

Challenges in **CYBERSPACE**

- 2** Cyberspace – The Fifth and Dominant Operational Domain
- 8** Transitioning to Secure Web-Based Standards and Protocols
- 11** Information Assurance Assessments for Fielded Systems During Combatant Command Exercises
- 13** Supplier-Supply Chain Risk Management
- 16** Internet-Derived Targeting: Trends and Technology Forecasting
- 21** Training and Educating the DoD Cybersecurity Workforce

Security

IDA EXPLORES CYBERSPACE

Information and communications technologies underpin virtually every national security and business transaction in the modern world. Cyberspace operations therefore permeate almost every mission of the Department of Defense (DoD) and its partners, demanding intense focus on the security of cyberspace and related assurance matters.

Cyberspace operations and cybersecurity are similarly pervasive in the wide-ranging research IDA conducts. The articles collected in this set of *IDA Research Notes* describe ways to characterize cyber environments and act effectively within them.

In the opening article, retired **General Larry Welch** sets the stage by describing ways to mature our understanding of cyberspace operations. Cyberspace is a domain, he writes – a place, not a mission. As in more commonly understood domains – land, sea, air, and space – military superiority in cyberspace is derived from our freedom of action in, through, and from it, and from our ability to deny adversaries freedom of action at times and places of our choosing. Related activities include constructing cyberspace, passive defense, active defense, exploitation or operational preparation of the environment, and attack. Associated with these activities is the need to define the capabilities to conduct missions in, through, and from cyberspace.

The paper following General Welch's article focuses on a form of cyberspace construction; the following two relate to passive and active defense. An aspect of cyberspace exploitation is discussed in the next; and the concluding article addresses the workforce aspect of necessary capabilities.

Researchers from IDA's Information Technology and Systems Division – **Dr. Elizabeth McDaniel, Coimbatore Chandrasekaran, Dr. William Simpson, and Dr. Kevin Foltz** – describe IDA work to help DoD leverage the emerging web services model. IDA is designing and testing a pilot project that fosters secure information

sharing through common interfaces and protocols; the pilot has potential to become the DoD enterprise solution.

Dr. Shawn Whetstone describes IDA's work on behalf of the operational test and evaluation community in response to the 2003 National Defense Authorization Act. The legislation requires annual operational information assurance assessments during major training exercises conducted by Combatant Commands and the Services. Dr. Whetstone explains how IDA helps DoD's Director, Operational Test and Evaluation accomplish these assessments by applying IDA's expertise with operational and information technology; our familiarity with assessments performed during large-scale exercises; and our understanding of the Department's efforts to improve information assurance.

Dr. Serena Chan provides an overview of IDA's role in developing supply chain risk management capabilities in the face of increasing dependencies on information and communications technology in DoD as well as throughout the national economy. IDA work in this area supports Initiative 11 of the Comprehensive National Cybersecurity Initiative.

Jason Dechant and Zachary Rabold explore security-related exploitation of cyberspace. They detail findings obtained from two years of "red teaming" exercises in which IDA researchers – at the behest of a DoD sponsor – acted the part of adversary forces, employing open source Internet browsing in a manner useful to selecting targets and planning attacks.

In the concluding article, **Ryan Wagner and Stephen Olechnowicz** illustrate IDA's role in helping DoD ensure its access to a plentiful pool of highly trained cybersecurity experts. He explains IDA's contribution to determining skill sets and qualifications necessary within an effective information assurance and cybersecurity workforce.

CYBERSPACE – THE FIFTH OPERATIONAL DOMAIN

Gen. Larry D. Welch USAF (Ret.)

The Problem

The concept of cyberspace as a domain has been in vogue for only a few years. Still, extensive operations in cyberspace have been a reality for decades. Hence, while cyber operations are not new, our understanding of cyberspace as a domain requires further maturing.

Cyberspace as a Domain – Similarities and Differences

A more evolved, productive understanding of cyberspace can build on extensive experience in cyber operations and on similarities with approaches to operations in other domains. Though there are important dependencies in cyber operations impacting political, economic, and diplomatic activity, this article will concentrate on military activity in, through, and from cyberspace. For the rest of this article, the term cyber operations will include creating military effects in, through, and from cyberspace.

This article also emphasizes the similarities between dealing with challenges and opportunities in cyberspace and in the other operating domains – land, sea, air, and space. This is not intended to minimize the challenges in cyberspace but instead to emphasize the need to build on proven capability-development expertise – and on processes that have enabled a wide range of military force capabilities over the years.

The fundamental imperative for maturing understanding is to treat cyber as a place, not a mission. That is, cyberspace is a domain in, from, and through which military operations create intended effects. The fundamental military objectives relative to this domain are essentially the same as in the other domains, again – land, sea, air, and space. The primary objective is freedom of action in, through, and from cyberspace as needed to support mission objectives. The corollary is to deny freedom of action to adversaries at times and places of our choosing. The ability to do both provides for cyber military superiority.

There are other important similarities in the demand for and nature of military superiority in the five domains. Military operations do not depend on access and operations in all areas of the domain at all times. For example, maritime superiority requires control of selected areas of the seas at

It is no more possible to control all of cyberspace or all of the networks of interest at all times than it is to control all of air space or all of the maritime space.

all times and other areas only at selected times. Similarly, air superiority requires control of selected areas at all times and other areas at selected times. The same is true of cyberspace. Even so, there remains significant confusion about the concept of cyber superiority.

While there are key similarities, there are also fundamental differences between cyberspace and the other domains. One is that the hierarchy of other domains is geophysical in nature.

The hierarchy begins with the land surface of the earth surrounded by the maritime domain. All the land and seas are surrounded by the air domain, and the air domain is surrounded by the space domain. In contrast to the other domains as illustrated in Figure 1, cyberspace is embedded in all domains and operation in all domains is dependent on operation in cyberspace. Hence, military operations in all domains depend on operations in, through, and from cyberspace.

A second fundamental difference is that cyberspace is constructed by man and constantly under construction. It changes from moment to moment. Military interest in cyberspace is dominated by the use of networks for friendly and adversary operations. Most of the networks of interest are connected, leading to the perception that the cyberspace of interest to military operations is a single network. This is not a useful concept for cyber operations. It is no more possible to control all of

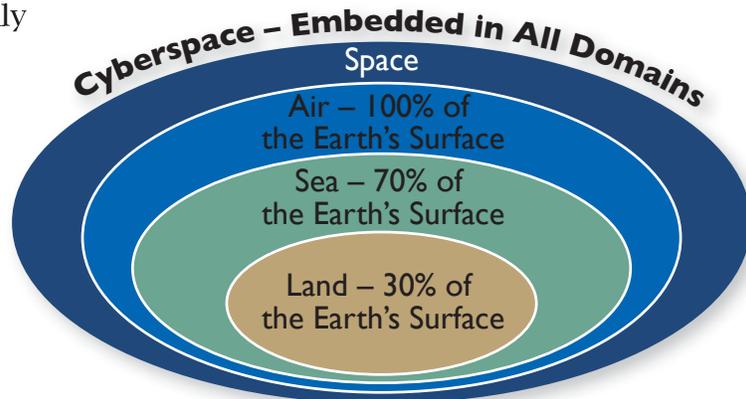


Figure 1. Cyberspace – the Embedded Domain

cyberspace or all of the networks of interest at all times than it is to control all of air space or all of the maritime space. As is the case for other domains, the imperative for freedom of action in, through, and from cyberspace is to define the segments of cyberspace where such action is needed.

