IAnewsletter

The Newsletter for Information Assurance Technology Professionals

Volume 5 Number 4 • Winter 2002/2003

Growing Up With Guns

also inside—

- Anatomy of Cyberterrorism
- US/UK/CAN/AUS/NZ CND Technical Conference
- Computer and Telecommunication Infrastructure
- IEEE 802.11 Countermeasures

contents

feature

IA initiatives

in every issue

About IATAC & the *IAnewsletter*—

IAnewsletter is published quarterly by the Information Assurance Technology Analysis Center (IATAC). IATAC is a DoD sponsored Information Analysis Center, administratively managed by the Defense Technical Information Center (DTIC), Defense Information Systems Agency (DISA).

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

IATAC Director:	Robert J. Lamb
Deputy Director:	Abraham T. Usher
Inquiry Services:	Peggy O’Connor
Technical Analysts:	April Perera Jim Peña Brad Soules

IAnewsletter Staff—

Creative Director:	Christina P. McNemar
Art Director:	Ahnie Senft
Designers:	Maria Candelaria Holly Shipley Trang Dam

IAnewsletter Article Submissions

To submit your articles, notices, programs, or ideas for future issues, please visit http://iac.dtic.mil/iatac/news_events/author_submission.htm and download an “Author’s packet.”

IAnewsletter Address Changes/Additions/Deletions

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

IATAC
Attn: Peggy O’Connor
3190 Fairview Park Drive
Falls Church, VA 22042

Phone:	703/289-5454
Fax:	703/289-5467
E-mail:	iatac@dtic.mil
URL:	http://iac.dtic.mil/iatac

Deadlines for future Issues—

Summer 2003	27 June
Cover design:	Holly Shipley
Newsletter design:	Ahnie Senft

Correction—Cover design by Holly Shipley in issue 5/3

Distribution Statement A:

Approved for public release;
distribution is unlimited.

IATAC Chat

Robert J. Lamb, IATAC Director

I wanted to start out with an update of a new Office of the Secretary of Defense Command, Control, Communications, and Intelligence (OSD–C3I) initiative, which IATAC is supporting. On October 22, 2002, Mr. Robert Lentz sponsored a meeting regarding information technology (IT) product evaluations. The meeting was attended by a broad spectrum of the information assurance (IA) and information technology (IT) community including Unified Commands, agencies, and Service labs.

The clear consensus of the participants was that the current state of product evaluation within the Department of Defense (DoD) is fragmented, with little to no information sharing of the results. Combatant commands, Services, and agencies are independently evaluating information technology (IT) products that support their operational requirements. As a result, there is significant duplication of effort between the combatant commands, Services, and agencies seeking to independently assess commercial products. A more coordinated, enterprise approach could result in substantial time and cost savings to DoD. Mr. Lentz requested that IATAC assume responsibility for this effort. By leveraging IATAC's Web presence and capabilities, a means of facilitating information sharing between DoD organizations regarding IT product evaluations was developed and implemented. IATAC is serving as the collection and dissemination point for these evaluations.

The objective of this initiative is to establish a capability for DoD to internally share information related to ongoing, programmed, or completed evaluations of IT commercial products to minimize duplication, assist decision makers through compilation of available information, and enhance/improve the documentation of instructions and implementation of products through the compilation of "best practices" associated with various products. It was agreed this would be accomplished through the existing IATAC infrastructure, and through the leverage of IATAC's established roles and responsibilities as an Information Analysis Center (IAC).

In the succeeding months, we have reached out to those in attendance, among others, to collect product assessments, create abstracts, and post those abstracts to our Web site. To date we have received approximately 250 reports and completed in excess of 160 abstracts that are now posted at http://iac.dtic.mil/iatac/pdf/dod_tool.htm.

This Web site is restricted to .mil and .gov domains only and those seeking the full reports may request them from IATAC. Please visit that URL and if you see a tool abstract that is useful, let us know and we will forward the full report. Also, if your organization has completed assessments, please forward the results via E-mail (iatac@dtic.mil) so that we may incorporate them into the collection.

