research in supervisory control and data acquisition systems, radio frequency identification, and wireless sensor networks. He received a B.S. degree from the University of Maryland, an M.S. degree from Capitol College, and an M.S. degree from AFIT under the Information Assurance Scholarship Program. He is currently pursuing a PhD in computer science at AFIT.

Dr. Richard "Rick" Raines | is the director of the Center for Cyberspace Research at AFIT. Dr. Raines received a B.S. degree in electrical engineering from the Florida State University, an M.S. degree in computer engineering from AFIT, and a PhD in electrical engineering from Virginia Polytechnic Institute and State University. He teaches and conducts research in information security and global communications.

References

1. The Scholarship For Service (SFS) is a unique program designed to increase and strengthen the cadre of federal information assurance professionals that protect the government's critical information infrastructure. This program provides scholarships that fully fund the typical costs that students pay for books, tuition, and room and board while attending an approved institution of higher learning. Additionally, participants receive stipends of up to $8,000 for undergraduate and $12,000 for graduate students. The scholarships are funded through grants awarded by the National Science Foundation. Information is available at *https://www.sfs.opm.gov/.*
2. The Office of the Assistant Secretary of Defense for Networks and Information Integration (ASD (NII)) annually announces a DoD IA Scholarship Program (IASP) grant and scholarship competition. Information is available at *http://www.nsa.gov/careers/opportunities_4_u/students/undergraduate/iasp1.shtml.*
3. *http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure.*
4. *http://www.affirm.org/publications/cio-challenges-surveys-reports/AFFIRM2008CIOSurveyFinal.pdf.*
5. The AFFIRM Emerging Issues Forum has conducted annual surveys of the senior federal IT community to determine the most critical challenges facing the federal CIO. The survey has been conducted for 13 years. The results can viewed at *http://www.affirm.org/publications/cio-challenges-surveys-reports/AFFIRM2007FederalCIOSurvey-FinalReleased.pdf.*
6. Ibid.
7. Cyber In-Security: Strengthening the Federal Cybersecurity workforce, *http://www.boozallen.com/consulting-services/services_article/42415933?o42242052=*
8. The Certified Information Systems Security Professional (CISSP®) was the first credential in the field of information security, accredited by the American National Standards Institute to International Standards Organization Standard 17024:2003. CISSP® certification is an objective measure of excellence and a globally recognized standard of achievement. Additional information is available at *http://www.isc2.org.*
9. The Certified Information Security Manager (CISM®) certification program is developed specifically for experienced information security managers and those who have information security management responsibilities. The CISM certification is for the individual who manages, designs, oversees, and/or assesses an enterprise's information security. Additional information is available at *http://www.isaca.org/*
10. The GIAC Security Essentials Certification (GSEC) was created to provide assurance that a certified individual holds the appropriate level of knowledge and skill necessary for anyone with hands-on technical responsibilities in the key or essential areas of information security. GSEC is appropriate for security professionals who want to demonstrate they are qualified for IT systems hands-on roles with respect to security tasks. Candidates are required to demonstrate an understanding of information security beyond simple terminology and concepts. Additional information is available at *http://www.giac.org/certifications/security/gsec.php.*
11. The DoD Workforce Improvement Program (DoD 8570.01-M) provides guidance for the identification and categorization of positions and certification of personnel conducting IA functions within the DoD workforce supporting the DoD Global Information Grid. Additional information is available at *http://www.dtic.mil/whs/directives/corres/pdf/857001m.pdf.*

Dr. John Sokolowski

by Angela Orebaugh

This article continues our profile series of members of the Information Assurance Technology Analysis Center (IATAC) Subject Matter Expert (SME) program. The SME profiled in this article is Dr. John Sokolowski, at Old Dominion University (ODU).

Dr. Sokolowski is a leading national scholar and researcher in the field of modeling and simulation (M&S) and the executive director of ODU's Virginia Modeling, Analysis, and Simulation Center (VMASC). He was appointed to the position after working at VMASC for nearly a decade as a project scientist and research director. He has led over $10 million in research projects while working at VMASC. Additionally, he has led a number of research areas including Hampton Roads emergency evacuation and insurgency concerns in foreign countries. As part of his vision for advancing the field of M&S, Dr. Sokolowski intends to involve as many public and private Virginia universities as possible and has already developed a partnership of five state universities that will produce cutting edge research. Dr. Sokolowski is interested in both pure and applied research areas that will improve the M&S discipline and identify areas that can benefit the most from the discipline. [1] Dr. Sokolowski leads VMASC in the following formal research clusters:

- Medical/Health Care
- Military/Homeland Security
- Transportation
- Serious Gaming
- Social Sciences
- Computational Sciences and Artificial Intelligence
- Enterprise Engineering

Dr. Sokolowski stresses the importance of pure research within the formal research clusters at VMASC. In 2007, one VMASC pure research project, "Data, Models, Federations and Conceptual Links *via* Common Reference Models," received international recognition. This project examined computer simulation interoperability issues and proposed solutions that could have a significant impact in information assurance (IA). This project earned VMASC researchers "SIWzie" awards at the Simulation Interoperability Workshops in Genoa, Italy and Orlando, FL. These awards are given to the highest rated papers at recognized conferences. As Mike McGinnis, the executive director of VMASC and a retired brigadier general points out, Dr. Sokolowski creates conditions that have promoted high quality research at VMASC. [2] These conditions create the potential for significant M&S contributions to important organizations in IA and other fields.

Dr. Sokolowski, a retired Naval officer, was a leader of the M&S division of the US Joint Forces Command (USJFCOM). He led the M&S research and development effort that is now the centerpiece of the USJFCOM Joint Training Program. At VMASC, he continues to develop a cooperative relationship between ODU and USJFCOM through the creation of an ODU-USJFCOM Cooperative Research and Development Agreement tasked with building the next generation M&S architecture.

Dr. Sokolowski holds a bachelor's degree in computer science from Purdue University, a master's in engineering management from ODU, and a Ph.D. in modeling and simulation/engineering from ODU. His dissertation proposed a way to improve upon existing mathematical models of how leaders make decisions. In his research, he included information related to a decision maker's experiences and characteristics, and his research showed this model to be more realistic in predicting how a human would make decisions. [3] In 2009, Dr. Sokolowski published an M&S textbook titled "Principles of Modeling and Simulation – A Multidisciplinary Approach." ■

References

1. *http://www.odu.edu/ao/news/index.php?todo=details&id=20790*
2. *http://www.odu.edu/ao/instadv/quest/VMASCSokolowski.html*
3. Ibid.

Upstream Intelligence: A New Layer of Cybersecurity

(Article 1 of 3)
by Tyson Macaulay

Upstream Intelligence (UI) is information about specific Internet protocol addresses (IPs), domains and Autonomous System Numbers (ASNs) behaving in manners indicative of threats. This intelligence is derived from massive data sets available from carriers and service provider network elements. UI quantitatively identifies IPs, domains, and ASNs, which threaten online assets, whether they are classified data, personal information, industrial control systems, or business information like strategic plans or intellectual property. UI is a source of information available beyond the enterprise perimeter up into the carrier networks that form the bedrock of the Internet, and a place typically considered "no man's land." UI helps precisely identify active but ever-changing threat agents on the Internet among billions of benign devices and trillions of hourly communication sessions. With UI, a powerful tool becomes available to those seeking to protect not only online assets, but also the very networks that support them. Many of the UI capabilities discussed in this series are also espoused in the Cybersecurity Act 2009 (s.733), including information sharing and distribution capabilities, and are echoed in the 2010 Nation Broadband Plan from the Federal Communications Commission (FCC). [1, 2]

Despite its lawless reputation, at its lower levels, the Internet is actually a highly engineered environment that is being re-purposed to provide novel intelligence, enabling a new security layer to buttress any enterprise security program. UI and the resulting cybersecurity improvements could possibly become a de facto security element of enterprise networks in the coming years, perhaps even as commonplace as firewalls.

This is the introductory piece in a series of seven articles exposing the concept of UI. The following articles will dig into granular technical and business issues, challenges, and potential solutions around UI. As a solution, UI consists of proactive and accurate identification of compromised devices and networks on large scales in real time.

UI exists now. Large carriers use UI routinely on a day-to-day basis to recover vast amounts of their backbone infrastructure from illicit usage and abuse. In the case of Bell Canada, Canada's national carrier, forms of UI are deployed to substantial benefit, recovering up to 30% of the core network bandwidth – an enormous 75Gbps of bandwidth (approximately 20 full DVDs or 40 million pages of text every second) on a daily, peak basis. [3] This is not unusual among the large and modern carriers. Significant asset recovery was the reason Upstream Intelligence was developed and deployed in the first place, but this need only be the starting point of this capability. This series of articles will discuss some of the current capabilities associated with UI and suggest some of the places the security community can leverage capabilities.

Threats, Risks and Upstream Intelligence

Persistently changing and evolving threats and threat agents are driving up risks and elevating the need for new security capabilities to counter new risks. The new technical risks driving UI are largely related to the new breed of malicious software (malware) designed and distributed for criminal profit, state-sponsored offensive activities (spying) or ideological offensive purposes (terrorism and sabotage). This software manifests itself as the most successful form of crime and "violence" on the Internet: identity theft, credit card and banking fraud, spamming, phishing, and denial of service attacks.

UI identifies threat agents and targeted assets, rather than malware and the vulnerabilities they exploit. Malware increasingly passes undetected through firewalls, intrusion detection systems (IDS) and anti-virus (AV) systems. In some cases, these controls are less then 30% effective against known (previously identified) malware; in virtually all cases, vendors now include "generic" signatures for heuristic analysis (guessing) as a

safeguard against the new (previously unidentified) threats they cannot keep up with. [4, 5]

In the early 1990's to early 2000's, malware developers wrote viruses and worms that wreaked havoc by destroying data and systems, but it was more of a game. They claimed credit for bigger and more malicious infections and took pride in watching information technology (IT) managers scramble to stop the damage and fix systems, at huge expense. At that time, malware developers would share and publish exploit code. Now there is money to be made and strategic advantages to be gained through malware exploitation. Exploit code is shared less and the best code is not shared at all, rather it is guarded like an industrial secret. Prior to release, malware code is carefully and professionally tested against all known AV/IDS signatures using publicly available tools, and released into the wild in secret. [6] Malware code and testing is more the work of highly educated and well-coordinated teams, not brilliant loners working from basements.

Layered Security

UI represents a new layer of security for organizations of all sizes, and makes new capabilities possible when applied within existing security layers.