Missions in Cyberspace

The specific level and scope of the need for control of cyberspace is dependent on the specific activity conducted in, through, and from cyberspace. In general there are six classes of activities. They are:

- constructing cyberspace,
- passive defense,
- active defense,
- exploitation or operational preparation of the environment,
- attack, and
- defining the needed capabilities to conduct defined missions in, through, and from cyberspace.

Only the first activity is unique to the cyber domain. Unfortunately, the motivations driving construction of most of cyberspace did not include considerations of defense against cyber intrusion or cyber attack. Further, in addition to damage to forces and operations in the domain, cyber attacks can destroy mission-essential segments of cyberspace. Hence, defense in cyberspace includes freedom of action to conduct cyber operations impacting operations across the domains, protecting access to the needed segments of cyberspace, and protecting the existence of those segments of cyberspace. The adversary cannot destroy segments of the air, sea, or space. The adversary *can* destroy segments of cyberspace.

Cyberspace may also be unique in the breadth of effects from cyber operations. Dr. Richard Ivanetich recently suggested to me that it is useful to think of the range of effects as physical, logical, or cognitive. In the physical realm, the effects can include causing physical damage by causing physical assets such as power generation to self-destruct. In the logical realm, the effect can be disrupting functions essential to computer control of the networks, information flowing or stored in the networks, and/or the decision support systems supported by the networks. The cognitive effects include the strategic influence aspect of information warfare impacting the decision processes and capabilities. This range of effects can be generated with attacks against adversaries. They can also be part of the challenge of defending against adversary cyber attacks.

Priorities for Meeting Challenges and Leveraging Opportunities

The similarities and differences suggest a set of priorities for meeting the challenges and leveraging the opportunities in cyberspace to meet mission demands.

The first priority is to identify those segments of cyberspace where freedom of action is essential to mission accomplishment. This does not start with an attempt to map the network. It starts with identifying the decisions required to conduct and support operations. This is followed by mapping the information collection, manipulation, storage, and movement required to support the decisions. When these two needs are understood, those segments of cyberspace (networks) essential to operations can be defined. This process will require an attitude of constraint. Given the current cyber culture, the demand will remain unconstrained unless a new level of discipline is imposed. While every decision maker from the platoon leader to the joint task force commander can make a case that unfettered access to information wherever it resides in cyberspace is essential to the effectiveness of his or her operation – an unconstrained approach based on these demands would virtually guarantee that, in the face of adversary cyber operations, every decision maker will suffer from loss of effectiveness due to the vulnerabilities of mission-essential segments of cyberspace.

The next priority is to focus on making those networks sufficiently defensible to ensure continued,

even if degraded, support for operations in the face of attacks on access, information, or the network itself. There is a perception that currently constructed cyberspace is so vulnerable that there must be a hedge to operate without access to cyberspace. The time when such a hedge was feasible passed at least a decade ago. It is no more feasible to conduct military operations without access to cyberspace than it would be to operate without access to the seas or the air. Instead, the focus needs to be on ensuring that selected segments of cyberspace are defensible, defended, and sufficiently robust to function under attack. This may require giving up some of the characteristics of the use of cyberspace that we have come to expect in our daily lives. It may require a drastically reduced number of gateways to essential networks. It may require active defenses that produce collateral damage to non-combatants whose resources are being used by adversaries to attack our operations and conduct their own. It will certainly require a combination of

passive and active defense capabilities that respond at the speed of the networks and the clear and timely authority to use those capabilities.

The next priority is to develop and field the cyber forces needed to support the six classes of activities in cyber operations.

Building Cyber Forces

There is a perception that developing forces with cyber capabilities is a unique process understood only by cyber experts. The reality is that the process required to build forces with cyber capabilities does not differ greatly from the complex process of building the capabilities required to operate a Modular Brigade or an Aegis Cruiser or a Fighter Wing. In each case, the process is similar to that shown in Figure 2. It does take special understanding of each cyber activity to define missions, describe the desired

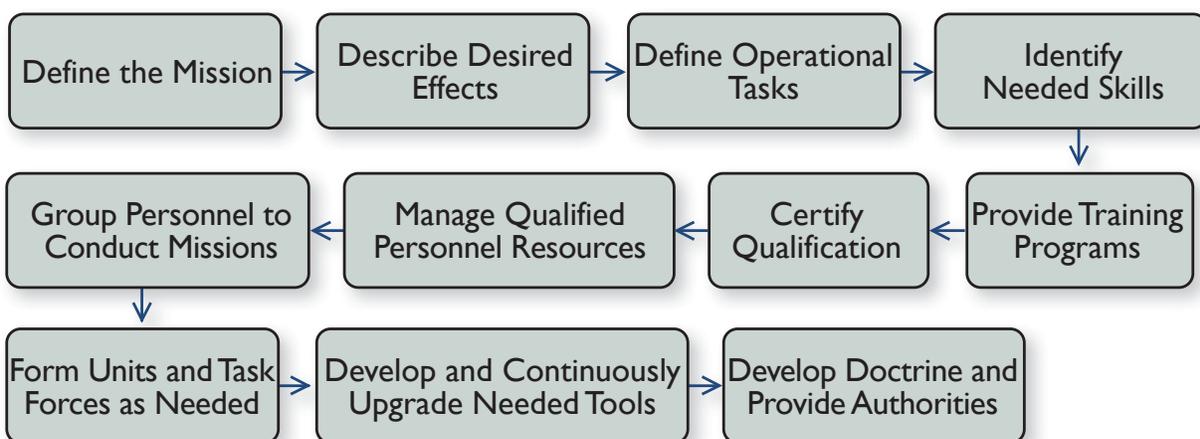


Figure 2. Force Building Process

effects, define operational tasks, and identify needed skills. Each class of activity requires a specific set of skills, tools, concepts, doctrines, and authorities. Still, the process is similar to complex processes that the military departments and defense agencies have successfully executed for a wide variety of new capabilities.

The point of Figure 2 is not to precisely describe either the sequence or the details of the force building process but to illustrate that it is a set of activities that the military departments and defense agencies know well and have performed successfully for decades. The military services have adapted to new demands, new environments, and new capabilities on a regular basis. Adapting to the demands of cyber operation is no more difficult than adapting to the change from the cold war to the post-cold war - adapting to the change from force-on-force operations to counter-insurgency and post-conflict operations. The issue now is to move forward rapidly to build the needed cyber forces with the needed set of capabilities to produce the desired set of military effects across the spectrum of cyber operations.