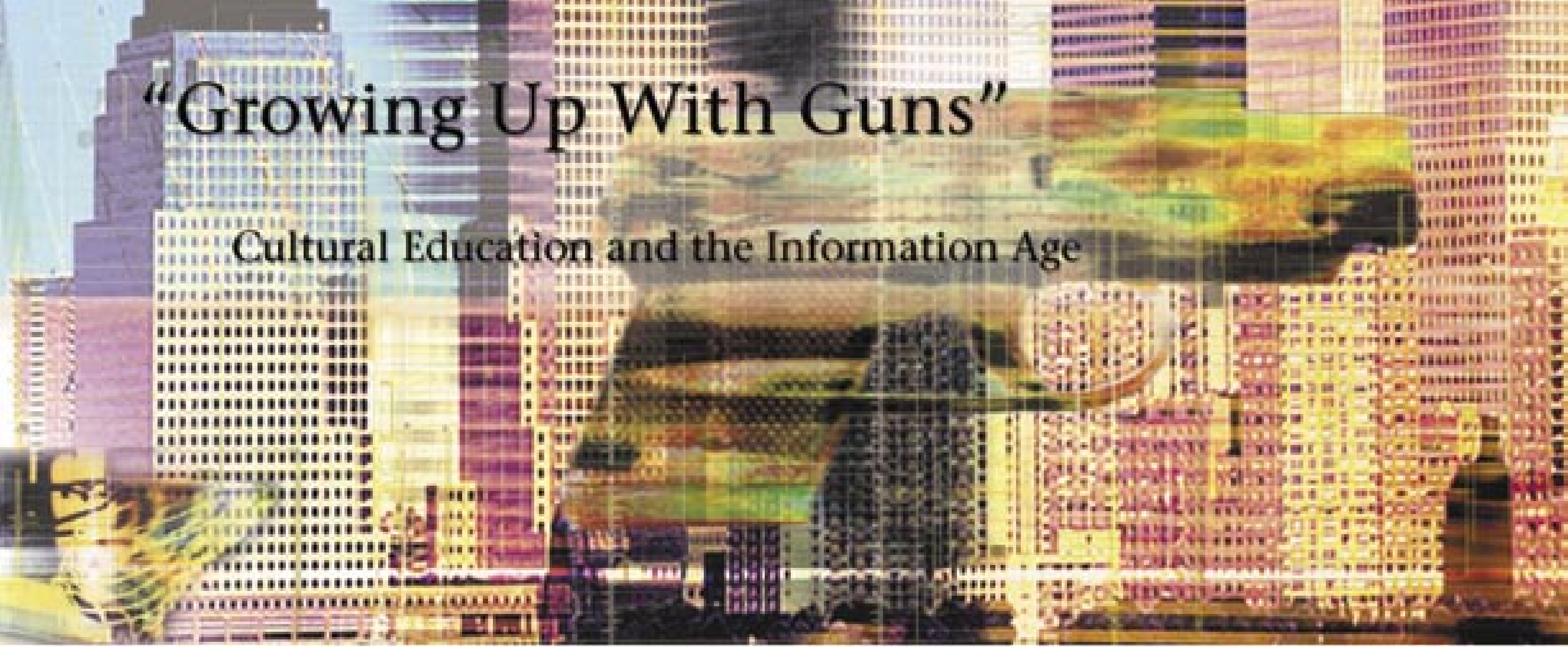
Information Operations (IO) Calendar

IATAC is continuing to publish the IO Calendar every other week. It's a composite of all training and conferences reported to us or that we've discovered in our own research. We publish it electronically via E-mail and post it to our Web site. If you have or know of an upcoming event, please send us an E-mail at iatac@dtic.mil detailing the specifics. I would also add that under certain circumstances (Government/DoD sponsored events) we can post "pop ups" on our Web site and similarly include them in the *IA Digest* published twice weekly and the *IAnewsletter*. The composite of these current awareness initiatives will help get the word out on your event.

DTIC Mission Success Stories

As many of you probably know, the Defense Technical Information Center (DTIC) sponsors thirteen DoD Information Analysis Centers (IACs). IATAC is one of the thirteen. To learn more about the other IACs please visit DTIC's Web site at http://iac.dtic.mil. To gain more insights into the great work they all do, DTIC sponsors a specific Web site detailing their accomplishments in support of DoD and government at http://iac.dtic.mil/mss.

Bob



"Growing Up With Guns"

Cultural Education and the Information Age

by Leslie "Jake" Schaffner, Jr., CAPT USN (Retired), M.Sc.

***Editors Note**—The following is a keynote address from The Policing Cyberspace International Conference, November 2–5, 2002. The views and opinions in this article do not reflect those of IATAC or the Department of Defense (DoD).*

During a decade of working with information operations and infrastructure protection issues, I have observed a pattern of audience response in meetings that I feel has implications for America's technological future. From what I've seen, I am convinced our culture must supply its citizens with a common framework for discourse, debate, and decisions about technology. Meeting this need is essential for our country to meet the challenges of the Information Age.

Two types of debate

In the 1990s, when I first began dealing with information security issues, few members of the U.S. Military had experience in protecting information systems. Nevertheless, the officers who were responsible for advising the Secretary of Defense and the Chairman of the Joint Chiefs of Staff about the emerging information issues diligently studied the technologies, prepared position papers, conducted exercises, and in general, sponsored a vigorous debate within the Executive Branch about the implications of the Information Age on the United States Military.

When assigned to brief senior officers or civilians on an issue, I followed a routine of preparing a short position paper, then staffing it for review and peer commentary the day before the meeting. At the briefing, the paper would be delivered in the form of a slide presentation. Personnel who attended the meeting would bring up their own points for discussion once the presentation had concluded. This process provided a common context for a face-to-face discussion between senior leadership so they could debate the issue, make their decision, and communicate via letter or memorandum.

It wasn't long before I noticed the discussions after the briefings generally followed one of two courses.

The typical and most frequent scenario featured debates that were crisp and professional—the decisions were usually made with a minimum of emotional deliberation. The majority of these cases involved known technology issues and reflected the experience of mature staffs who were skilled in distilling information for busy officials so they could efficiently move issues ahead.

The second and less frequent scenarios began as isolated events, but over time began to occur more frequently. In these situations, the briefing started and then went awry almost as soon as it began. Attendees debated definitions instead of discussing the issue the briefing was designed to address. Some topics dragged through 10 or more briefings and years of work without closure.

Over time, my fellow staff officers and I noticed that these difficult and acrimonious situations generally shared similar characteristics. The discussions were almost exclusively about information system issues, but they occasionally also involved the introduction of new technologies or operating methods. My engineering background led me to look for systemic causes of these problems and discouraged me from accepting quick and trite explanations. I could not accept that all briefings about new technologies or information system issues would automatically result in rancorous debate or staffing chaos so there had to be another reason

A shared context

I discovered a reason while observing a major briefing for a group of high-level flag and general officers. The briefing dealt with a recently developed telecommunications technology. The debate was especially charged; not only was the briefing officer unable to progress past the fourth or fifth slide due to arguments between the senior officers, but the senior officers were emotional with one another in front of their staff (an almost unheard-of situation). No matter how hard he tried, the briefing officer could not successfully communicate the implications of the technology to the generals and admirals in the audience.

The discussion was suddenly brought to a satisfactory conclusion by the oldest officer in the room—a grizzled Marine

Corps general. In an elevated voice full of years of experience, he turned to three senior Service officers and stated that the technology in question was simply a modern variation of one that his Service had employed in a prior conflict. He briefly discussed how the technology had enhanced the performance of the weapons he commanded in that engagement. The room paused for a moment—then the debate proceeded to a resolution in less than five minutes.

Mulling over what I had observed, I came to a conclusion. I have used this thesis to evaluate many briefings and meetings over the years, and in every case it appears to hold true. While my personal observations and opinions do not necessarily constitute academic proof, I submit them for consideration. The reason the general was able to bring the briefing to a rapid conclusion was that he and the other senior officers had all "grown up with 'guns."