Layering security is the fundamental concept underlying "defense in depth." If a threat agent breeches one layer (typically the outer most perimeter) it should be immediately confronted by an underlying layer with a new security control or safeguard independent from the compromised layer. This concept applies equally to both physical and logical IT security, and has a long and illustrious career as a security tenet. Designing IT security in layers and the placement of the various security elements is referred to as the "security architecture." Architectures will consist of many layers, but the number will vary depending upon factors, such as the value of the assets being protected, the size of the organization, budget, and even the manner in which a given security practitioner assesses risks.

Typically, an organization would have an outermost security perimeter composed of a security router configured to drop the most obvious and typical sorts of attacks, such as port sweeps and scans. A second layer may consist of an outer firewall performing stateful filtering on traffic. A third layer may contain de-militarized zones (DMZs) for public facing network services such as email [Simple Mail Transfer Protocol (SMTP)] anti-virus and anti-spam services, domain name services (DNS), web services, virtual private network (VPN) services and many more. A fourth layer may consist of a physically distinct firewall device (ideally a different manufacturer from

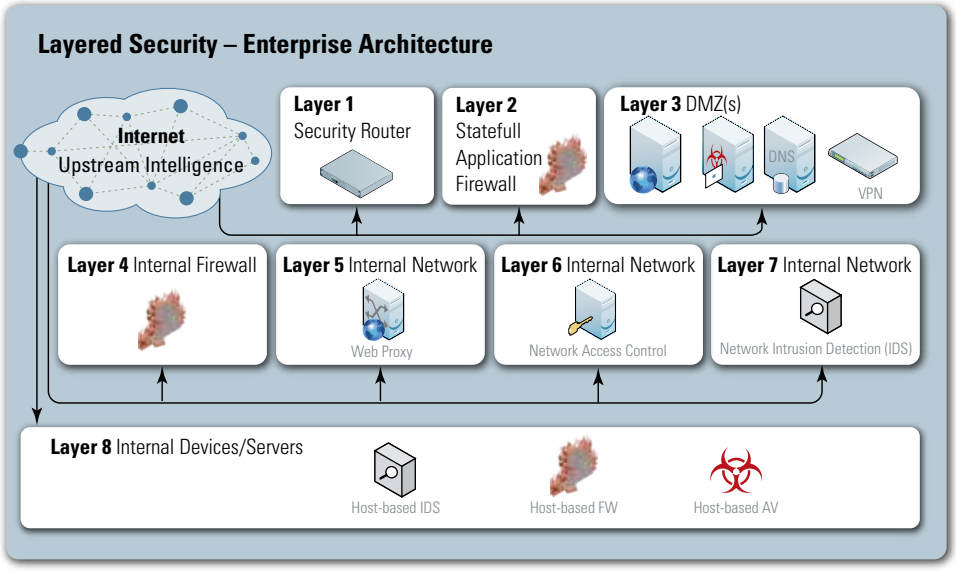


Figure 1 Layered enterprise security architecture with UI

the layer two/three device) that separates the DMZ devices from internal information servers. A fifth layer may consist of the proxy-service used to secure and monitor outbound traffic from internal sources. A sixth layer might include network access controls for all devices seeking to physically connect to the internal network. A seventh layer may be network IDS and related intrusion prevention services (IPS). Layer eight might be the host-based anti-virus, firewall and IDS loaded on every desktop and computer server. And the final layer may be the user access control login and credential services.

Figure 1 shows a logical representation of this example of a layered security approach with UI. UI provides two enhancements to the existing defense-in-depth designs. UI extends the enterprise perimeter by identifying potential threats before they hit the network perimeter, allowing for proactive treatment using existing security layers. For instance, security elements such as firewalls, proxies, or IDS can be configured with UI to recognize suspicious sources and destinations, rather than waiting for higher-level, more vulnerable session and application communications to begin, by which time it might be too late. [7]

Threat Agents Addressed Through Upstream Intelligence

UI exposes threat agent infrastructure. Table 1 is a simple overview of the prime types of threat agents mitigated with UI and the assets they typically target. Many threat agents are, in effect, a composite of several of the categories defined below, operating under several profiles according to where the opportunity for profit lies. The network elements and the threat agents they reveal are described in depth later in this series.

"Strike Back" and Cyber Offense

The collection, analysis, management, and deployment of UI are not about "strike-back" – launching punitive counter-attacks against those that appear to be attacking you. Furthermore, UI is not necessarily related to, or intended for, offensive capabilities. Such strategies are fraught in that they can inflict substantial injury on legitimate individuals and devices that are essentially victims too. They are unaware that they have been compromised by malware that now controls their computer system(s). UI should neither be associated with the debate about who, if anyone, should have responsive (offensive) activities against cyber-threats. Does the responsibility lie with the police, the military, or with extranational forces, such as NATO or the UN? Is it all or none of the above? [8]

UI has evolved inside large carriers and service providers for defensive purposes and self-preservation as opposed to being developed for offensive purposes. UI is a critical way to maintain network assurance in the face of threat agents that have absolutely no concern for the welfare of the network, even though it is their livelihood. That said, much of the value and intelligence available in UI is largely untapped at this time.

This is our opportunity to develop this capability further into a real-time system for information and intelligence sharing, and to identify threat agents and threatened assets on the Internet

Threat Agent	Profile	Targeted assets
Professional Bot Herders	Like malware wholesalers, they invest in the development and management of "bot herds," and then rent them out to any of the other threat agents.	Seek to gain control of devices to re-purpose them on-demand and rent or sell the "herd" to any and all of the other agents.
Organized Crime	Gangs and crime syndicates, often engaged in debit and card fraud, who find that security-chip card technology is forcing them online for better "returns."	Personal identity information for identity theft and multiple forms of fraud. Personal banking information.
Industrial Espionage	Mercenary-type entities hired to target specific corporate assets and industries.	Intellectual property, financial, and production information, plans and strategies
Foreign Intelligence Services	State-sponsored entities, possibly paramilitary, often operating from identifiable networks or geographic regions, if you can trace them.	National secrets, plans and strategies and industrial secrets, plans and strategies
Spammers	Specialize in harvesting legitimate email addresses from sources such as websites, blogs, social networks, webmail providers and any other possible source. Generate massive lists of addresses, both real and randomized/guessed to send junk-email (spam).	Individuals that will buy either (semi) legitimate products ("organic Viagra"), submit to fraudulent transactions or identity theft, pyramid schemes or fencing stolen goods.
Phishers	In close effort with Spammers, Phishers attempt to attract individual users to websites loaded with malicious software to compromise the user devices once they connect to a website, and gain access to contents or make them into "bots."	Individual fraud and identity theft, industrial espionage as described above, and public sector entities for national security assets.
Activists and Terrorists	Ideologically motivated entities typically without the resources to develop exploits independently, but with enough resources to hire compromised devices from herders or leverage off-the-shelf exploit "kits."	Industrial sabotage of assets (physical or logical), public sector entities, government and military for planning, strategic or national security secrets.

Table 1 Threat agents targeted by Upstream Intelligence

rather than continue to address the endless cycle of vulnerability patching and signature scanning.

Articles to Come in the UI Series

This issue of the *IAnewsletter* contains two additional articles about UI:

- The second article in this series is about the anatomy of UI and security. It describes the major elements and activities within a carrier or ISP network that combine to generate UI. It also includes a discussion on open and closed source information, which seeds the intelligence, and the types of events correlated from network elements to enhance UI accuracy.
- The third article discusses intelligence and information sharing at a business level. In the UI creation process, the more sources that can be engaged the richer the information set; however, competitive and proprietary instincts, laws and even public-funding can prevent such collaboration. Therefore, multiple business models for information sharing and intelligence synthesis should be reviewed and considered by policy makers, suppliers and consumers of UI alike.

Later editions of the *IAnewsletter* will feature articles on the following UI topics:

- Technical management and delivery of UI
- The relationship between UI and the world of privacy and compliance, including a discussion that samples precedent legislative and legal opinions
- Practical uses for UI, which demonstrate a wide variety of ways to increase organizational security, and
- Case studies, which demonstrate UI capabilities in real-world scenarios. ■

References

1. Cybersecurity Act 2009 - *http://www.govtrack.us/congress/billtext.xpd?bill=s111-773*
2. Federal Communications Commission, National Broadband Plan: Connecting America, 2010 - *http://www.broadband.gov/*
3. Bell Canada Q4 2009
4. *http://www.av-camparatives.org*
5. *http://www.av-comparatives.org/comparativesreviews/main-tests* - November 2009 results
6. *http://www.av-comparatives.org*
7. The author is referring to the seven layer OSI protocol stack, where source and destination information is contained in lower, network-levels and encapsulate higher-level session (i.e., TCP, UDP, ICMP) and application (i.e., *http,* smtp) protocols. Including the payload itself which might contain actual malware.
8. For further discussion see: Federal Computer Week, March 22, 2007 - Cybersecurity defense requires a good offense, *http://fcw.com/articles/2007/03/22/cybersecurity-defense-requires-a-good-offense.aspx;* The Washington Post, Jan 3 2010 Pentagon computer-network defense command delayed by congressional concerns, *http://www.washingtonpost.com/wp-dyn/content/article/2010/01/02/AR2010010201903_pf.html;* also Wired Magazine: Vigilantism Is a Poor Response to Cyberattack *http://www.wired.com/politics/security/commentary/securitymatters/2007/04/securitymatter_0405*

About the Author

Tyson Macaulay | is a Security Liaison Officer for Bell Canada, with 18 years of Information and Communication Technologies (ICT) security experience. Tyson works on security and risk management solutions for the largest organizations in Canada. He also supports the development of engineering and security standards through organizations like the International Organization for Standardization (ISO), and is a university lecturer and author of three books and many published papers. His books include: *Securing Converged IP Networks* (2006), *Critical Infrastructure: Threats, Risks and Interdependencies* (2008) and *Industrial Control System Security* (forthcoming 2010). Tyson's work on Upstream Intelligence has been driven by the need to proactively address the increasing frequency, longevity and severity of undetected ICT compromises which are threatening international security and prosperity. Further research and references are available at *www.tysonmacaulay.com.*

Anatomy of Upstream Intelligence

(Article 2 of 3)
by Tyson Macaulay

Introduction

This article reviews the anatomy of Upstream Intelligence (UI) and security. It provides a description of the major elements and activities within a carrier or service-provider network that generate UI. UI is not something that is discovered intact. It is often seeded from disjointed threat intelligence fragments that evolve and grow in clarity through the combination and correlation of quantitative indicators (a more detailed discussion of this process will be available in article 4 of this series). UI may be seeded from open source information, closed-source information, or developed "from scratch." The scratch approach requires more effort and resources and is usually a by-product of an investigation into active, but unrecognized attacks and zero-day exploits.