Operational Gain-Loss Concept

The cyber domain exacerbates a long-standing set of perceived and real conflicts in gain-loss decisions impacting operations. The conflict between the gains to an ongoing combat operation from denying an adversary the use of cyberspace

at times and places of our choosing and the gain from exploiting the adversary's use of cyberspace is compounded by two factors. The first is a perception that combat operations and intelligence gain-loss are of interest to two different communities; therefore, there is conflict between communities - combat operations and intelligence. The second complicating factor is that adverse activities inside networks created by adversary action, insider threats, or inadequate attention to security measures can threaten the continued operation of a larger set of networks with consequences greater than the risk to an ongoing combat operation. Again, there is an inevitable conflict between the current combat operations gain from continued network operation and the loss risk to the network. Once again, this has been perceived as a conflict between two activities - current combat operations and network operations. The reality is that intelligence gain-loss, network gain-loss, and combat operations gain-

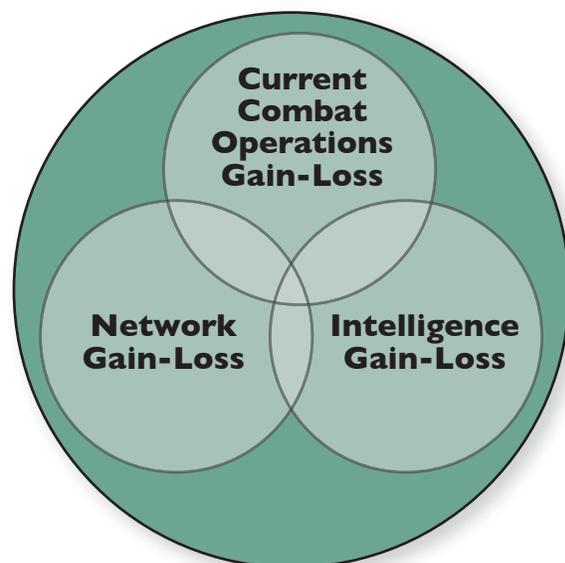


Figure 3. Operational Gain-Loss from Integrated Gain-Loss Considerations

loss are all operational matters and the operational commander responsible for the success of the joint operation needs to fully understand the full set of gain-loss risks and be the primary influence on gain-loss decisions. Operational gain-loss considerations must integrate a complex set of overlapping gain-loss considerations as illustrated in Figure 3.

At present, there is a structure and process to resolve intelligence gain-loss issues and an arbitrary practice to resolve network gain-loss issues. The current structure and processes do not integrate the gain-loss considerations as part of an overarching operational gain-loss decision process. This can have a wide range of serious consequences for military operations to include the loss of forces and failure in combat operations. Lack of a full understanding of such decisions can also have serious consequences for the intelligence information needed to support operations and for critically important networks and other critical infrastructure.

Further, many gain-loss decisions cannot await a complex set of processes. The need to deny adversary use of some segment of cyberspace may be the difference between success and failure of an ongoing operation and the cost of failure may be severe. At the same time, an adversary's exploitation of a network weakness could propagate to a wider network at Internet speed. Hence, there will need to be carefully defined rules of engagement, priorities, and authorities for timely gain-loss decisions.

Effective military operations have been increasingly dependent on

cyber operations for several decades. The most fundamental objectives in cyberspace are similar to the objectives in the other domains – land, sea, air, and space. The objectives are freedom of action to create desired military effects and ability to deny such freedom of action to adversaries at times and places of our choosing.

Effects in, through, and from cyberspace include constructing defensible segments of cyberspace (networks), defending essential segments of cyberspace, exploitation, and attack. Attack capabilities can include creating physical effects, disrupting logical operations, and creating cognitive effects. Defense capabilities need to also deal with this range of effects.

While the needed skills, tools, and authorities are different for cyber operations, the processes needed to build effective capabilities are similar to those that the military departments and defense agencies have used to build other capabilities. The need is to do the complex, detailed work. There are no silver bullets.

The long-standing need to integrate intelligence and network gain-loss considerations into the overarching operational gain-loss decision process remains unfulfilled. The consequences can be loss of military forces, combat failure, loss of essential intelligence information, and/or high consequence damage to critically important networks.

General Welch is a former chief of staff of the U. S. Air Force and former president of IDA.

TRANSITIONING TO SECURE WEB-BASED STANDARDS AND PROTOCOLS

Dr. Elizabeth A. McDaniel, Dr. William R. Simpson,
Coimbatore S. Chandersekaran and Dr. Kevin E. Foltz

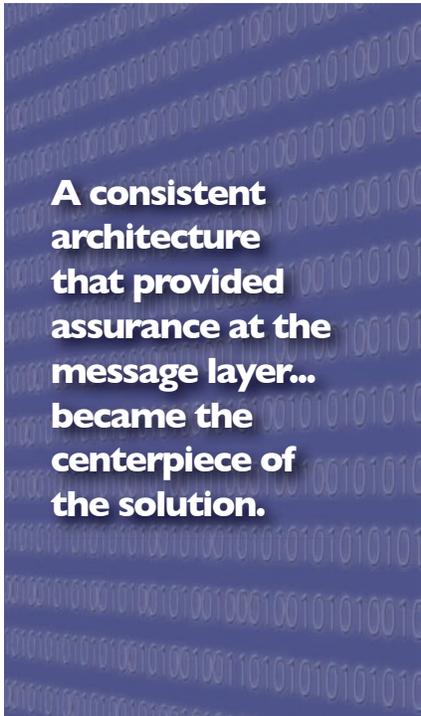
The Problem

Across DoD, non-standard IT arrangements and complexities grew with every new system and application. For example, in response to many procurement solicitations, vendors implemented their own security and communications solutions. As a consequence DoD organizations have thousands of systems with unique characteristics and vulnerabilities. The complexities of a myriad customized systems and applications - with often repeated data and information saved on local servers and computers - make information sharing difficult and expensive, and reveal uneven security policies and practices that add to enterprise vulnerabilities.

Our Approach to the Problem

IDA researchers are completing foundational work required to accomplish goals set in the DoD Information Enterprise Strategic Plan released in May 2010.¹ This has included designing and building a high assurance web-based approach to content sharing and information security. The research team designed a pilot system based on the evolving web service model that fosters net-centricity and information sharing, allows access from many devices, desktop and mobile, and conserves valuable DoD IT resources. The pilot solves the problems of interoperability and enterprise-wide security through the use of standard interfaces and protocols that guarantee interoperability and make the management of capabilities much simpler. The IDA team is currently collaborating with the Defense Information Systems Agency (DISA) and the Air Force on a pilot test in the Defense Enterprise Computing Centers.

In response to DoD CIO guidance, the Air Force Chief Information Officer committed to creating a web-based, net-centric solution. The challenge was to build a single consistent, net-centric information assurance architecture to support the key related elements of the DoD strategic plan, including integration of warfighter network and command and control



A consistent architecture that provided assurance at the message layer... became the centerpiece of the solution.

¹ Goal 1 in the plan is a “robust DoD Information Enterprise [that] provides the Department and mission partners access to discoverable, authoritative, relevant, trusted, and actionable information and services to enable effective and agile decisions for mission success.” Goal 2 calls for a “balanced suite of DoD Enterprise Services [to] be visible, accessible, understandable and trusted, enabling net-centric information sharing via a service-oriented information enterprise.” Goal 4 proposes a “unified and resilient DoD Information Enterprise where only authorized users (including mission partners) have ready access to their information; missions continue under any cybersecurity situation; and associated components perform as expected and act effectively in their own defense.”

capabilities, improving situational awareness, and optimizing transport of authoritative secure information. A consistent architecture that provided assurance at the message layer - using a claims-based paradigm for security based on Public Key Infrastructure and Security Assertion Markup Language-based authorization - became the centerpiece of the solution. The layered architecture in the pilot system takes advantage of greater usability, vendor flexibility through industry standards, and greater opportunity to improve or modify the overall implementation while allowing for legacy operations during adaptations to new approaches.