"Growing up with guns" implies that these officers shared a large body of knowledge, and more importantly, interpretations concerning firearms and other kinetic weapons. As a group, they understood terms like "collateral damage," "circular error probable," "blast radius," and "civilian oversight of the military." Their common understanding enabled them to expeditiously evaluate briefings and debates about related issues—they could readily "cut to the chase" and reach a logical conclusion.

Those senior officers all attended different educational institutions. They had different military experiences. They were born and raised in different parts of the country. Where did their common ground come from? In my opinion, it was their exposure to American popular culture.

Americans are bombarded by recurrent messages in print and electronic media regarding guns. As soon as we can watch television, or read a newspaper or magazine, we see weapons, their physical principles, and their effects on people and relationships. Action movies, techno-novels, news reports, coverage of the Gulf War and other conflicts, campaigns for firearm control, children's cartoons, and many other media offerings inform and teach Americans about various armaments and their effects on people and targets.

Another personal experience demonstrates the pervasiveness of this cultural education. During the mid 1990s, there were a number of White House staff members who had never served and more importantly, did not trust the Military. One might assume that officers attempting to obtain authorization from these civilians to carry out Military action would find themselves at a loss to communicate exactly what they proposed to do and why. Another reasonable expectation would be that decisions would require lengthy and laborious debate by politicians who were uncertain of the potential political consequences of their decisions.

To the contrary, on the few occasions that I observed such briefings, they generally lasted only a few minutes and the decisions arrived were logical, well-reasoned, and rapidly made. Why? These civilians, too, had "grown up with guns" and therefore shared a common cultural education with their military compatriots. They understood, at a primal level, the potential of weaponry for death, destruction, and personal loss.

My conclusion regarding the difficulties in the briefings I observed was that debates featuring weapons were successful because the participants shared a common context, a gestalt within which they could internalize and intellectually assimilate ideas and their implications. Conversely, attendees who focused on many information technology issues struggled because they had no common definitions, interpretations, or experiences that enabled them to advance their point of view.

Technology separated from culture

When I reflect on the arguments and discussions I observed in Government, I feel that this same lack of common understanding about information technology pervades our culture as we struggle to cope with the promises and perils afforded by advanced telecommunications systems and computing technologies. This difficulty is widespread because the U.S. has not incorporated recurrent references to computers, telecommunications, and more importantly, their potential impact on the everyday life of our citizens in our media and culture to the same degree that it does for "guns."

First, consider television broadcasts. I sampled programs from 120 channels available to me via cable, ranging from the traditional networks to local government access channels. I had no trouble finding references to firearms, explosives, war, or other forms of physical violence. They ranged from the History Channel's coverage of wars and battles to the Travel Channel's instructions on hunting game.

Conversely, references to computers were far more difficult to find. Most references, like that on the TechTV channel, only addressed new technologies as they related to the marketing of new consumer products. There was rarely any discussion about the potential risks of new products for privacy, safety, or reliability. Surprisingly, the most socially relevant discussions I found about computer usage and privacy were vignettes on "Law and Order" and "CSI" where the investigators talked about using E-mail records and hidden files on computers to track lawbreakers.

I have also noticed that schools offer instruction about how students can protect their physical safety, but I have found no equivalent advice on technology. My son and daughter researched more than 50 university Web sites and each of them provides a freshman orientation program on how to avoid an assault. Not one offers information on how students can protect themselves from identity theft or attacks by crackers using the university's network.

We do our home finances, exchange communications with friends, conduct business transactions, and do research to get answers for our homework or protect our personal health using the Web and networked information systems, but we treat these communications as if they were perfectly harmless and safe. It is as if there is a relationship between a person and a machine is somehow inherently safe simply because the person controlling the machine is out of view.

Finally, the issue of intellectual property theft via file sharing, warez sites, and other methods that show ignorance or disregard of copyright law protection. I have often asked teenagers, "What is the difference between stealing a CD from a music store and downloading music via Gnutella?" The answer is consistently the first is theft and the second is not. I have yet to receive an intelligent answer to why the downloading is not theft if the music was not paid for or if the purchaser violated copyright laws by posting the songs without the original artist's permission. Yet my children and their friends treat the posting of any form of information onto a Web site as if it were an announcement to come by and pick up free goods.

References to computers and related issues appear to be increasing in the media. But these sporadic mentions don't begin to cover the complexity of the issues and the rapid pace at which technologies change. I believe we are losing ground as we are struggling to talk about the myriad of topics which have daily impact on our lives.

Our society has had centuries to become familiar with "guns," whose operating principles have remained essentially the same as when they were invented. In comparison, the World Wide Web (WWW) came into existence in the last decade—the machines we use today employ hardware and software that advances so fast that today's versions appear not related at all to versions from only five years ago.

A young Royal Canadian Mounted Police (RCMP) officer I met at a recent conference nicely summed up the impact of technological change. During our discussion, he mused that advances and improvements are coming so fast that if he took a course at a local technical institute he could stay minimally up-to-date. Even with the sacrifice of his personal time, he acknowledged he would be proficient for only a few short moments after his course ended and before the technology passed him by again. Apply and compare his situation to single parents, adults with multiple jobs, and people with no time to emulate his diligence.

Considerations for change

I do not advocate slowing down the development or deployment of technology. Trying to shackle imagination and entrepreneurship is not the way to remedy our general lack of awareness about the issues raised by new capabilities. However, I do propose that we consider doing at least two things.

First, our society should discuss how to educate our children and fellow citizens about the benefits and perils of the technology we are developing and selling. We need education so recurrent and constant that each of us can become an informed user and maintain that proficiency. We need to know enough to automatically recognize issues such as E-mail is not inherently private, theft can be electronic and physical land our privacy is not necessarily respected by marketers.