This article begins with a discussion on the usual seed sources of UI, as well as the application of the network elements that husband and nurture the seed base into usable UI.

Open-Source

Open-source threat intelligence information is freely available on the Internet through groups with open memberships or simply posted to websites. Lists of suspected "bad" Internet protocol (IPs) addresses (such as spammers, distributed denial-of-service [DDOS] attackers, nefarious domain name system [DNS] servers, or web-hosting sites) are published by various security vendors, as well as unaffiliated/not-for-profit sites dedicated to security, such as the Spam and Open Relay Blocking System (SORBS) or SpamHaus. [1, 2] Open source intelligence also includes the signatures and profiles of known malware, available from a source like the US Computer Emergency Readiness Team (US-CERT). [3] The quality of open source security information is as diverse as the available suppliers. In the end, a lot of excellent information is available on an open source basis, but one thing can also be generally counted on—the best and most up-to-date security and threat information reaches open-sources last. In a world where threats can change minute to minute, and security posture changes at the same rate, open source information ranging in age from hours to days or weeks only begins to address the enterprise needs for cyber threat intelligence.

In a world where threats can change minute to minute, and security posture changes at the same rate, open source information ranging in age from hours to days or weeks only begins to address the enterprise needs for cyber threat intelligence.

Closed-Source

Closed-source information is not publicly available and is associated with information security operations, intelligence gathering, "softer" business, and professional relationships, particularly among carriers and service providers, of which there are approximately 1600 worldwide. [4] These carriers and service-providers share intelligence about compromised devices and networks on a practical and symbiotic basis at the engineering level, even while they may be harsh competitors at the management level.

Customer complaints are another form of closed-source information; persons or businesses attempting to cope with degraded network service will usually contact carrier or service provider because they figure (wrongly) that the degradation they are experiencing is related to a network problem. Such support calls frequently reveal severely compromised machines, much to the surprise of their owners

who are frequently running some form of reputable anti-virus or intrusion detection software.

Information fusion among open and closed sources occurs now, without the cost of complex information sharing methodologies or large teams in fortified 24/7 operations centers. These are mostly unfunded systems using *ad hoc* or improvised tools, frequently within carrier operations centers—the last line of defense against cyber attacks. These *ad hoc* tools and processes are effective for their stakeholders by providing a primordial form of UI, by applying open and closed-source threat intelligence within network elements, such as switches and routers. The discussion to follow will seek to build up from these initial approaches for UI creation.

Cooking from Scratch

Rather than harvesting a bulk list of suspect IPs, domains and autonomous system numbers (ASNs) from open and closed-sources, seed intelligence can be "cooked from scratch" through forensic processes where a degraded device is diagnosed and traced to external sources. Scratch sources often start with a single device exposing an external malicious entity, which under observation at the enterprise or optimally, the carrier-level, exposes its relationships with other malicious or compromised entities. The typical approach would begin with the identification of the device suspected of compromise. The network communication patterns and protocols of these devices are closely observed for relatively simple criteria, such as outbound destination, port and protocols, and especially the timing and traffic characteristics. Some of the most popularized UI investigations have started from scratch sources, such as the recent GhostNet research. [5]

Network Elements

Open-source, closed-source, and scratch seed information needs to be aggregated, correlated, and combined with observations from various network elements to form UI and tools like "heat maps" of compromised internal and external devices, as revealed by what they are doing on the Internet at large—not through signature based file inspection.

At a minimum, four major information sources can be combined with seed information within carrier and service provider networks. This process generates much richer information about the activities, intentions, and operating modes of the compromised devices and threat agents. These information sources are: traffic flows, DNSs, messaging infrastructure and peer-to-peer (P2P) infrastructure.

Traffic Flows

Most, if not all, large carriers and service provider networks will employ systems for monitoring the flow of traffic through the network junction points, both internally and at borders with other providers. A typical means of doing this is with a proprietary, but widely supported protocol from Cisco called NetFlow. [6] NetFlow allows providers to maintain a picture of traffic flows and volumes—basic tools for managing network quality and assurance. This information is also useful for understanding the threats posed by entities using the network for illicit and malicious purposes. Basic information supported by NetFlow includes source IP address, destination IP address, source port, destination port, IP protocol, ingress interface to the network, and some information about the type or quality of service associated with the traffic. NetFlow does not capture packets or payloads, and is not a content/media interception technology.

Analysis on large carrier traffic flow statistics (*via* NetFlow) is like a satellite view of road conditions—taking in an entire region or country at once with the ability to zoom down to very granular activities. Traffic flows can show ambiguous devices talking to suspicious destinations, and devices being scanned and probed from suspicious locations. However, traffic flow alone can be inconclusive because the Internet is

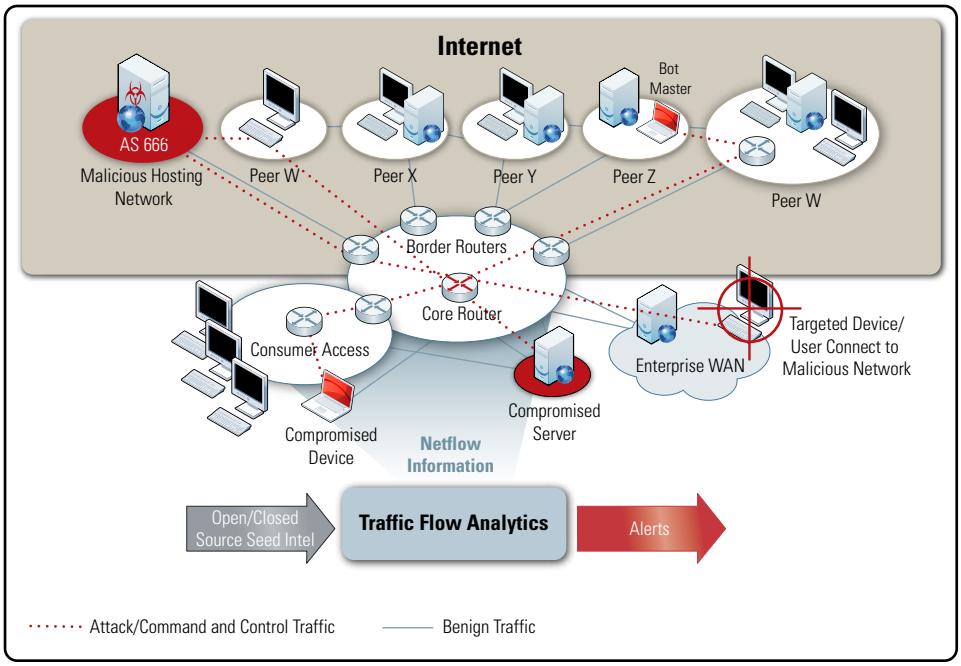


Figure 1 Traffic Flow Intelligence

made up of many independent carriers and service providers that do not share traffic flow data (for competitive and proprietary reasons) - therefore rendering observations incomplete.

Figure 1 illustrates where traffic flow data for UI might be derived from a carrier or large service provider network. If intelligence about a malicious or compromised device or network can be seeded, centralized traffic flow analytics can reveal the devices communicating with the seeded IPs, domains, and ASNs and flag them as suspicious.

Traffic Flow Caveats

There are challenges to gathering traffic flow information. For instance, logically, it is an expensive process because it burdens the routers. Traffic flow statistics gathered for typical operational purposes may only sample packets at rates of anywhere from 1:100 to 1:10,000. This provides sufficient information for network management, but can also result in lost or incomplete intelligence. Capturing traffic flow statistics on a 1:1 basis (receiving information for roughly every packet) is not practical for most operations oriented infrastructure. Requiring a specialized security infrastructure. Similarly, many indicators from traffic flow analysis will be inconclusive without examining the entire packet or data stream, a capability substantially beyond traffic flow analysis infrastructure.

Domain Name Service

Domain name service (DNS) is one of the Internet's most critical workhorses. It is a part of all IP infrastructure and essential plumbing. DNS translates human readable addresses (Ex. *www.address.com)* into a machine readable and routable address (Ex. 123.255.255.255). If DNS fails we all know about it very quickly because most or all IP-based communication will slow down or come to a stop. DNS is also a key infrastructure to threat agents who rely upon like everyone else, and frequently seek to compromise it. DNS service compromise can result in a wholesale fraud of dependent users. [7]

DNS infrastructure in carrier and service provider networks is large, and supports millions of users and queries at a scale beyond most enterprises. Through this scale, DNS can provide valuable forms of UI, for instance: which devices have been compromised by malware, who is attempting to control the compromised devices, who is launching attacks against specific assets, and where are they maliciously redirecting users (typically a compromised server). [8] Typically, the worst forms of malware encode a DNS name as the "call-home" command-and-control (C&C) address once a device has been compromised. Using a DNS name rather than an IP address provides the botmaster (controller of the malware) with the ability to change C&C servers to avoid detection and for redundancy. Awareness of DNS names being used for C&C operations allows DNS operators to set alerts whenever the C&C domain name is queried, and then commence response operations. DNS records may reveal useful information, such as the IP address of the victim, the machine's operating system, the time the malware was installed, the variant of malware active, and of course the C&C address itself. Alternately, DNS lookup statistics can reveal incongruous matches between IP addresses and domain names, or where a legitimate website has its users redirected to malicious servers masquerading as a legitimate site (an attack form known as 'pharming') in an effort to steal identity information and/or infect devices.

Figure 2 illustrates DNS infrastructure designs that provide substantial UI through the queries made by both consumers and businesses. This diagram shows enterprises routing their DNS queries through a carrier or service provider, where logs can be aggregated for common benefit—however, this is not a mandatory design.