The system is designed to protect five primary security aspects of information: confidentiality, integrity, availability, authenticity, and non-repudiation. Design principles, for example extensibility and information hiding, are supplemented by security mechanisms, including strong two-way authentication using DoD Public Key Infrastructure. The layered architecture is critical to the security approach.

Implications of the Research

Web-enabled information - made discoverable and accessible using open, standard protocols and techniques, via standard desktops or other edge devices from the field - facilitates information sharing and access to information for more informed decision making.

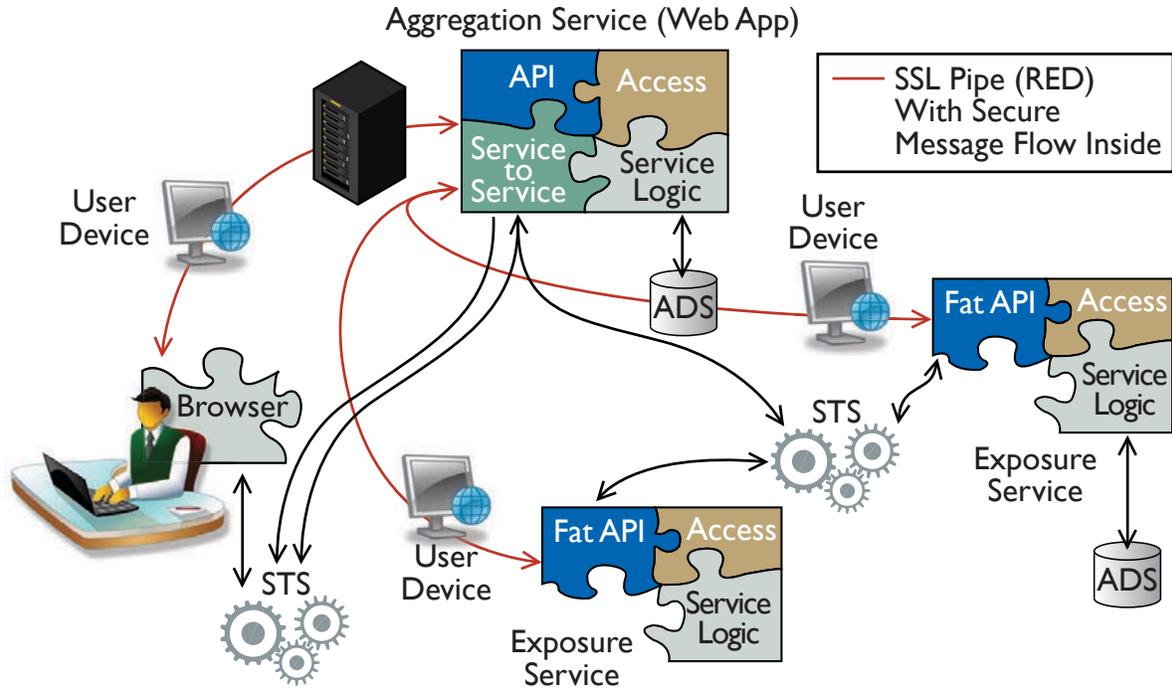
The model relies upon a layered architecture, in which each layer below the mission services can and should be implemented by industry-standard

COTS products, rather than custom software. Taking advantage of such standards will enable DoD to focus on developing higher level capabilities to fulfill its mission, rather than spending time on lower level integration tasks.

DISA currently has responsibility for centralized hosting, management, and deployment that includes end-to-end testing and performance monitoring capability. The Air Force and DISA will collaborate on bounded user requirements described through detailed business re-engineering and generating Quality of Service, performance, and access rules consistent with associated architecture products, support plans, and Service Level Agreements. Though this project focused on the Air Force's particular environment and net-centricity goals, IDA's research has potentially wide ranging implications for DoD. As a model for enterprise solutions, it can enable net-centric operations, foster information sharing, address security concerns, and create standards that will enhance DoD efficiency and cost saving. In describing this work to other DoD CIOs, our sponsor indicated that "the Air Force has been diligently working to move to a net-centric environment while improving our IT development and delivery processes. Our goal is to greatly improve the IT acquisition cycle time and build our capabilities in accordance with a well defined, standard engineering baseline."

CLAIMS BASED SECURITY

Based on verifiable credentials containing claims to identify or privilege



CLAIMS BASED IDENTIFICATION AND AUTHORIZATION

Authentication Using Verifiable DoD Certificate Credential and Authorization Using Verifiable Security Token Server SAML Credentials

Dr. McDaniel is a National Defense University Fellow in IDA's Information Technology and Systems Division - on detail from her position as Dean of Faculty and Academic Programs at the National Defense University iCollege.

Dr. Simpson is a research staff member in IDA's Information Technology and Systems Division. His analyses have focused on such diverse topics as integrated diagnostics, Internet scale distributed systems and artificial intelligence.

Mr. Chandrasekaran is a research staff member in IDA's Information Technology and Systems Division. He has conducted extensive research in such fields as identity management, distributed systems security, and cognitive systems.

Dr. Foltz is a research staff member in IDA's Information Technology and Systems Division. He has conducted research in networks, security, and testing.

INFORMATION ASSURANCE ASSESSMENTS FOR FIELDED SYSTEMS DURING COMBATANT COMMAND EXERCISES

Dr. Shawn C. Whetstone

The Problem

Ground rules guiding combatant command exercises frequently discourage introduction of elements that distract from training objectives. This has inhibited the ability to insinuate cyber disruptions into gaming scenarios, thus masking the effects of cyber attacks on exercises, potentially slowing awareness of problems and corrective actions.

To help monitor DoD efforts to improve its information assurance posture, the National Defense Authorization Act (NDAA) of October 2002 tasked the operational test community and information warfare centers to conduct annual operational information assurance assessments during major Combatant Command and Service training exercises. The Director, Operational Test and Evaluation (DOT&E) leads the efforts. To help accomplish this task, DOT&E draws upon IDA's expertise with operational and information technology assessments and familiarity with assessments performed during large-scale exercises.

Learning About Adversaries' Goals

IDA's role is to provide: (1) analytical support to DOT&E's oversight of the assessments and (2) analyses of data to identify issues and trends from multiple exercises, such as the relationships between cybersecurity and other security functions including physical access and disposal of information. Our work has confirmed an increased emphasis by attackers on gaining entry to secure areas for placing unauthorized devices, accessing unattended workstations, seeking improperly secured papers, and searching through trash for passwords or personal information to establish initial entry points into networks.