Secondly, technology developers should distribute products that are safe to use and inform their customers about their limitations or potential hazards. Developers need to accept responsibility to develop and market products that have almost no security flaws, function exactly as advertised, are easy-to-use, and respect consumers' confidentiality.

I believe that a written definition of what a term means is not enough. Americans need to comprehend the implications of the enabling hardware and software of our era at least as well as they understand the dangers and responsible use of firearms. When we are cognizant of information technology as those senior military officers were of "guns," then we will realize the full potential of the Information Age. ■

About the Author

Leslie "Jake" Schaffner, Jr., CAPT USN (Retired), M.Sc.

Mr. Schaffner is currently a Senior Associate at Booz Allen Hamilton Inc. He serves as a functional specialist in information operations (IO) for a variety of national security clients.

Previously, he served as a Senior Strategic Analyst at SCITOR Corporation; as the Director of IO Policy In the Office of the Deputy Director of Central Intelligence for Community Management (ODDCI/CM); served as Chief of the Capabilities Division, IO Directorate on the staff of the Joint Chiefs of Staff;, and as Commanding Officer of the USS Mahlon S. Tisdale (FFG–27).

He has authored/co-authored numerous publications, such as: Presidential Review Directive (PRD) 56, Director of Central Intelligence Directive 7/3, Joint Publication 3–13, Presidential Decision Directive (PDD) 67, PDD 63, DoD Directive S3600.1, and Joint Chiefs of Staff Instruction 3810.08.

CAPT Schaffner received his M.Sc. in Space Operations from the Naval Postgraduate School and earned his B.A. in Geography from the University of Texas, Austin.

US, UK, CAN, AUS, and NZ Computer Network Defense Technical Conference

by James Peña

The Office of the Assistant Secretary of Defense (ASD) Command, Communications, Computers, and Intelligence (C3I) Information Assurance (IA) Directorate recently hosted a US/UK/CAN/AUS/NZ Computer Network Defense (CND) Technical Conference in McLean, Virginia on December 4–6, 2002. The purpose of the conference was to promote information sharing on a variety of CND issues from strategic to operational levels. The conference drew over 100 participants from the five nations. Foreign participants were from Defence Science Technology Office (DSTO) UK, Defence Information Technology Group (DITG) UK, and the Computer Incident Response Team (CIRT) Canada. U.S. participants included Combatant Command representation from Strategic Command (STRATCOM), Pacific Command (PACOM), Joint Forces Command (JFCOM), along with DoD and Government Agency's, National Security Agency (NSA), Defense Information Systems Agency (DISA), National Reconnaissance Office (NRO), Rome Lab, Army Research Lab (ARL), and the National Infrastructure Protection Center (NIPC). The keynote speakers for each day were Mr. Robert Lentz, Director, ASD, C3I/IA branch, Mr. Marcus Sachs, Director, Office of Cybersecurity, and Mr. Errol Schwartz, Director, National Sigint Incident Response Center (NSIRC). The conference featured over 25 presentations related to CND, law enforcement, and information sharing along with two days of afternoon forum discussions.