DNS Caveats

Gathering DNS intelligence is greatly facilitated by large, centralized DNS services with large user bases. While consumer based ISPs often have this infrastructure design in place, many enterprises do not. Instead, they have DNS services scattered throughout network domains without centralized logs. Similarly, internal users might be pointing their computers to external DNS services,

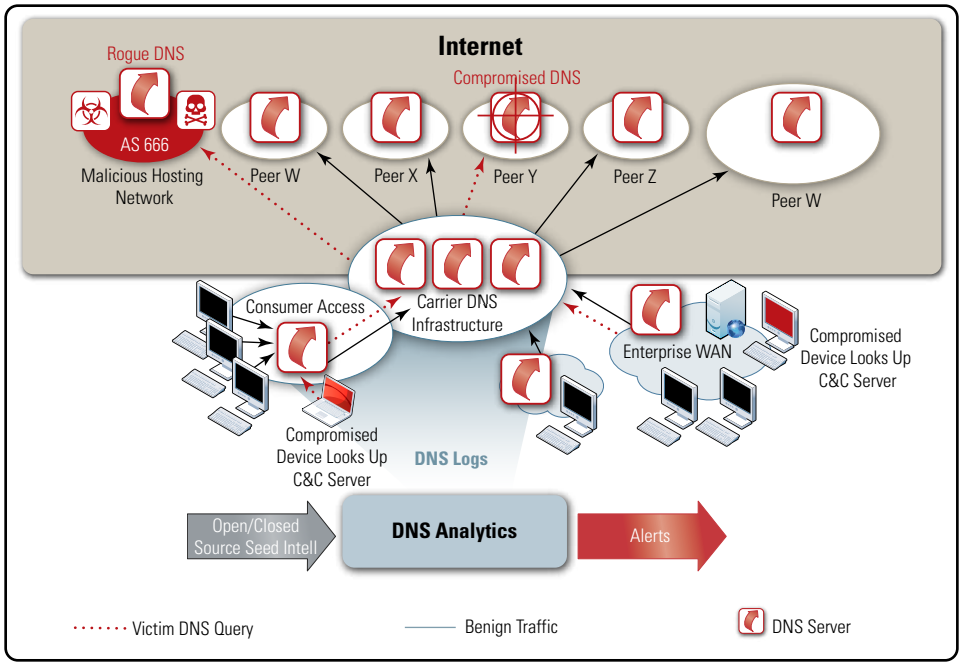


Figure 2 DNS Intelligence

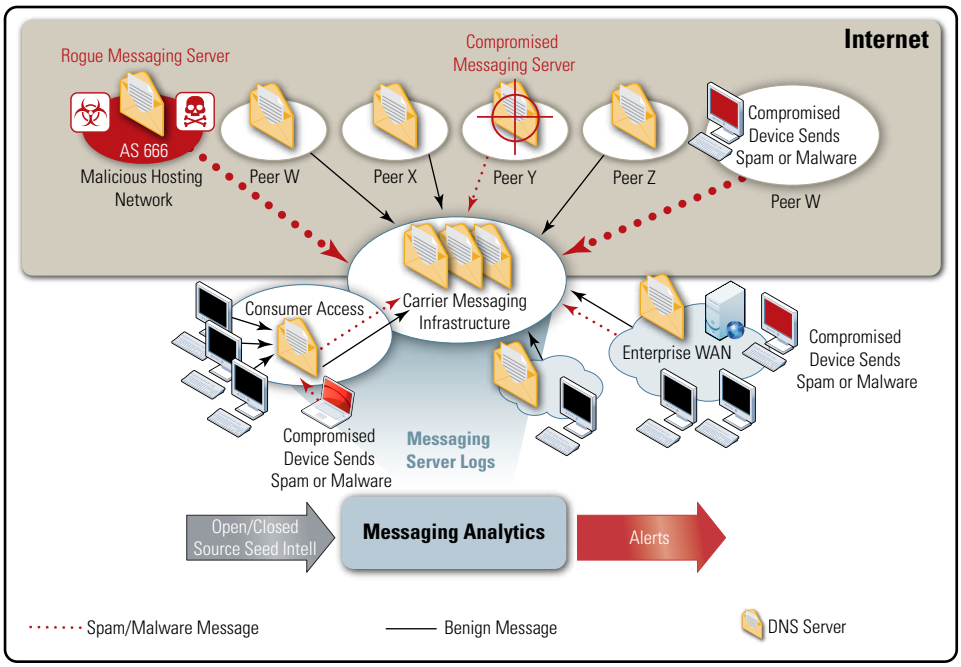


Figure 3 Messaging Intelligence

where the lookup transactions are simply not seen. To maximize DNS intelligence, organizations would need to centralize logs and disallow external lookups, for instance by denying most systems access to port 53 (the default DNS query port) on firewalls. Similarly, to maximize diagnostic and forensic capabilities, DNS logs need to be both extensive and maintained for weeks or months, a resource intensive and expensive demand.

Messaging (E-mail) Infrastructure

Messaging infrastructure for filtering viruses, phish and spam is increasingly deployed in the core carrier and service provider networks, as more than 95% of e-mail on the Internet is illicit, junk, or malicious. Entities that elect to host and manage independent messaging infrastructure must dedicate more resources to deal with the illicit messaging arriving at their perimeter, including: 1) more bandwidth to carry bad messages to the perimeter; 2) more filtering software and servers; and 3) more people to keep the servers running. This situation represents an efficiency opportunity in the trend towards outsourcing message cleaning. A significant by-product of large-scale message cleaning is the intelligence available as illicit or malicious messages are being filtered.

Messaging infrastructure will usually support a variety of filters. It is useful to understand the nature of these filters because the intelligence reports they generate can be applied to proactive (versus purely reactive) threat and risk management. The first distinction among different filters involves “inbound” and “outbound” message filtering. Inbound filtering relates to messages arriving at the messaging aggregation point from domains external to the destination domain. Inbound filtering metrics indicate threats to the organization, enterprise, or user base. Outbound filtering relates to messages from an organization destined for external domains. Outbound filter reports are of particular interest because they can indicate compromised internal devices, which often manifest their degraded state through the illicit e-mail messages they start producing. [9]

Figure 3 illustrates messaging intelligence sources, as they may be available from service providers hosting centralized cleansing infrastructure. Inbound messages sent to protected domains can provide information about targeted attacks on branded assets and help identify machines that may have been compromised as sending sources. Filtered outbound messages may indicate that an internal device has been compromised and is attempting to use preconfigured messaging services for illicit purposes.

Like DNS queries, messaging intelligence is most efficiently derived from large, centralized infrastructures. While some enterprises have shifted or are shifting to upstream/outsourced infrastructure, many continue to support internal and dispersed infrastructure.

Messaging Caveats

Like DNS queries, messaging intelligence is most efficiently derived from large, centralized infrastructures. While some enterprises have shifted or are shifting to upstream/outsourced infrastructure, many continue to support internal and dispersed infrastructure. Gathering messaging cleansing logs from dispersed enterprise assets, possibly from a variety of vendor solutions, is a significant challenge to message intelligence. Similarly, as with traffic flow and DNS, log management and archiving is an expensive operation.

Traffic Shaping Infrastructure

Traffic shaping infrastructure is widely used to manage huge traffic volumes associated with the mostly illicit activities of P2P systems that threaten the overall network. [10] Traffic shaping infrastructure is another key network element used in the generation of UI. Traffic shaping analysis involves real-time inspection of Internet traffic streams looking for telltale signs of P2P applications such as Kazaa, eMule, bitTorrent, and a range of similar tools. These applications distinguish themselves not just by large bandwidth consumption, but also by the ports and protocols they use, the format of the payload, and the P2P coordination server addresses they communicate with. Traffic shaping infrastructure has become critical to carriers, and is credited with reclaiming a substantial part of the Internet from activities that threaten the assurance of the whole system, not just copyrights on music and movies. [11]

In considering traffic shaping infrastructure for UI, both proactive and reactive capabilities become apparent. Proactively, traffic shaping can function as detection infrastructure—monitoring and issuing alerts when P2P sessions are initiated from within a domain, gateway or specific IP address. P2P protocols are frequently used for command and control signaling by malware and botnets. Similarly, many P2P clients are embedded with malware, which will support file sharing according to user expectations, but will also index and surreptitiously expose everything on the host computer and any available network drives. In this way, personal or corporate information residing on the system or local network will become exposed to the P2P network. Analysis of P2P search strings cascading through the file sharing networks shows evidence of many queries related to espionage and identity theft. [12]

Figure 4 illustrates centralized traffic shaping infrastructure managed by most large carriers. This infrastructure will detect and cap the bandwidth consumption of individual IP addresses.

Traffic Shaping Caveats

Like the other large UI sources, P2P intelligence has challenges. This infrastructure, as it typically operates today, can manage vast amounts of traffic, but logging and reporting on dozens of gigabits per second and thousands of terabits per day is computationally very expensive, requiring major investments given normal traffic-shaping infrastructure does not log anything. Another weakness in traffic shaping UI is that the

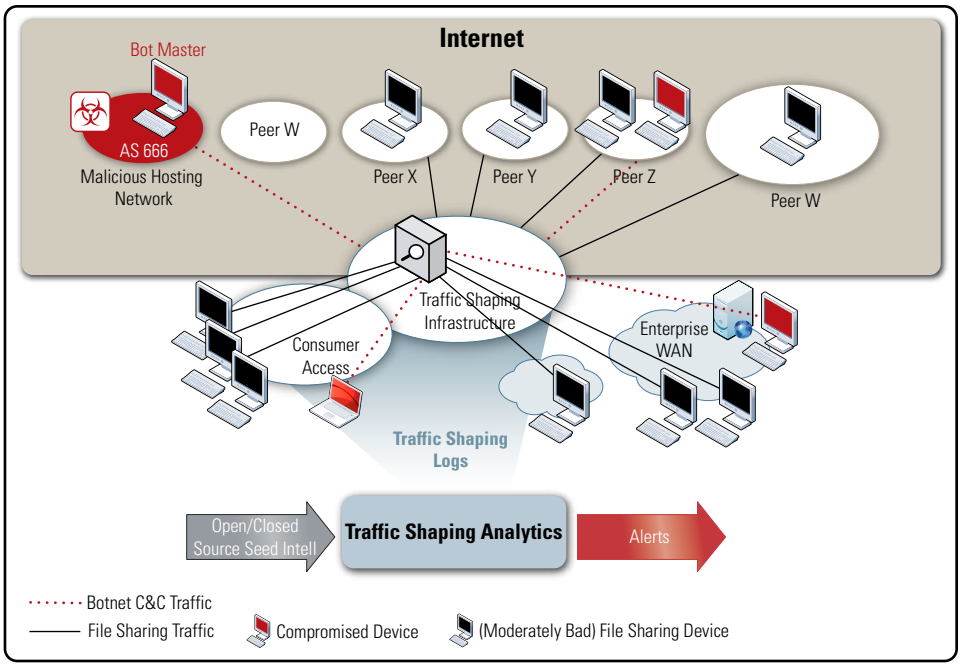


Figure 4 P2P Intelligence

payloads can also be encrypted (a simple configuration option for most client packages), which can make P2P traffic harder to distinguish.

Web Proxy Intelligence

An additional source of UI typically available at the corporate rather than carrier level is the web proxy server logs. Most large organizations will implement web proxy servers for internal users accessing external resources on the web, but also for other services like *FTP*. These proxy servers have a variety of useful security purposes, from managing traffic consumption internally to limiting the types and content of web pages that users access. Web proxy settings are generally part of the corporate browser configuration and read by any desktop/local software needing access to Internet resources, including malware. Therefore, web proxy logs can be a good source for intelligence when seeded with information about known, harmful IPs, domains, and ASN where malware would communicate for command and control purposes. To the extent that web proxy traffic logs are available, they are an excellent source of intelligence especially when combined with seed information and correlated with traffic flow, messaging, DNS, and P2P intelligence at the carrier level.