Exploitations during training exercises are increasingly focused on intelligence gathering rather than on disrupting information systems and networks - an observation that mirrors experiences in the commercial sector. Factors contributing to these trends include restrictions on permitted attacker activities and the realization that intelligence gathering is valuable for adversaries and the opposing forces in the exercise environment. Network defenders are countering

Increasing operational realism during training exercises by allowing cyber warfare to disrupt operations is needed to understand the potential operational effects of cyber activities.

adversaries' intelligence gathering activities with increased protection of critical operational information and deception operations that provide false information to known compromises.

Red team focus on intelligence-gathering highlights the interplay between interoperability and security. Operators are increasingly using chat tools and web portals to communicate and exchange critical operational information. The assessments are helping establish an appropriate balance between an operator's desire for accessibility through improved interoperability and the need to protect operational information.

Areas of Continuing Research

IDA's analysis confirms that improvements continue to be needed in network defenders' abilities to detect and respond to malicious activity. Improvements can include network sensors, analysis tools, and methodologies for analyzing data.

The DoD has emphasized compliance control measures for monitoring information assurance preparedness. The current measures

are necessary but insufficient for predicting performance during exercises. IDA's assessments have helped to identify additional operationally relevant controls, but research is needed to improve and identify measures to better capture those aspects of defensive posture that affect performance.

Increasing operational realism during training exercises by allowing cyber warfare to disrupt operations is needed to understand the potential operational effects of cyber activities. Exercise ground rules have typically prevented such disruptions deemed to potentially distract from training objectives. However, an increasing awareness of the importance of cyber warfare is opening the door for venues that permit cyber attacks to disrupt systems and for retaliatory cyber strikes against the adversary. More research is needed to increase the rigor of information assurance testing to the levels enjoyed by weapon system testing.

Dr. Whetstone is a research staff member in IDA's Operational Evaluation Division. He holds a doctorate in nuclear engineering from the University of Michigan.

SUPPLIER-SUPPLY CHAIN RISK MANAGEMENT (S-SCRM)

Dr. Serena Chan

The Problem

The growing trend of globalization and outsourcing provides opportunities for adversaries to penetrate the Government's supply chain of information and communications systems. Their purposes might be to obtain knowledge, gain access, insert malicious code, or corrupt information or components bound for mission-critical systems and networks. Supply chain risk is an increasing concern as globalization produces more complex supply chains, and outsourcing creates greater dependency on external suppliers instead of developing products in controlled or trusted environments.

The complex, transitory, and global nature of the commercial ICT marketplace makes it challenging to assure that articles of supply and the suppliers can be trusted to do only that which is expected or specified...

Supply chain risks must be evaluated early and continually throughout the acquisition life cycle in order to effectively develop and implement defensive countermeasures and mitigations. Risks can be introduced at any point in the supply chain and may be passed along downstream to intermediate product and service users or end-users. IDA is supporting its sponsor in developing supply chain risk management (SCRM) capabilities that are responsive to the increasing dependencies on information and communications technology (ICT) that enable trusted mission systems and networks.

National Security Presidential Directive 54/Homeland Security Presidential Directive 23 created the Comprehensive National Cybersecurity Initiative (CNCI) to improve how the Federal Government protects sensitive information on agency networks from cyber threats. CNCI includes 12 efforts that either formalize existing cybersecurity processes or introduce new policies and business practices to better protect computer networks and systems. CNCI Initiative 11 called for DoD and DHS to lead an interagency effort on SCRM.

DoD increasingly relies on ICT components and services to support its critical information and weapons systems. The complex, transitory, and global nature of the commercial ICT marketplace makes it challenging to assure that articles of supply and the suppliers can be trusted to do only that which is expected or specified and to do so reliably and dependably. To help address this challenge, DoD established a SCRM Pilot Program.

The SCRM Pilot Program is intended to improve DoD's understanding of what practices work effectively; what gaps

exist in policy and guidance; how the current or proposed practices, processes and procedures for discovering, using, and managing risk information perform; what general impediments to implementing robust supply chain risk management for the acquisition of ICT exist; and what the anticipated cost, schedule, and performance impacts may be. The pilot activities are also intended to validate the timeliness and actionability of all-source intelligence available to acquisition professionals.

IDA has developed and continues to refine the Key Practices and Implementation Guide for the DoD SCRM Pilot Program.¹ This document provides insights and methods to mitigate risks that arise from the suppliers in a DoD acquisition program. It includes examples of practices expected to mitigate identifiable vulnerabilities and associated threats. Each practice has the potential to impact procurement or an acquisition's cost, schedule, or performance.

IDA also assisted in standing up the Threat Assessment Center (TAC) in the Defense Intelligence Agency and continues to provide analytic support and develop training. Additionally, IDA conducted vulnerability assessments on selected covered acquisition programs, studied techniques for verifying trust in Integrated Circuits (IC), and validated

DoD's Strategy for Systems Assurance and Trustworthiness. IDA continues to support additional vulnerability assessments, criticality integration, and prioritization efforts. Related outreach activities have included IDA presentations at the 15th Republic of Korea - United States (ROK-US) Defense Analysis Seminar, the 2010 Military Communications Conference (MILCOM), and the 2010 Institute of Electrical and Electronics Engineers (IEEE) International Conference on Technologies for Homeland Security.²

IDA is helping DoD discover, define, learn, and establish capabilities related to supplier and supply chain risk management (S-SCRM) of ICT. Integral to this has been the development of an S-SCRM enterprise framework that brings together intelligence mitigations, technical mitigations, and business mitigations into a trade space to reach a collective view and to review and adjudicate decisions to obtain a Risk Reduction-Return on Investment (RR-ROI), illustrated in Figure 1. *Intelligence mitigations* refer to the ability to apply knowledge to manipulate one's environment or situation. *Technical mitigations* refer to measures to alleviate the consequences of a realized flaw or failure potential in an item of supply. *Business mitigations* are the process capabilities that use and apply knowledge, know-how, and tools to conceive, design, develop, produce, deliver, and sustain

¹ US Department of Defense, *Key Practices and Implementation Guide for the DoD Comprehensive National Cybersecurity Initiative 11 Supply Chain Risk Management Pilot Program*, February 25, 2010.

² (a) Greg Larsen and Forrest R. Frank, "Assuring Operational Readiness through Management of Supply Chain Risks," *15th Republic of Korea - United States (ROK-US) Defense Analysis Seminar*, Seoul, Republic of Korea, April 13-17, 2010. (b) "Cybersecurity Supplier-Supply Chain Risk Management," 2010 MILCOM Classified Technical Panel, *Military Communications Conference (MILCOM) 2010*, San Jose, CA, October 31 - November 3, 2010. (c) Serena Chan and Gregory N. Larsen, "A Framework for Supplier-Supply Chain Risk Management: Tradespace Factors to Achieve Risk Reduction - Return on Investment," *2010 IEEE International Conference on Technologies for Homeland Security*, Waltham, MA, November 8-10, 2010.