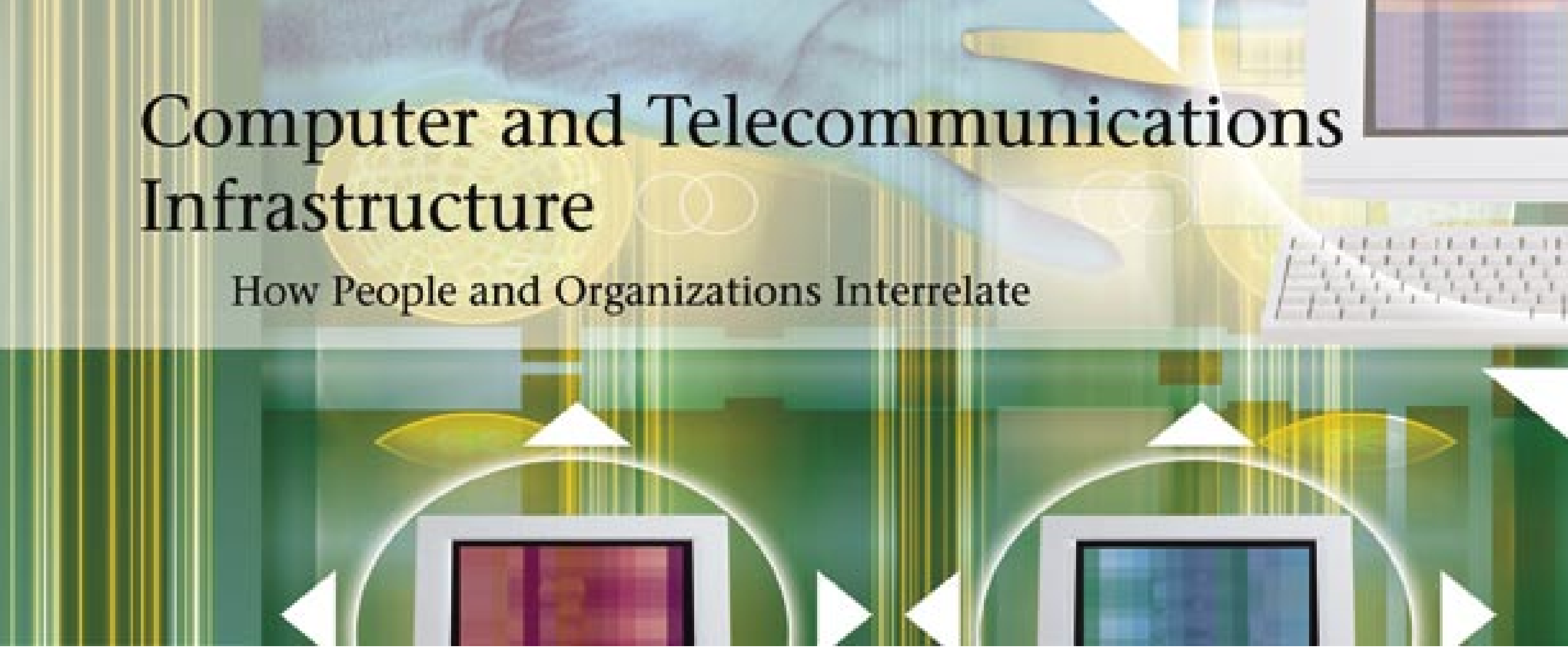
Day one

The first day started with Mr. Robert Lentz giving an overview on the Information Assurance (IA) mission, evolution of IA/CND, and IA Strategy and Transformation Roadmap. Mr. Lentz spoke of international actions needed in considering CND and expanding visibility into FIRST and other international groups, insuring incident reporting procedures are integrated to achieve a Common Operational Picture (COP), the importance of sharing information with the countries represented at the conference, understanding how CND operations will transition from peacetime to wartime. Each country then presented an overview of how they were organized for CND operations. A common conclusion realized by all of the participants was that information sharing between the nations is vital and that policies within the U.S. are changing to allow for broader exchange of operational CND information. The DoD Computer Emergency Response Team (CERT) and Joint Task Force for Computer Network Operations (JTF–CNO) also gave a presentation on CND trends and threats related to DoD.

Day two

Mr. Marcus Sachs outlined the National Strategy to Secure Cyberspace and the importance of ensuring that government, industry, and the public understand their roles in national strategy. Mr. Sachs pointed to Level 5 of the National Strategy for Securing Cyberspace, which called on nations to establish a national and international cyber watch and warning center, promote a global "culture of security," and encourage other countries to appoint a national cyberspace coordinator. He also mentioned ways to enable a "secure" Internet—accountable addressing (like IPv6), trusted (or trustworthy) software, and a working public key infrastructure. Other initiatives needed for a "secure" Internet are ensuring networks are built secure from the ground up, adopting best practices, protection from and for, clueless users, certification of network engineers and mechanism for information sharing. His closing thoughts were: security starts with the individual, seek to instill a "culture of security," what we build now is the foundation for the future, and International cooperation plays a key role in securing cyberspace. Mr. Aldrich of the Information Assurance Technology Analysis Center (IATAC) gave a U.S. CND legal briefing, focusing on legal authority and understanding what is required to obtain information related to law enforcement and counterintelligence issues. Items stressed during the briefing were the importance of knowing what legal authority is collecting information

...continued on page 24



Computer and Telecommunications Infrastructure

How People and Organizations Interrelate

by Paul Mays

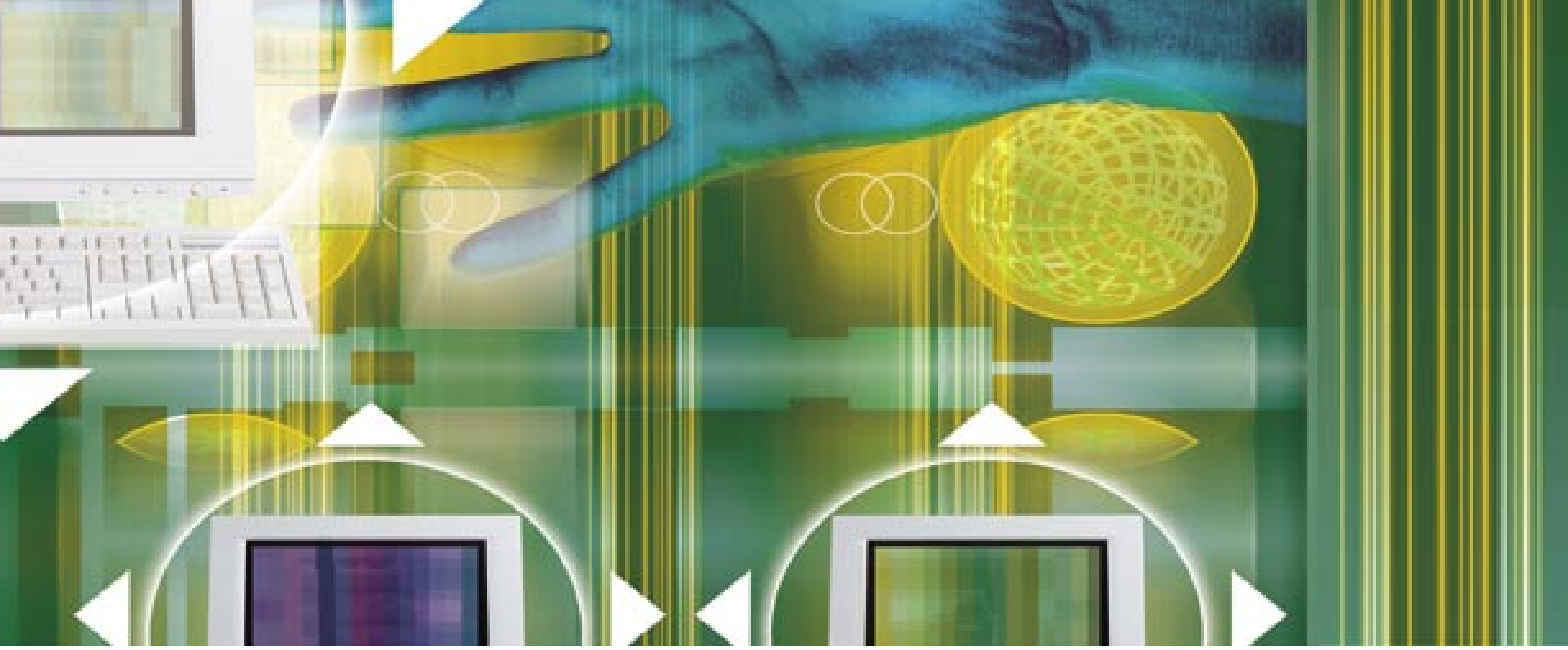
On a conceptual level, computer networks and telecommunications infrastructures can be viewed as systems of systems that allow us to communicate, accomplish tasks, and conduct organizational and external functions. Within this conceptual construct, our vulnerabilities would not only be understood as technological vulnerabilities within hardware and software but also our individual and group processes, interactions through communications, and organizational dependencies that rely on, or transported through, that technology. This article discusses this process-centric viewpoint and outlines the interrelationships between people, their organizations, and the supporting communications networks and automations services. In so doing, we will discover a new set of issues encountered in planning information assurance (IA) activities. The measure of our success in dealing with these issues will be realized in the identification, defense, and sustainment of critical individual tasks, group processes, and organizational functions within a hostile or potentially hostile environment.