Conclusion

No single network infrastructure element can identify all compromised devices, even if deliberately configured and deployed for this purpose. The combined and correlated security capabilities of several infrastructures seeded with quality threat information (open-source, closed-source, or scratch) is required. This approach is more practical considering that dramatic reconfiguration and investment in of existing infrastructure, such as traffic flow, DNS, messaging, traffic shaping or web proxies, may not be possible as costs in processing power and storage could be prohibitive. However, smaller incremental improvements in each infrastructure element to do a little more can add up to the needed capabilities.

The UI sources discussed in this article will generate vast amounts of information that must be efficiently managed to be viable and valuable. UI will change, decay, and expire very quickly. Article 3 of this series will discuss potential business models to effectively support UI management, while subsequent articles will present technical options and discuss privacy issue concerns associated with this scale of information collection, correlation, and generation. ■

References

1. *http://www.us.sorbs.net*
2. *http://www.spamhaus.org*
3. *http://www.us-cert.gov/*
4. A "major" carrier can be large in terms of customers, coverage or simple dominance in a market (IE, a national monopoly or duopoly)
5. *http://www.scribd.com/doc/13731776/Tracking-GhostNet-Investigating-a-Cyber-Espionage-Network*
6. *http://www.cisco.com/en/US/technologies/tk648/tk362/technologies_white_paper09186a00800a3db9.pdf*
7. Nominum, Layered defenses to prevent DNS cache poisoning; Whitepaper 2009, *http://www.nominum.com/*
8. At the highest level, there are two distinct variants of threat: "threat-from" and "threat-to."Threat-from is about the threat agent and the resources and characteristics of a given agent. At the coarsest level, some threat-from information is free and widely available from sources like CERT, MacAfee, Symantec, Counterpane and plenty of others. Like threat-from information, coarse threat-to information is also publicly available from sources such as the Department of Homeland Security / Public Safety Canada, Information Sharing and Analysis Centers (ISACs) and a variety of other open sources. These sources may provide information about which industries or sectors appear to be experiencing generalized threats. This type of public domain threat-to information is of limited value because it does not contain specifically actionable intelligence either. Ideally, threat-to information will contain detailed metrics such as asset ownership, asset names and locations (physical and logical), asset role, asset interdependencies, asset valuation, and business impact assessments. This sort of threat-to information is rare, never in the public domain and highly sought-after by industry; it is highly tactical and can support detailed response and remediation, especially when combined with detailed threat-from information.
9. For a more detailed discussion of messaging filter-types see: Macaulay, Tyson, Upstream Security, July 2009 *http://www.tysonmacaulay.com*
10. See Census of Files Available *via* BitTorrent *http://www.freedom-to-tinker.com/blog/felten/census-files-available-bittorrent*
11. Bell Canada internal findings related to return on investment for P2P analysis and management infrastructure.
12. Lili Shue, Peer-to-peer networking security and controls, IT Governance Institute, 2003; *http://www.enhyper.com/content/p2psecandcontrol.pdf*

Business Models of Upstream Intelligence Management and Distribution

(Article 3 of 3)
by Tyson Macaulay

Introduction

Upstream Intelligence's (UI) ability to combat cyber threats is, in part, determined by the business model employed. Business models impact the collection, management and distribution of UI.

This article discusses how business models affect UI based on one of two assumptions. The first assumption is that there is an optimum business model for UI collection and management, rather than multiple ways to achieve the same degree of accuracy and timeliness. The second assumption is that UI possesses monetary value and may be bought and sold. Under the first assumption, this article discusses a theoretically optimum structure for UI collection and management at a business level. Under the second assumption, this article addresses the pros and cons of available business models, including commercial, not-for-profit, and government (public sector) ownership/management. Distribution of UI is the subject of a distinct, subsequent article.

UI in the World Today

The precursors of UI exist today in a variety of forms from a variety of sources, such as product vendors, voluntary associations, government funded information sharing and analysis centers (ISACs), cyber intelligence boutiques, and network providers. The information and intelligence available from these sources vary in utility and resemblance to the target UI (as described in articles 1 and 2 of this series), but are important elements in the UI ecosystem's evolution. [1]

Security product vendors increasingly offer subscription-based "feeds" related to malicious domains or compromised IP adresses that have been observed in members of their client-base. This client-base elects to share data from the vendor-solutions it has purchased. Security product vendors may also aggregate events from clients around the world, and receive/retrieve suspicious and overtly malicious binaries for identification and fingerprinting.

Open-sources from voluntary peer associations dedicated to stopping spam, bot-nets, and other malicious activity generate UI based on member contributed intelligence and independent research. This information is often available for free to members or to special consumers such as law enforcement; sometimes it is freely available to all consumers. Often membership is open, but from time to time it is closed or limited to "invitation only."

ISACs are a contemporary example of intelligence aggregation refineries in the civilian world, though they are usually the result of a government subsidy with some private sector participation. ISACs collect, analyze, and sometimes correlate open and closed-source intelligence, possibly about both cyber and physical threats. The resulting ISAC cyber intelligence is often vulnerability related versus threat information, targeted at industry specific users often available only to enrolled members.

National carriers and service providers have large volumes of cyber intelligence available to them through their native infrastructures and subscriber bases. In the case of the carrier, much of this information is founded on network observations and heuristics associated with IP addresses, domains, and Autonomous System Numbers (ASNs) acting in ways that affect network assurance through illicit or suspicious activities. These capabilities are not predicated upon signature based analysis and therefore detect activity resulting from both known and unknown malware. UI capability can also be found in professional cyber intelligence refineries and boutiques. Refineries are akin to a second or third level processor of intelligence taking feeds from multiple sources, aggregating and cleansing, and re-selling the result. Boutiques tend to develop their own primary research through independent observation and analysis, typically seeded from open and closed sources and proprietary open and

closed sources and proprietary honeypots. [2] In either case, boutiques and refineries add value through sophisticated correlation, weighting, and distribution capabilities.

It is likely that all of these (non-exhaustive) sources will be tapped in the course of creating optimal UI, which benefits immeasurably by seeding from a variety of feeder sources. No single source of security observations can independently generate comprehensive threat intelligence: collaborative seeding is mandatory.

Collection Networks

Business models associated with UI will in part be defined by their collection network for (open and closed-source) seed information. To the extent possible, collection networks should include a variety of different sources and ideally be composed from as many viable sources as possible. The fundamental reason for extending the range of sources is a matter of sample richness, resiliency, and redundancy. Sample richness is a simple concept: the larger the sample, the greater that chance that a given malicious IP, domain or ASN will enter the sample pool for assessment. Resiliency and redundancy of the seed sources is critical, because the time when users' most benefit from UI may also be the time that seed sources and UI suppliers are also under stress and prone to degradation. Network theory and the associated models and empirical proofs found in nature show that a UI system would benefit from adopting looped structures with many overlapping, multi-tiered suppliers relationships. [3, 4]

Figure 1 depicts a contemporary information sharing structure found throughout the Internet. This is the foundation level for UI seed information—composed of product vendors, volunteer associations, and refiners/carriers as described earlier. These entities, to greater or lesser extent, depend on one another to validate and enrich their data sets through information sharing. Consumption and sharing rates among the entities vary significantly according to cost and availability, but they all consume all of the open-source information for reprocessing purposes. Some will share closed-source information under quid pro quo agreements, or purchase subscriptions. The sharing "circuits" tend to develop according to who knows whom and, as importantly, who is competing with whom.

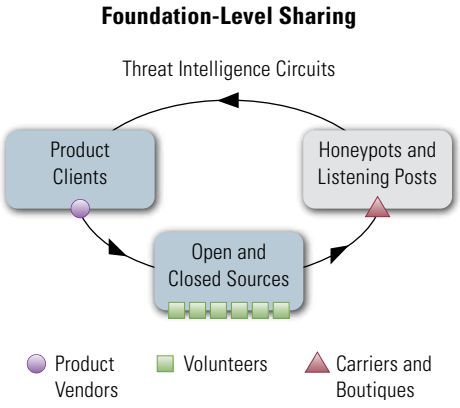


Figure 1 Micro Level Threat Intelligence Sharing Circuit

A subsequent intermediate level of information sharing related to threat and seed information for UI exists above the foundation level. At this level, there are approximately six different types of communities: web, domain name system (DNS), network, peer-to-peer (P2P), messaging and anti-virus (AV)/malware. These broad communities exist today, having evolved as a matter of commercial market opportunities (which defined the vendors) and personal interests (which defined the volunteers). Membership in these communities is neither restrictive nor prescribed; entities may be members or suppliers to several, though not usually all, communities. Unlike the community level, sharing between communities at the intermediate level is inconsistent. Each community possesses independent capabilities to generate its own intelligence, but many of the IPs, domains, and ASNs identified by one community are identified in the others. Similarly, they all possess false positives or expired intelligence, which is detected and expunged at different rates. The intermediate level is where UI management improvements need to

start creating a richer, more resilient, and redundant body of seed information to power highly effective UI.

UI will be best seeded and supported by a final, highest (theoretical) macro-level of cyber threat information sharing shown in Figure 2. This level of sharing involves tapping as many (if not all) the community level sharing networks that have probably developed independently according to geographic, linguistic, and cultural attributes of the members. Combining these sources has to be a very deliberate act and requires the introduction of weighting capabilities applied by a correlation and refinement engine to address the wide variations in suppliers and client subscribers. Once a weighted and correlated set of seed information about suspect IP, domain, and ASNs is compiled, it can be applied as a filter on raw network flows (at the carrier or enterprise level) to reveal previously undetected, suspicious communications.

The advantage of deliberately structuring threat aggregation systems according to this model is that a wide range of independent sources can be used for seeding UI. The constant incorporation of "loops" from micro level structures to community level structures injects substantial redundancy and resilience into the system. If one part of the feeder network is disrupted or even compromised, the remaining loops can compensate through alternate data pathways. Under these structures of loops within loops, it is less likely that a threat IP, domain, or ASN will appear from only one source. Conversely, to the degree threat information is compiled using few sources and no loops, the more prone it will be to gaps, blind spots, and the injection of misinformation.