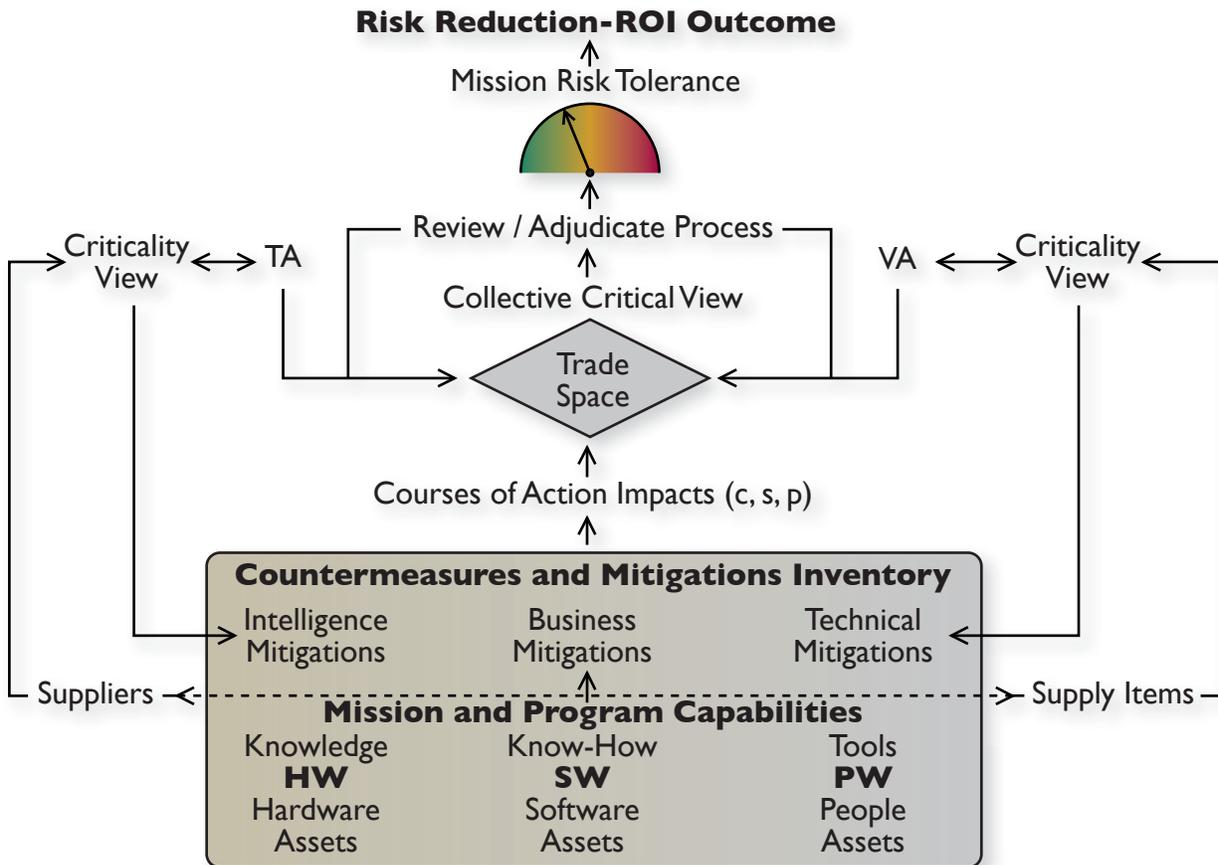


Figure 1. Supplier-Supply Chain Risk Management (S-SCRM) Enterprise Framework
 (Illustration adapted from the paper Dr. Chan presented at the 2010 IEEE International Conference on Technologies for Homeland Security, Waltham, MA, November 8-10, 2010)

hardware, software, and people to implement a system. Intelligence mitigations are derived from conducting Threat Assessments (TAs); technical mitigations are derived from conducting vulnerability assessments (VAs); and business mitigations are derived from mission and program capabilities and best practices. These mitigations require a *collective critical view* to assess the cost (c), schedule (s), and performance (p) impacts in order to determine the best course of action. These impacts are the foundation upon which risk decisions are made to manage supplier and supply chain risks.

The IDA-developed enterprise

framework for S-SCRM captures the underlying complexity and scope of concerns relevant to managing globalization and outsourcing effects of ICT risks. Using this framework, IDA is continuing research efforts to identify policies and processes to counter and mitigate threats to supply chains, to define priorities and ways to specify risk, and to assess the quality of RR-ROI decisions.

Dr. Chan is a research staff member in IDA's Information Technology and Systems Division. She holds a doctorate in engineering systems from the Massachusetts Institute of Technology.

INTERNET-DERIVED TARGETING: TRENDS AND TECHNOLOGY FORECASTING

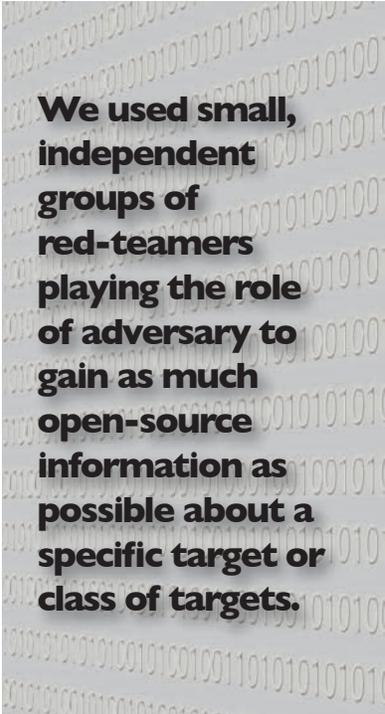
Jason A. Dechant and Zachary S. Rabold

The Problem

For several years, mounting evidence has pointed to adversary use of the Internet as a resource for target selection and attack planning. One recent example was a bomb plot targeting former President George W. Bush's residence; the suspect's computer revealed extensive use of the Internet for targeting purposes.

To better anticipate nefarious use of the Internet and understand how it may be used for targeting purposes, the DoD developed an experimental red-teaming approach involving multiple independent teams emulating adversary targeting and planning cells. The teams are given laptop computers, uninterrupted workspace, a wireless Internet connection, and three days to complete their mission. The purpose of these experiments is to determine whether the Internet may be used to develop a list of potential targets to attack, to focus the list based upon a set of criteria, and to design notional concepts of operations for attacking targets.

Between 2008 and 2010, IDA conducted 10 Internet-Derived Targeting (IDT) missions. For each of these missions, we used small, independent groups of red-teamers playing the role of an adversary to gain as much open-source information as possible about a specific target or class of targets. At the conclusion of the tenth IDT mission, DoD asked IDA to conduct an analysis of all of the missions to assess what could be learned about using the Internet for targeting. Additionally, we were asked to consider how adversary use of the Internet may evolve in the near-term (between 2010 and 2015), considering the proliferation of and advances in online technologies. Specifically, DoD asked IDA to examine how evolutions in the capabilities of mobile online technology, social network platforms, and online imagery may have implications for adversary targeting activities.¹



We used small, independent groups of red-teamers playing the role of adversary to gain as much open-source information as possible about a specific target or class of targets.

¹ IDA also reviewed how online search functions and “enthusiast” websites – websites that provide valuable targeting information from communities of amateur followers – will evolve to support online targeting in the next five years. These online features are discussed in detail in Chapter 3 of Jason Dechant and Zachary Rabold et. al. *Internet Derived Targeting: Trends Analysis and Technology Forecasting* Paper P-4687 (Alexandria, VA: Institute for Defense Analyses, 2011).