> *The real question is not whether machines think but whether men do. The mystery which surrounds a thinking machine already surrounds a thinking man.*
>
> *B.F. Skinner, Contingencies of Reinforcement*

As B.F. Skinner, the late eminent behavioral psychologist alluded to in the previous quote—it is not the behavior of the machine that is the mystery but rather the behavior of the person interacting with it. The vast global information grid (GIG) and supporting infrastructure have no purpose or meaning without people performing activities within it. These activities are the actual vulnerabilities. Here is the foundation of our challenge—as network defenders determine those vulnerabilities not only within the context of technology but also by the manner in which we work within that technology and our expectations of that interaction. As we adopt new tasks and revise old functions resulting from the discovery of new applications available through the use of computer network technology, we should consider the consequences of losing them. This is particularly important if these tasks are critical path functions that have been entirely transported to computer networks vulnerable to attack. Ultimately, we must look at the supported organization's functionality and dependence on those processes and understand that defense-in-depth occurs along many aspects.

Let us consider for a moment how to visualize these aspects from the individual's perspective. The initial level in our understanding should be focused on the myriad of tasks that an individual performs in meeting their obligations to an organization. Some of these tasks can be accomplished exclusively by the individual. For example, adding a new name to a personal contact list can be done by the individual and requires no other human interaction. On the other hand, some tasks form part of a larger group process that accomplishes a more complex function or activity. An example of this might be individual contributions that ultimately lead to the publication of an operational plan. We need to understand that these people must perform these kinds of tasks using computer networks. And, if those actions are dependent upon the reliable, secure operation of those networks, then we must be able to visualize critical activities that have become dependent on computer networks and computer assistance and then understand what would happen if those activities were suddenly halted due to a computer network attack. This would allow us to begin understanding risk management as we decide what parts of networks are really critical to the people using them and taking risks by not working all potential technical vulnerabilities equally.

Now let us turn our attention to the second aspect we noted earlier. If we observe organizations closely, we will notice that there are a variety of tasks, sub-tasks, and tiered processes that lead to accomplishing that organization's functions and missions. These organizations in turn, work with other organizations and activities to accomplish even broader functions. In many cases, the unique contributions of one organization to another create dependencies between organizations—one cannot function without the other's participation. From a macro-level perspective, those



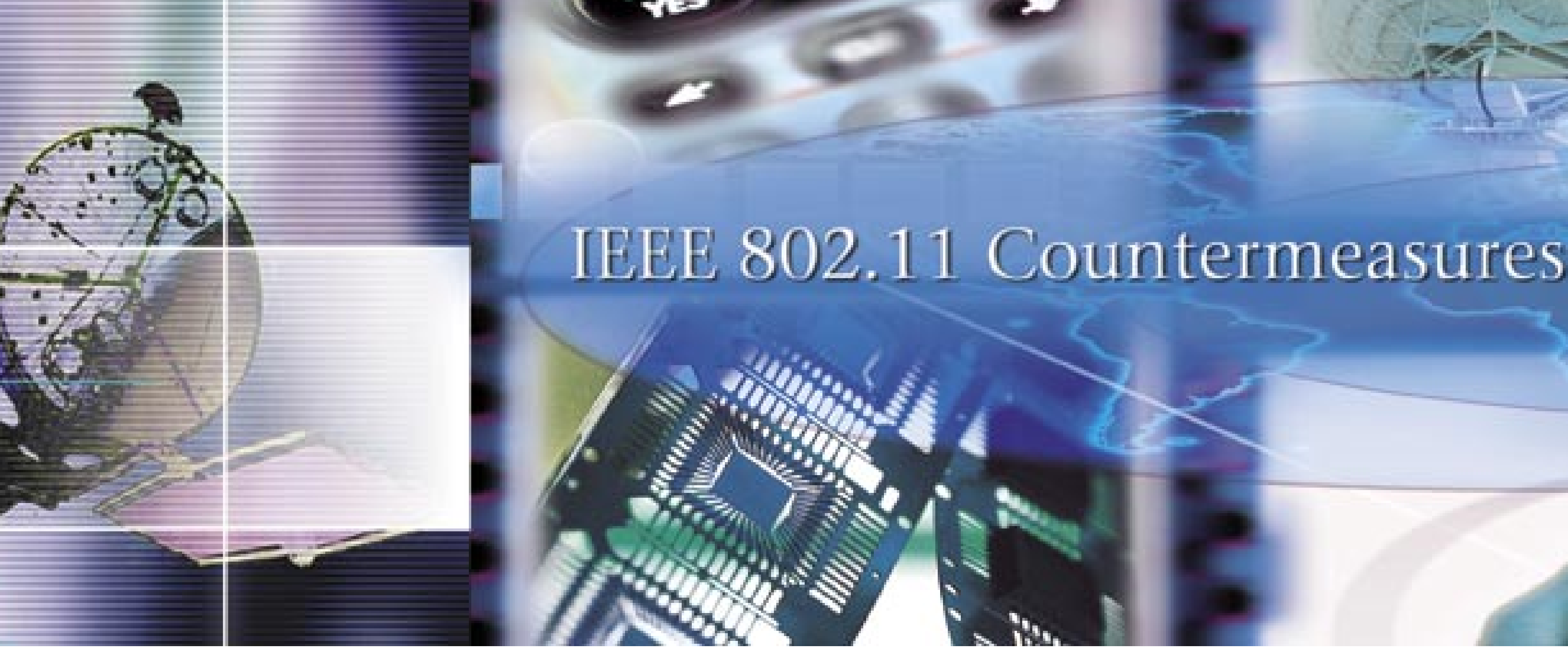
cross-organizational functions and coordinated efforts are potentially delayed by barriers for passing data caused by lack of appropriate communications technology. Hence, the focus of network designers and defenders is maintaining good communications. But how well do we understand all those activities that move back and forth between organizations in accomplishing those functions and performing coordination? And, are these organizational tasks standardized for specific activities? Or has the convenience of rapid communications created a larger problem of non-standard processes and an inability to really track operational threads of activities through the people, organizations, and missions that are accomplished? As a simple example, some organizations publish their operational plans on Web sites, while other organizations may only provide a point of contact in order to obtain an operational plan through E-mail. In this example, "protecting the distribution process for planning" is not a standard approach that can be applied to both organizations. In one case, maintaining the Web site is the most important aspect, while the other is maintaining E-mail services.