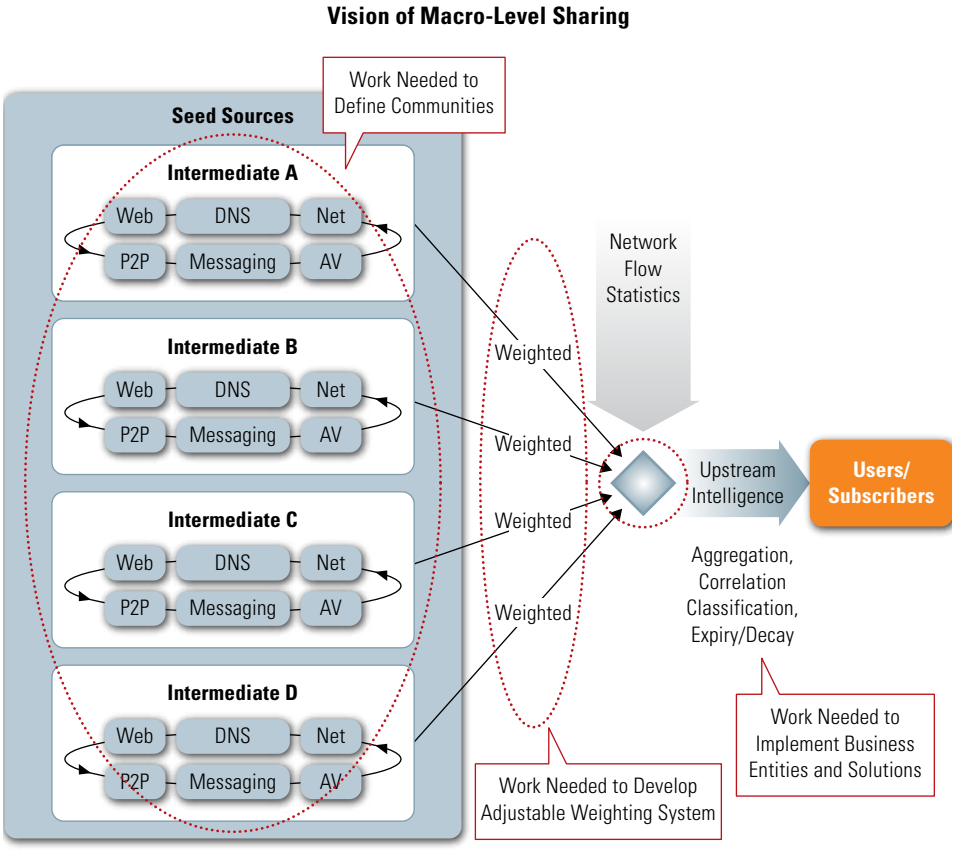


Figure 2 Macro Level Threat Aggregation, Weighting and Refinement

Value-Added Weighting and Refinement at the Macro Level

Beyond mere aggregation and correlation through hierarchical intelligence loops, UI seed information generates further value. Network flow statistics from bulk sources such as Tier-1 carriers with seed intelligence will allow for final extraction of UI: the (potentially real-time) identification of zero-day threats and newly compromised devices. As illustrated in Figure 2, the value-added process includes at least three elements: aggregation-correlation of the seed information with network traffic statistics (from sources such as traffic flow, messaging, DNS and P2P infrastructure); classification of results for reliability and sensitivity; and expiry/decay rating. At a minimum, these attributes will impact the application of resulting information for UI purposes.

Another value-added process that any UI management service-provider will clearly require is the management of "rehabilitated" IPs, domains, and ASNs and false positives. Frequently, owners of compromised devices will become aware of a compromise and fix the problem; but in the meantime, these owners may remain on a variety of black (bad/compromised) or grey (suspicious) lists, which inhibit their ability to conduct business. UI managers will need to develop appeal processes and automated processes that recognize when correlation scores start to fall for a given piece of UI. A rising score would indicate an increasing number of sources reporting a malicious or compromised IP, domain, or ASN. A falling score would indicate that a malicious or compromised IP, domain, or ASN may have been recently rehabilitated.

UI Management Models

UI management of the structures just discussed can be undertaken through a variety of business models as there are no specific organizations that must

perform this role. It is worth reviewing a few of the broadest categories of potential UI management organizations–because while there are several alternatives, each comes with different advantages and challenges.

Government/Safety

Public safety is enhanced by UI, especially when considering it can be used to protect everything from critical infrastructure to personal privacy. For this reason, government or safety entities have a legitimate interest in managing UI services. Government and safety entities also possess a certain amount of moral authority and public trust, which could accelerate UI adoption and deployment, to the substantial benefit of business and society. Recent proposals for government-led information sharing capabilities might be found in the recent Federal Communications Commission's (FCC) 2010 document, "Connecting America: National Broadband Plan," which calls for the Department of Commerce's (DOC's) National Telecommunications and Information Administration (NTIA) to establish a, "National Broadband Clearing House to promote best practices and information sharing." [5, 6] In this report, the FCC explicitly calls for the creation of a "cybersecurity information reporting system" to be run by the FCC and Department of Homeland Security (DHS) in collaboration. [7] Either of these possible creations may plausibly lead to government-supported UI management entities.

Simply because government or safety entities can undertake UI management does not mean that they should. Placing cliché concerns about the speed and efficiency in the public sector aside, there are other challenges that need to be considered. Initially, unlike a private sector capability, a public sector UI solution could be negatively influenced by political decisions regarding how UI seed information is gathered, shared and weighed. Similarly, supporting a vast and open national client base would rapidly become an expensive process. Users fees would probably be required sooner or later, amounting to a subsidized service competing with, or mooting a competitive private-sector solution. Additionally, a potential challenge for the public sector UI provision relates to "freedom of information" or "access to information" laws and requests. Certain UI gathering and management processes will be sensitive and should not be available upon request. This would require the managing public entity to possess national security or a similar status to receive exemptions, thereby further complicating the mandate and organization. Finally, privacy considerations can create particular complexity in the public sector.

Value-Added Process	Description
Aggregation	Threat intelligence about compromised, suspicious or known malicious IPs, domains, and ASNs are collected from multiple communities and sources.
Correlation and Weighting	Threat information is processed looking for IPs, domains, and ASNs that are more or less common across sources, increasing or decreasing their correlation scores respectively.
Reputation Sorting	Some sources of seed information may be highly trusted while others may have unknown trust or possibly even suspected of injecting misinformation. Similarly, some sources will strive to remain very current and validate their threat intelligence carefully; other sources may propagate out of date threat intelligence in good faith. The extent to which the IPs, domains, and ASNs can be obtained from trusted sources increases their weight. Weighting in turn supports remediation and/or response decisions by subscribers. Sorting may also determine the type of subscriber that may receive the UI. For instance, a national security entity may wish to make UI associated with some assets available only to other national security users/subscribers.
Expiry/Decay	All threat information and UI loses value as it ages. This "decay rate" cannot be expressed in precise, mathematical terms as it might be for radiation or milk. Depending on the threat agents, intelligence may have a useful life of mere minutes. However, most UI will remain valid for extended periods of time, especially information about compromised end-point devices and victims. Expiry and decay rate information will be important for the purposes of not only managing cached intelligence and subscriptions (please refer to part 4 in this series), but for subscribers to appropriately manage their response to positive "hits" once UI is injected in their security infrastructure.

Table 1 Threat agents targeted by Upstream Intelligence

Not-For-Profit

Not-for-profit (NFP) is a business model already widely used in the open and closed-source cyber threat world. Groups such as Spamhaus, MAUG and other fee-for-service cyber intelligence groups are incorporated as NFP entities. The NFP approach is also supported by a large and probable consumer (and therefore contributor) of UI: government. In the US especially, the NFP approach to cybersecurity information sharing has been tacitly endorsed by both the US Senate through pending legislation and the Department of Energy (DOE) through a recent solicitation. In its pending Cybersecurity Act, the Senate is proposing the establishment of regional "information sharing" NFPs to distribute what could amount to UI, as well as additional threat information. Similarly, in early 2010 the DOE issued a multi-million dollar request for proposal for an NFP to coordinate cyber threat information sharing among electricity producers. Beyond government endorsement, the NFP model has the advantage of appearing neutral and not favoring one vendor or technical solution over another, thereby defusing objections

from a growing range of powerful competitors in the field of UI development and distribution (*i.e.,* defense contractors, telecom firms, systems integrators, product vendors, and an ever growing list of boutiques and start-ups.)

Many of the intelligence suppliers to an NFP UI manager would be for-profit, commercial entities—vendors, carriers, and boutique—charging the NFP for the UI they contribute. Given the probable scope and scale of the UI ecosystems, a substantial amount of the operating budget might be consumed by subscriptions from UI communities. In the end, NFPs may have substantial operating costs, possibly where a majority of the operating costs are subscriptions, not salaries and capital for the NFP itself. Such costs for an NFP probably require more than moderate user fees. These fees generate expectations related to service level commitments, and issues associated with liability, errors, and omissions. A typical NFP has few assets and therefore cannot support the liability that clients might require–insurance for errors and omissions– escalating costs further. It is possible that the advantages of an NFP generate no substantial cost savings or improved quality for end users. Again, Government subsidy could inhibit the private sector from an opportunity to commercially and competitively provide UI services. Finally, to the extent that an NFP is publicly funded or subsidized, the stability of the NFP could be subject to political interference, impacting anything from organizational stability, client confidence, operating budgets, and staffing appointments.

Independent UI Refineries

A dedicated refinery business model is another form of UI management entity that might be devised. Such an entity would possess little or no intelligence capabilities, being focused purely on gathering cyber threat intelligence sources, aggregating, correlating, and weighing the results for distribution to subscribers. Given the wide range of potential competitors and communities that would likely be sources of UI, such an entity could function in a non-aligned manner like an NFP. Similarly, a purely commercial boutique UI refinery would presumably be established by private investment and funded from profits, therefore applying efficient market principles to the business.

Conversely, an independent UI refinery without links to larger companies or government may face a variety of issues. Putting aside the obvious challenges associated with the financial stability of most new companies, the lack of reputation and operating history may prove difficult to overcome. Without a reputation as a trustworthy or a pedigree, a boutique may have difficulty getting a wide range of UI sources to obtain the necessary information for aggregation, correlation and distribution, whether as paid subscriptions or otherwise. Similarly, any independent refinery will be by definition a small(er) operation and subject to acquisition, possibly as a deliberate part of the investors "exit strategy." This could mean that a UI management source relied upon by entities such as government, might suddenly come under new management whose motives are less transparent. Essentially, a variety of measures associated with stability weigh down the merits of independent UI refineries.

Integrated Producers

An integrated producer and manager of UI might take the form of a telecom carrier or a larger security vendor. Such a producer should have first-hand access to a large quantity of UI from its own, native infrastructure, and established relationships with a variety of other cyber threat information sources, open and closed. Such an entity would benefit where the independent UI refineries falter: financial stability, established reputations, and (potentially) publicly regulated ownership.