IDT Trends Analysis

IDA researchers compiled lists of websites used during the 10 missions. Using automated software,² from the aggregated list of websites, natural categories emerged. We determined which individual websites were most frequently used across all IDT missions, for each IDT individually, and for different classes of targets. A number of findings emerged from the analysis of the 10 missions:

1. Commercial websites (e.g., those of private companies) were the most frequently used category of websites shown in Figure 1.
2. The majority of the most useful websites across all IDT missions were from government and defense domains, though common news media sites also proved useful.
3. Despite the proliferation and increased use of social networking sites (e.g., Facebook), blogs and message boards, those sites were not used frequently.

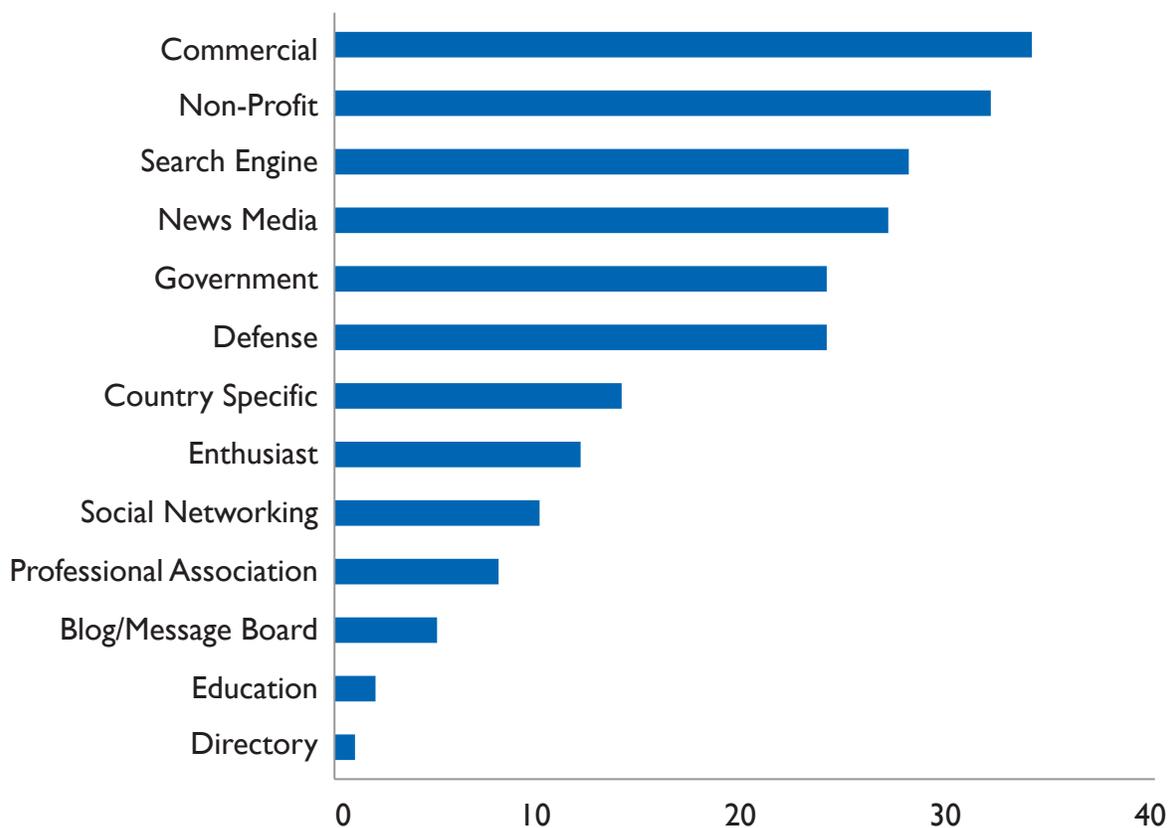


Figure 1. Most used categories of websites during IDT “red-team” missions, 2008-2010.

² An IDT red-team member’s “online signature” is a traceable, digital path used by that member to select specific mission-related targets. Red teamers’ signatures are collected by using a computer tracking program (SpectorPro), online search history, and other online track methods, as well as a conscious effort by red teamers to record their specific online behaviors.

Technology Forecasting

The second part of the study examined how adversary use of the Internet may evolve in the near-term (2010-2015) given the proliferation of and advances in online technologies. This began with an in-depth literature review of key technology areas that may assist and enable adversary targeting using the Internet: (1) mobile online technology, (2) social network platforms, and (3) online imagery. To supplement the findings of the literature review, the project team interviewed experts in each technology area's industry, as well as relevant professionals at IDA. These interviews, if not conducted in a one-on-one setting, took place at official on-the-record industry meetings, seminars, and workshops - mainly at the Web 2.0 Expo held in New York City from September 27-30, 2010 - or in exchanges by telephone and e-mail. The three technology areas where advances are expected in the near-term are discussed below.

1. Mobile Online Technology

In the near-term, mobile near real-time, online technology will enable adversaries to obtain more than a basic understanding of targets using mobile augmented reality and improved Internet browsing capabilities.³ Additionally, static imagery capabilities (e.g., Google Earth) combined with mobile, Internet-connected imagery (e.g., camera phones and online webcams) will allow adversaries to project themselves onto a common mapping plane with a

target and conduct "omnipresent" real-time (or near real-time) surveillance of a target. From a human targeting perspective, this near real-time surveillance can be done electronically and instantaneously with little or no person-to-person interaction with the target.

2. Social Network Platforms

Trends in social networks facilitate the information collection and information consumption stages of targeting. In its examination of social network platforms, IDA found that five developments will drive the growth and utility of social networks for targeting purposes: the integration of facial recognition technology, content integration across websites and platforms, geo-location awareness, cross-platform integration, and user-generated applications. The implications of these developments to social networks center on their increasing importance in everyday social interaction and the increasing amounts of data they connect and replicate. While personal information on a target may be more useful than it was in the past, the volume of data available also means there is more noise to filter out.

Social network information can be exploited in a variety of ways. For example, it is possible to map clusters where social network use was important and unimpeded and, by contrast, locations where it was discouraged. Done in the proper location, it is possible to locate where sensitive work may be taking place

³ Augmented reality on mobile technology uses a device's cameras, compass, GPS systems, and data browsing and storage capacities to allow users to get information about a location or facility and overlay the information on a common mapping plane.

that would warrant more extensive restrictions on mobile and Internet use. In addition, accessing a single networking site will allow an adversary to target the exposed individual's connections by seeing his or her social, economic, and lifestyle preferences. There is also the opportunity to use social networks for denial and disruption attacks, or as part of information operation (IO) efforts.

Social network use will continue to expand globally, especially in currently under-connected and under-utilized locations. As developers and advertisers seek ways to exploit real-time content, social networks are facilitating a convergence of previously compartmentalized content and activity, resulting in an increased aggregation of content in one fixed place with recognized vulnerabilities. Personal data are becoming more easily accessible via social plug-ins in cross-platform applications (e.g., connecting Facebook and Twitter accounts). Increasingly, gaining access to a single networking site will open up an individual's entire social networking universe to exploitation.