What have we discovered? First, we need to know how people use their computers, networks, and their expectations of them. From this, we can develop a process for differentiating critical and non-critical tasks. As part of that evaluation, we should expect critical tasks that we have identified as contributing to key group processes permitting an organization to function. As the organization provides its functional contributions to other organizations, we need to understand the dependencies that are created between organizations. Throughout this analysis we should know which critical tasks are dependent, partially dependent, or independent of computer networks. Defending the appropriate segments of networks on which these tasks are transported will allow us some capability for risk management and the ability to measure our success in sustaining our organization's mission. We should also be prepared to assist in figuring out contingencies or identifying critical tasks dependent on networks that cannot be accomplished if the network or computer fails. The approach of understanding networks from the individual and organizational process viewpoint will allow us to do exactly that. ■

About the Author

Paul Mays

Mr. Paul Mays is a retired U.S. Army Military Intelligence officer and MICA Knowlton Award recipient. While on active duty he supported operations for USPACOM, USCENTCOM, USEUCOM, USSOCOM, and USSOUTHCOM. Currently, he is an analyst in the Joint Task Force for Computer Network Operations (JTF–CNO) where he provides intelligence and operational planning support for DoD computer network operations. He is an active member in the U.S. Armed Forces Communications Electronics Association, Association of Old Crows and is pursuing a Master of Science degree in Management of Information Systems. He is a member of IATAC and may be reached at iatac@dtic.mil.



IEEE 802.11 Countermeasures

by Tyson Macaulay

IEEE 802.11b wireless LANs (WLANs) have been commercially available for five years, but have already attained a world-wide market of $1.5 billion (U.S. currency) as of 2001. The value of this market is expected to grow by 20 percent per year over the next four years, while the cost of components is expected to fall significantly. The result is that the installed base of WLAN components will increase by over 30 percent per year compounded for the next 4 years, and that is just the "b" variant of IEEE 802.11. [1]

IEEE 802.11 comes in two other main variants that will inevitably increase its reach and popularity—IEEE 802.11a and IEEE 802.11g. IEEE 802.11a possesses many features in common with 802.11b, but operates at a higher frequency (5 Ghz instead of 2.4 Ghz as in the case of 802.11b) and uses a different radio-carrier technology. The fundamental difference is that IEEE 802.11a supports data rates up to 54 Mbps whereas 802.11b supports a "mere" 11 Mbps. To complicate this issue further, IEEE 802.11g has recently been ratified and promises to deliver 54 Mbps of bandwidth in the 2.4 Ghz spectrum, again using very a different radio-carrier. Most if not all the countermeasure techniques discussed herein are applicable to any of the IEEE 802.11 wireless LAN standards.

The average cost of a WLAN network card is less than $100, while a base station controller, or access point (AP) costs less than $350. Most access points will support a full subnet of 256 addresses, all managed via on-board dynamic host configuration protocol (DHCP). "Starter Kit" bundles are available with a basic AP and client network card (station) for less than $400. WLAN services are deceptively simple to establish. No technical skills are required beyond the ability to follow basic setup instructions. The APs are simply plugged into the Ethernet LAN and they self configure.

Why is IEEE 802.11 so popular?

WLANs can provide significant advantages to organizations if implemented securely. They are as follows—

- WLANs are far cheaper to install and run than fixed-line Ethernet systems (approximately 30 percent savings according to studies from Gartner Group [2])
- WLANs offer greater movement and workplace flexibility
- WLANs allow remote, transient and visiting staff to immediately access network resources and increase productivity

What security problems are we trying to solve?

WLANs present significant security challenges, such as—

- Poorly configured WLANs are an open door into the organizational networks.
- WLANs can be detected and attacked from remote locations. Saboteurs, spies, hackers, the curious, and the malicious need not enter a building to access wireless systems.
- Without specialized equipment, it is not possible to detect when a WLAN has been turned on inside an office. They make no noise, require not special infrastructure and can be easily hidden from sight.
- WLANs, especially unauthorized WLANs, become active and inactive on a moment's notice as users power-up, shutdown, and reboot normal desktop systems and generally go about their business.
- Routine or scheduled inspections for wireless devices will always be insufficient. [3] So-called "wardriving" is now endemic. Using free, Windows based software [4] from the Internet, the lowest resource threat-agent (i.e., teenager) can now scan for the presence of WLANs and gather enough configuration information to attempt to join the network. In major urban centers, it is not uncommon for organizations to be scanned several times per day. [5]

Wireless Equivalent Privacy (WEP)