Countering the integrated producer model are the qualities that make not-for-profit and government options more appealing: non-partisanship and altruism. UI management owned and operated by a large commercial entity, such as a carrier or a security vendor, will come with baggage: 1) competitors may not have comparable access to all services; 2) there may be a proclivity to bundle UI capabilities with their own products; 3) there may be proprietary interfacing and integration challenges with competitor's products; and 4) there may be a tendency to provide the best UI and services to the highest bidder while ignoring clients who represent margins too thin to service. Addressing such challenges through anti-competitive regulation, fines, and oversight might be considered a solution to such issues, but they represent another entirely different set of challenges.

UI Vouchers or Tax Credits

It is very difficult to assess which business model is the most appropriate for UI management in the coming years. Most likely, there will be a need in the market for more than one model and possibly all models. Some models are more appropriate for delivering different quantities and qualities of UI to different stakeholder groups. In the event that some sort of public subsidy and oversight is deemed appropriate to ensure standards, perhaps a form of UI vouchers or tax credits for businesses and consumers to use with "charter suppliers" will evolve, rather than directing large sums at a single solution.

Conclusion

The collection of seed threat information and its application against massive network flows is fundamental to the accuracy and timeliness of UI. Network theory, elegantly and empirically supported in nature, provides useful templates for UI business structures: information sharing loops at all levels of aggregation create both accuracy and resiliency

under ever changing conditions. The more challenging business questions are related to ownership and management. The most cautious approach to these questions in the immediate future may be to remain aware of the potential for publicly run or subsidized entities to retard commercial service-development, without providing adequate solutions. ■

References

1. See Article 1 of this series - Upstream Intelligence: a new layer of cybersecurity and Article 2 of this series - Anatomy of Upstream intelligence.
2. A honeypot is a device or even entire network placed on the open Internet intended to bait malicious entities into engaging and seemingly compromise assets. In fact, the assets will carefully observe the attack techniques for the purposes of intelligence gathering.
3. Network theory is about the study of the characteristics that make networks more or less efficient and resilient under different conditions.
4. Eleni Katifori, Damage and fluctuations induce loops in optimal transport networks, Rockefeller University, May 2009.
5. US Federal Communication Commission - National Broadband Plan - *http://www.broadband.gov/.*
6. US Federal Communications Commission, Connecting American: National Broadband Plan 2010 - Recommendation 9.13.
7. Ibid. – Recommendation 16.8.

IATAC SPOTLIGHT ON A CONFERENCE

Black Hat USA 2010

Since its inception in 1997, this conference has successfully brought together information security leaders from across government, industry, academia, and even underground researchers. It offers a vendor-neutral environment where specialists can openly share insights and experiences and receive cutting-edge, high tech training. As a result, it is a highly anticipated event annually, and this year is no exception. This event takes place 24-29 July 2010.

This year, Black Hat® presentation topics include: "Cybersecurity: A Year in Review (Legally Speaking) - Google/NSA, Warrantless Searches, and Attacks," which will discuss the controversy surrounding the Google®-NSA partnership; "Unauthorized Internet Wiretapping: Exploiting Lawful Intercept," which will delve into how law enforcement information monitoring has weaknesses that could allow for untraceable communications interception; and "The Chinese Cyber Army: An Archaeological Study from 2001 to 2010," which will provide an in-depth look at arguably our largest cyber adversary. Additionally, Black Hat® will provide briefings on in-depth technical topics offering those in attendance the opportunity to learn about our most critical information security weaknesses, and the emerging solutions that will help us combat them.

For more information about Black Hat® as well as the briefings and training events it offers worldwide, visit *http://www.blackhat.com/.* ■

State-of-the-Art Report on Information and Communications Technology Supply Chain Security Risk Management

by Karen Mercedes Goertzel and Theodore Winograd

A critical aspect of the US government's effectiveness is the dependability, trustworthiness, and survivability of the information and communications technology (ICT) on which its ability to perform its functions, activities, services, and missions relies. However, as our adversaries find their efforts to compromise government information systems and networks increasingly confounded by the expanded reach and effectiveness of information assurance (IA) and cybersecurity controls and countermeasures, they seek new targets and avenues of attack. Among these: the supply chain for ICT products that are the "building blocks" of those systems and networks. Supply chain attacks attempt to either proactively compromise those building blocks before they can be deployed in systems or networks, or to delay or prevent their delivery when and where they are needed.

The Information Assurance Technology Analysis Center (IATAC) is developing a state-of-the-art report (SOAR) on managing security risks in the supply chain for off-the-shelf (OTS) ICT products, including commercial-off-the-shelf (COTS) and government-off-the-shelf (GOTS) hardware computer, networking, and telecommunications hardware and firmware, and COTS, GOTS, open source, shareware, and free software. The SOAR also touches on supply chains for "ICT-as-a-service" (*e.g.,* plain old telephone service, cloud computing "as-a-service" offerings) and ICT custom-production outsourcing under contract as a risk avoidance measure.

The SOAR discusses both threats to supply chain processes and product and data flows, and threats from a compromised supply chain to the products in it. Threats to and from the supply chain can be realized at any point during the product acquisition, creation, and delivery cycles. They can originate from outside or inside the supply chain. Moreover, the supply chain for a vast majority of OTS ICT products actually consists of a number of "feeder" supply chains, each delivering a part or component to be integrated together creating the final ICT product. This makes the "supply chain" for ICT products a diffuse and complex amalgam of actors, product and data flows, and processes at multiple levels of supply sourcing, often widely—even globally—dispersed, and seldom all identifiable or traceable.

The SOAR begins by providing some context for its discussion of ICT supply chain security risk management by clarifying its relationship with supply chain management (SCM), supply chain risk management (SCRM), and supply chain security. SCM is most concerned with availability, visibility, and efficiency of supply chain processes and how moving parts, components, products, and associated data flow through the supply chain. SCM also deals with the accountability of participants in the supply chain, so that the right parties can be held responsible when something goes wrong. SCRM—in the sense that term is commonly used—focuses on minimizing risks that prevent timely product flow from supplier to acquirer, or that unacceptably increase the costs associated with establishing and sustaining that flow. However, in the SCRM context, breakdowns in supply flow are seldom if ever imagined to be anything but unintentional or intentional but non-malicious.

It is not SCRM but supply chain security that has been concerned with malevolent intent, and on managing risks that involve the sabotage, illicit penetration, or illicit diversion of tangible (physically-delivered) product supply chains. The compromises that most concern supply chain security involve the smuggling of contraband and undocumented aliens, planting of weapons of mass destruction, theft, counterfeiting, and interruption or diversion of product flows. Supply chain security focuses exclusively on the physical security of processes, facilities, and infrastructure involved in the manufacturing, handling, and transportation as cargo and freight of tangible products. To date, supply chain

security has not paid attention to the security of electronic, or cyber, supply chains, such as those that deliver software and digital media *via* the Internet.

To some extent supply chain security addresses the impact of supply chain compromises on the integrity and trustworthiness of products that have high-confidence imperatives, (*e.g.,* airplanes, automobiles, medical devices, pharmaceuticals, food, children's toys, *etc.*). The driving concern with such products is that the intentional compromise of their supply chain processes and flows could render the products unreliable, unsafe, or outright harmful.

Though the physical supply chain for hardware and packaged software shares many characteristics and risks with supply chains for high-confidence and safety-critical goods, it has not generally been a specific focus in supply chain security, beyond numerous efforts by law enforcement and customs officials, to seize counterfeit ICT hardware and software products at point of origin or point of entry, and to apprehend the counterfeiters.

While the cyber supply chain for software shares a number of characteristics with cyber supply chains for digital media (*e.g.,* music, video, publications), the risks differ to a great extent, mainly due to the differences in the products being delivered, and the

In recent years, the security risks…in the ICT supply chain have risen to prominent attention in the national and homeland security communities.

criticality and sensitivity of the functions they are often used to perform. Indeed, the nature of ICT products is at the core of what makes the imperatives for ICT SCRM unique. As it contains executable logic, ICT in particular is a target for corruption or tampering with the knowledge that such products are likely to be used in processing or transmission of sensitive or private information, or in controlling or monitoring security-critical or safety-critical processes. Compromises of ICT products in the supply chain now are often specifically intended to render those products vulnerable later—after their operational deployment—to illicit access and control, or sabotage.

In recent years, the security risks unique to, particularly intense, or numerous in the ICT supply chain have risen to prominent attention in the national and homeland security communities. This attention has culminated with the acknowledgement of the problem in the Comprehensive National Security Initiative (CNCI), and its establishment of Initiative 11 to focus on SCRM for ICT used in government systems. The real concern here is that supply chain compromises are not only increasingly both intentional and malevolent, but also reflect a strategy of systematic targeting by nation-state adversaries, terrorists, or organized crime.

CNCI has reinterpreted "SCRM" to focus on the management, through mitigation or avoidance, of risks associated with the intentional, malevolent compromise of ICT supply chain processes, product flows, data and artifacts, and/or data/artifact flows. Specific compromises of concern are:

1. Gaining access to and corrupting or tampering with ICT products within the supply chain. The objective of such alterations is either to sabotage the products ability to function as expected, or to subvert their functionality, through modification or augmentation;
2. Replacing or augmenting product inventory with defective or malicious counterfeits;
3. Preventing product delivery within a required timeframe;

4. Misrepresenting products to fool their acquirers into trusting them excessively or using them inappropriately.

To avoid confusion with SCRM as it has traditionally been defined, what CNCI terms SCRM, the SOAR terms supply chain security risk management—which is, in fact, the focus of the SOAR. However, because it is often difficult to determine the motivation of every supply chain compromise perpetrator, and because for certain types of compromises (*e.g.*, counterfeit insertion, supply chain disruption, and product corruption) the outcome is the same regardless of motivation, and finally because the mitigations and countermeasures to non-malevolent compromises frequently help protect against malevolent ones, and vice versa, this SOAR addresses management of all supply chain risks involving intentional compromises, regardless of their motivation.

Specifically the SOAR surveys:

- **The Problem Space**—The SOAR discusses current and anticipated threats to the availability, integrity, and trustworthiness of the ICT supply chain and the accountability of its participants, and threats from a compromised ICT supply chain to the products that move through it. ICT supply chain vulnerabilities to those threats are also addressed;
- **The Solution Space**—The SOAR describes current and emerging approaches to mitigating supply chain risk through anti-threat countermeasures, as well as current risk avoidance strategies;
- **The Initiatives Landscape**—The SOAR introduces a number of government, industry, academic, and international efforts to identify, assess, mitigate, or avoid risks that arise in the ICT supply chain;
- **The Research Landscape**—The SOAR describes recent, past, and current scientific and technical research and development of ICT supply chain risk mitigations.