3. Online Imagery

As commercially available satellite technology enables higher resolution imagery and more frequent refresh rates, it will become increasingly easy for adversaries to use open-source platforms to geo-locate and geo-orient locations of interest and to determine best approaches. Based on recent developments in online, open-source imagery, it appears there is a strong demand for real-time functionality among users of online imagery platforms. It does not appear as though real-time satellite

imagery will be accessible in the near-term; however, it does appear that there will be increased near real-time functionality across online imagery platforms which could provide targeters with useful information about a given location.

Augmenting online satellite imagery with user photographs, webcams, tracks, and near real-time layers will provide opportunities for adversaries to garner previously unforeseen insights about a location. Additionally, growing online imagery capabilities allow targeters to detect change in near real-time, over long periods of time, and in a time series. Adversaries casing targets can notice changes in a target's security posture and perhaps even defenders' response times and routes of approach. Targeters may also be able to supplement and, potentially, even replace harbor sites by using emerging online imagery capabilities in combination with tracking technologies and applications. Used in combination, changes may be observed over long periods of time or constantly, as opposed to the finite timeframes available during ground reconnaissance missions.

Implications for Targeting Activities and Defense Intelligence

IDA's technology forecasting analysis revealed not only noteworthy emerging firms, technologies, and capabilities, but also several trends relating to how individuals, groups and societies are leveraging elements of the Internet.

The technology areas researched by IDA do not change targeting fundamentals. The opportunities and risks associated with the planning phases of a targeting operation are instead redistributed.

While the quantity and quality of information yielded from remote reconnaissance would appear to be greatly improved using expanded Internet capabilities, targeters still risk exposure. As adversaries utilize advanced Internet capabilities, they expose themselves to the same identification vulnerabilities as their targets, creating opportunities for offensive targeting.

Successful targeting still requires key pieces of information, not all of which may be available on Internet sites. Thus, denial and deception activities will likely continue to be worthwhile.

The proliferation of sensors on vulnerable platforms, coupled with

their increased use, enables individuals to act as sensors and be used in many different ways. This research points up the importance of being attentive to the potential for targeters to leverage such witting and unwitting intelligence sources and assets.

The results of these IDA analyses have been used by government sponsors to better understand adversary use of the Internet and to expose potential vulnerabilities posed by open sources.

Jason Dechant is a research staff member in IDA's Strategy, Forces and Resources Division. He is currently a doctoral candidate at George Mason University's School of Public Policy.

Zachary Rabold is a research associate in IDA's Strategy, Forces and Resources Division. He holds a master's degree in international relations from the University of Chicago.

TRAINING AND EDUCATING THE DoD CYBERSECURITY WORKFORCE

Ryan R. Wagner and Stephen M. Olechnowicz

The Problem

As technical training and associated certifications continually and rapidly evolve, DoD is challenged to ensure its workforce is appropriately and robustly credentialed in ways most suitable to providing secure networks.

Just as well trained and educated people are often the key to success in conventional conflicts, the same holds true for cyber warfare. DoD's information assurance (IA) and cybersecurity workforce are charged with defending DoD's cyber infrastructure and data from threats posed by a range of adversaries.

Who Makes Up the IA Workforce?

IDA's involvement with IA and cybersecurity workforce issues stretches back to 1998, when it led the first comprehensive study on DoD IA personnel. Since then, IDA has helped DoD expand, train, and professionalize the IA workforce.

One of the perennial debates regarding the cyber workforce is the definition of whom it includes. A narrow view would focus on only those who spend most of their time on IA issues, such as information system security architects, intrusion detection system log analysts, and incident handlers. A broader view of the workforce includes any individual with privileged (administrative) access to an information system. In 2004, DoD Directive 8570, "Information Assurance Training, Certification, and Workforce Management," took the broader approach and mandated that "Privileged users and IA managers shall be fully qualified..., trained, and certified to DoD baseline requirements." This definition of the workforce covers military personnel, civilians, and contractors - more than 100,000 people, some deployed in theater and others working in the major network operations and security centers in the United States. The policy further directed the creation of a companion Manual¹ that defines a series of categories, specialties, and job functions for the IA workforce. The decision was made to use industry cybersecurity certifications rather than have DoD create its own.

One of the major challenges in the creation of the Manual was to identify and verify the industry certifications that meet the Manual's requirements. During the development of the Manual, IDA developed a robust methodology for systematically assessing the certifications for their applicability to workforce

¹ DoD 8570.01-M, *Information Assurance Workforce Improvement Program*.

The cybersecurity positions, categories, and specialties... must evolve with the environment. Certifications that lose relevance... will need to be removed... and the bar for entry to new certifications should be raised...

categories, levels, and specialties. The methodology includes analyses of certification course material, labs, proprietary exams, and interviews with practicing professionals holding the certifications. IDA continues to be DoD's trusted resource for independent analyses of a wide variety of both managerial and technical certification offerings.

In concert with the American National Standards Institute (ANSI), IDA helped develop International Organization for Standardization/International Electro-technical Commission (ISO/IEC) 17024, "Conformity assessment - General requirements for bodies operating certification of persons," which set out a series of requirements that ensure certification vendor quality, and that the certifying body is independent of the training provider. The standard was designed with cybersecurity certifications in mind, and the DoD now requires that certification vendors are accredited in compliance with the ISO 17024 standard.

As a result of interactions with IDA researchers, major IA certification vendors have enhanced their course material and exam questions. The goal is to ensure that successful completion of a certification requires a person to draw from various cybersecurity disciplines to apply their knowledge and demonstrate analytical skills. This helps ensure that certification holders have not simply engaged in rote memorization but rather have an operational understanding of cybersecurity.

As information technology and information assurance race ahead, IDA has been actively involved in updates to the Manual. This year, IDA researchers were part of a team involved in redefining the specialty

profession of Information Assurance System Architect and Engineer (IASAE). The resulting draft certification constitutes a major change to the specialty in an effort to reflect changes to and new understandings of the IASAE roles. The draft recommends a mix of training and formal education for prospective IASAEs.

The Future of the DoD Cybersecurity Workforce

The relentless pace of progress in IT is bringing numerous new capabilities to DoD's doorstep, each with a variety of additional security concerns. The movement of IT from a custom, in-house service to a commercial commodity is also changing the field. The cybersecurity positions, categories, and specialties, along with their associated functions, must evolve with the environment. Certifications that lose relevance or fail to stay current will need to be removed from the Manual, and the bar for entry to new certifications should be raised as the field of commercial cybersecurity certifications grows more competitive.

From having performed one of the first studies on the workforce over a decade ago to today's research on the future of the field, IDA is working closely with DoD to ensure that it has a plentiful pool of highly-trained IA experts to defend its networks and ensure the success of its missions.

Mr. Wagner and Mr. Olechnowicz are research staff members in IDA's Information Technology and Systems Division. Mr. Wagner holds a master of engineering degree from the Massachusetts Institute of Technology and has worked as a senior security engineer with Verizon Business.

Scan the Quick Response Code for a pdf version of this journal.



IDA is the Institute for Defense Analyses, a non-profit corporation operating in the public interest.

IDA's three federally-funded research and development centers provide objective analyses of national security issues and related national challenges, particularly those requiring extraordinary scientific and technical expertise.

IDA | RESEARCH NOTES

4850 Mark Center Drive • Alexandria, VA 22311-1882

www.ida.org