The distribution code for the new SOAR on *ICT Supply Chain Security Risk Management* has not yet been determined. Depending on its ultimate disposition, the SOAR will either be directly downloadable or orderable from the IATAC website at *http://iac.dtic.mil/iatac/*, or through the Total Electronic Migration System (TEMS) at *http://iac.dtic.mil/iatac/TEMS.html* in August 2010. ■

Karen Mercedes Goertzel and Theodore Winograd have co-authored several of IATAC's state-of-the-art reports. Both authors can be reached at iatac@dtic.mil.

Letter to the Editor

Q ***A colleague of mine recently forwarded me a new electronic publication IATAC recently distributed, the Technical Inquiry Production Report (TIPR). What is the TIPR, and how can I sign up to receive it?***

A As most of our customers know, IATAC provides a free, four-hour technical inquiry service for registered customers of the Defense Technical Information Center (DTIC). Though a few of the inquiries we receive result in *IAnewsletter* articles, and some lead to the research we conduct when developing a State of the Art Report, IATAC wanted a medium to more regularly share some of the inquiries we receive and the responses we provide with the information assurance (IA) community. The Technical Inquiry Production Report (TIPR) provides us that medium.

The TIPR is a short e-mail publication, like the IA Digest, that we send out quarterly in both HTML and plain text format. IATAC distributes the TIPR in conjunction with the release of the *IAnewsletter*. It features a brief synopsis of an IATAC Subject Matter Expert and a sample of the technical inquiries and responses IATAC fielded that quarter. It provides subscribers with a snapshot of the types of questions IATAC customers have and the research capabilities IATAC provides. We hope it also provides our subscribers with a general idea of emerging trends in IA.

To subscribe to the TIPR, just e-mail IATAC at iatac@dtic.mil, and we can add you to our distribution list. ■

Old Dominion University

by Angela Orebaugh

Old Dominion University (ODU) is located in Hampton Roads, Virginia, one of America's major seaport areas. In addition to its 185-acre main campus in Norfolk, ODU operates higher education centers in Hampton, Virginia Beach, and Portsmouth, as well as a thriving distance learning network. With an enrollment of more than 23,000 students, the university offers 70 bachelor's, 60 master's, and 36 doctoral degree programs and two educational specialists degrees.

ODU's Batten College of Engineering and Technology offers a number of programs at the undergraduate and graduate level. The Modeling and Simulation (M&S) program is a multi-disciplinary program supported by more than 35 faculty members from all six academic colleges. The Bachelor of Science Degree in Modeling and Simulation Engineering (M&SE) prepares students to enter the workforce as M&S engineers and scientists, and to enter graduate programs in modeling and simulation. The M&SE curriculum requires all students to complete a minor in another discipline such as computer science, computer engineering, electrical engineering, engineering management, mechanical engineering, aerospace engineering, civil engineering, physics, or mathematics. Emphasizing studies across disciplines ensures students gain multiple perspectives essential for analyzing complex problems in information assurance and other technical fields of study. The M&S Graduate Program emphasizes the following research areas:

- M&S Fundamentals
- Defense and Security teamed with US Joint Forces Command (USJFCOM)
- Emergency Management Training, Analysis and Simulation Center (EMTASC)
- Medicine and Bio-Science - teamed with Eastern Virginia Medical School
- Education and Gaming - teamed with NASA Langley Research Center
- Transportation - teamed with the Commonwealth of Virginia
- Engineering and Science
- System of Systems and Enterprise Decision Support

Research scientists and facilities at the Virginia Modeling, Analysis and Simulation Center (VMASC) support the M&S Program. VMASC is a multi-disciplinary/research center that has been in operation for 13 years. Working with more than 100 industry, government, and academic members, VMASC furthers the development and applications of modeling, simulation, and visualization as enterprise decision-making tools to promote economic, business, and academic development. VMASC concentrates on seven core modeling and simulation applied research areas:

- Transportation
- Homeland Security and Military Defense
- Virtual Environments
- Social Sciences
- Medicine & Health Care
- Game-based Learning
- Business & Supply Chain Modeling

VMASC's state-of-the-art capabilities consist of approximately 6,000 square feet of lab space including two general purpose labs, a visualization lab, a human factors lab, and a 74-seat virtual reality theater supporting live, virtual, and constructive simulation integration. VMASC's accomplished faculty members work in varied fields of expertise to successfully expand on and bring unique innovations to modeling and simulation research and development. ■

References

1. *http://www.vmasc.odu.edu/ACADEMICS/academics.html*
2. *http://eng.odu.edu/msgp/*
3. *http://www.vmasc.odu.edu/ABOUT/about.html*

Security and User Traffic Monitoring - Where Do You Draw the Line?

by Chris Silva

Government and defense organizations are massive entities with users who vary in their technical abilities and security awareness. In most organizations, users are generally aware of protections such as Secure Sockets Layer (SSL), but largely unaware of the implications of using those tools, especially when it comes to monitoring an organization's network for data leakage. Therefore, organizations must strike a balance between protecting stakeholder rights while securing data.

Most organization disclosures state that employee activity is subject to monitoring, but the amount and nature of monitoring can vary. Employees can expect organizations to review transactions within government-owned systems. Organizations can also monitor communications *via* owned assets where some degree of personal use (*i.e.*, e-mail) may be expected.

Organizations have shown that they need to monitor Internet activities to prevent access to inappropriate content in the workplace and to detect patterns of access that are contrary to data security policies. Vendors have begun to release technologies that allow agencies to monitor SSL-encrypted traffic and detect data leakage *via* covert channels. Many technologies copy traffic and examine it for suspicious activity, rather than intercepting traffic, reviewing it, and then passing it on after review.

Research firm IANS recommends that organizations pursuing monitoring demonstrate that they meet requirements for limited purpose, adequacy, and relevance. To this end, responsible organizations should profile standard web traffic and exempt activity where anticipated interactions would not expose organizational/confidential information, or where employees reasonably should expect privacy to be ensured.

According to IANS, there are no tools that do this, so it is incumbent upon the organization to monitor traffic to create a whitelist/blacklist before beginning interception. Organizations should not decrypt traffic going to known banks, pharmacies, or retailer sites, but they may examine traffic bound for known file-sharing sites, such as Trueshare or Filesanywhere, or for traffic that is net-new to its baseline, as it could indicate some degree of suspicious activity.

Once an organization profiles normal web traffic, it needs to demonstrate clear procedures to examine anomalous SSL traffic. Initially, organizations should evaluate the web traffic's ability to negatively impact its protection of sensitive data. Next, the organization should either choose to allow the traffic without monitoring, block the traffic due to perceived risk, or continue to monitor traffic to evaluate changes in risk profile or to pursue criminal prosecution with law enforcement.

In the event that normal activities reveal information that might expose employees to financial or reputational harm, it would be incumbent upon the organization to exercise care by severely restricting and monitoring access to sensitive information, or to apply scrubbing or filtering solutions to remove information that causes undue harm for employees subject to monitoring.

In an era where more data flows into and out of companies, agencies, and departments through different and varied types of applications and services, the need for monitoring is high. However, with this responsibility comes an incumbent need to track and police how information is gathered, used, and discarded. ■

About the Author

Chris Silva | is the Senior Vice President of Research and Service Delivery at IANS. In this role, Chris runs all daily operations of IANS' syndicated research and custom client advisory activities. Chris is committed to innovating the IANS research methodology to better serve security professionals. Chris comes from within the Information Technology research industry and is a veteran of several established research businesses. Chris served four plus years at Forrester Research, most recently as a Senior Analyst working to serve Security/Risk and Infrastructure/Operations professionals. Chris is a graduate of the Isenberg School of Management at the University of Massachusetts.

FREE Products Order Form

Instructions: All IATAC LIMITED DISTRIBUTION reports are distributed through DTIC. If you are not a registered DTIC user, you must register prior to ordering any IATAC products (unless you are DoD or Government personnel). To register online, visit: *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 ☐ **Firewalls** ☐ **Intrusion Detection** ☐ **Vulnerability Analysis** ☐ **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 this report will be shipped)

State-of-the-Art Reports (SOARs)
- ☐ Measuring Cybersecurity and Information Assurance
- ☐ The Insider Threat to Information Systems (soft copy only. DTIC user code MUST be supplied before this report 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. Softcopy back issues are available for download at *http://iac.dtic.mil/iatac/IA_newsletter.html*

Volumes 11	☐ No. 1	☐ No. 2	☐ No. 3	☐ No. 4
Volumes 12	☐ No. 1	☐ No. 2	☐ No. 3	☐ No. 4
Volumes 13	☐ No. 1	☐ No. 2		

SOFTCOPY DISTRIBUTION

The following are available by email distribution:

- ☐ IADigest
- ☐ IA/IO Scheduler
- ☐ Research Update
- ☐ Technical Inquiries Production Report (TIPR)

Fax completed form to IATAC at 703/984-0773

Calendar

August

LandWarNet 2010
3–5 August 2010
Tampa, FL
http://events.jspargo.com/lwn10/Public/MainHall.aspx

Air Force Information Technology Conference (AFITC 2010)
30 August–1 September 2010
Montgomery, AL
http://www.mc2-afitc.com/

September

The Summit on IT Governance, Risk and Compliance
21–22 September 2010
Boston, MA
http://www.misti.com/

IANS New England Information Security Forum
28–29 September 2010
Boston, MA
http://www.iansresearch.com/forums/calendar.html

October

C4IST Exhibition
4–7 October 2010
Fort Huachuca, AZ
http://www.afceac4ist.com/

AUSA Annual Meeting and Exposition
25–27 October 2010
Washington, DC
http://www.ausa.org/news/meetings/Pages/default.aspx

CSI 2010: Security. Strategy. Success
26-29 October 2010
National Harbor, MD
http://www.csiannual.com/

2010 TechNet Asia-Pacific
25-28 October 2010
Honolulu, HI
http://events.jspargo.com/tnap10/public/enter.aspx

November

NSA Ops 1
16 November 2010
Fort Meade, MD
http://fbcinc.com/event.aspx?eventid=Q6UJ9A00LY86

NSA Ops 2
17 November 2010
Fort Meade, MD
http://fbcinc.com/event.aspx?eventid=Q6UJ9A00LY8X

NSA Ops R&E
18 November 2010
Fort Meade, MD
http://fbcinc.com/event.aspx?eventid=Q6UJ9A00LY94

To change, add, or delete your mailing or email address (soft copy receipt), please write us at: 13200 Woodland Park Road, Suite 6031, Herndon, VA 20171, 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