WEP is the security element that has been bundled to IEEE 802.11 directly and serves to provide confidentiality

and authentication services to IEEE 802.11 networks. WEP uses a shared (symmetric) secret-key to encrypt data at the data-link layer medium access control (MAC) layer using differing sizes of keys, depending on the manufacturer. The baseline security is 40-bit encryption using the RC4 algorithm. The IEEE 802.11 standard was amended in late 2000 to allow for the support of 128 bit encryption keys. However, WEP was still found wanting. The primary design flaws that make WEP vulnerable were not addressed by an increase in key size. There were two fundamental flaws found in WEP [6] security—a flaw in the use of key scheduling and random number generation that weakens the RC4 algorithm, but not to the point of making "practical" attacks feasible. The flaw was displayed mathematically rather than in real life. The second weakness was in the way WEP handled the RC4 keys to be used for encrypting the IEEE 802.11 data payloads, specifically, there is a problem with the use of an initialization vector (IV). The IV is concatenated to an RC4 key to make up the actual key that WEP uses for converting cleartext to cyphertext (i.e., encoding). Unfortunately for WEP, this IV is also transmitted in the IEEE 802.11 packet header in the clear along with the cyphertext for the purposes of rapid decryption at the receiving end. The IV was a sequential number that repeated more or less frequently, depending on the amount of traffic. This repeated IV allowed "crackers" to compare different encrypted payloads—for which part of the key is known—with enough sample data the full RC4 key is derived. Thus, an attempt to improve and simplify performance has damned WEP. Combined, these two distinct flaws punched a hole in WEP security.

The nail in the coffin of WEP's reputation was the release of tools on the Internet in mid 2001 that ostensibly allowed any low-resource "script kiddie" to successfully crack WEP keys without any significant skills or equipment. [7]

Despite all the forgoing, WEP serves a useful function in hardening an 802.11 network and should not be discounted completely for the following reasons—

- In order to crack WEP keys, you need to collect very specific types of packets from the data stream which occur infrequently. This means that you need a lot of traffic. Possibly days, if not weeks, worth of traffic on an average WLAN. For a determined attacker, this is very possible. But this requires far more patience and resources than a drive-by hacker possesses.
- Even with the right tools, such as WEPCrack, getting these tools to run can be a trick itself and requires significant knowledge of UNIX. [8] Again, a barrier to entry for non-programmers, and non-UNIX hacker-wannabe's.

IEEE 802.1x

IEEE 802.1x was introduced and popularized by hardware vendors once the flaws in WEP had been so badly exposed that it became a business imperative to offer a security alternative to WEP. IEEE 802.1x is actually the Internet Engineering Task Force's (IETF) extensible authentication protocol (EAP) applied to the IEEE 802.11 networks. IEEE 802.1x is also not an encryption scheme like WEP and therefore is not a strict replacement for WEP, rather IEEE 802.1x is an authentication scheme which can also be used to derive and refresh cryptography keys. [9] By this means IEEE 802.1x is a significant improvement in authentication and also allows for keys to be automatically refreshed for use in WEP itself, or optionally another crypto suite.

While IEEE 802.1x is definitely an improvement on WEP, it often requires significantly more infrastructure (such as a Radius Server) and is not supported by all vendors. The IEEE 802.1X standard was written for wired IEEE 802.3 networks so that it's application to wireless networks lies beyond the standard's original intent. The task of adapting IEEE 802.1X to 802.11 media is the task of IEEE 802.11i, which is providing several significant enhancements. [10]

IEEE 802.11i

As mentioned earlier, IEEE 802.1x is a partial implementation of IEEE 802.11i and therefore some of the "11i" features have already been discussed. Over and above the ".1x" security improvement, 11i offers yet more improve-

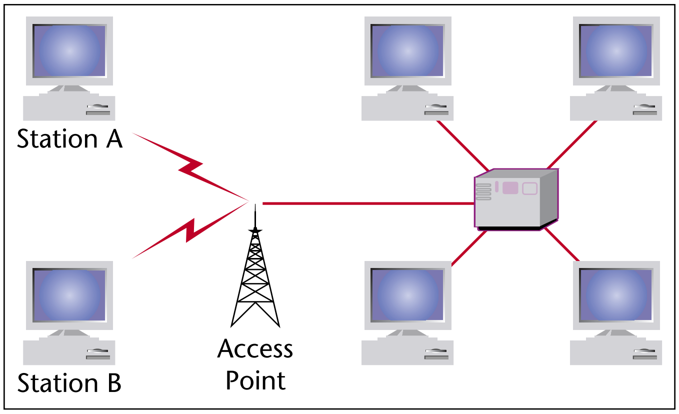


Figure 1. WLAN Overview [6]

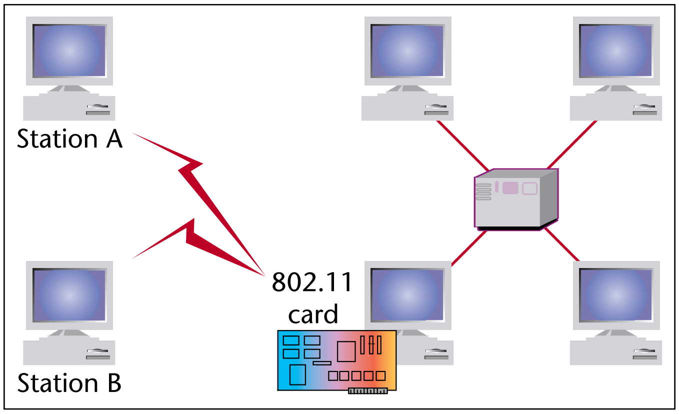


Figure 2. Peer to Peer Overview

ments. Specifically, 11i restricts stations from sending any data traffic until authentication has been successfully completed. 11i also mandates mutual authentication between the stations and the access point, as opposed to just the stations authenticating but not the access point. Furthermore, 11i supports optional AES-based crypto suites, specifically wireless robust authentication protocol (WRAP). [11]

Countermeasures and IEEE 802.11

Beyond the security provisions native to IEEE 802.11 specification itself, there are a variety of additional countermeasures available to organizations with WLAN "issues" shall we say. For the purposes of this discussion, the author has split the countermeasures into two specific classes—passive and active.

- A "passive countermeasure" could be described as a siege defense—implement a security system designed specifically to withstand attack.
- An "active counter-measure" could be considered defense through offense—the difference between coping with a problem and eliminating a problem.

The former style of countermeasure is well advanced and available from a wide variety of vendors. The latter style of countermeasure may be well-established in the military signals world, but is virtually unknown in the consumer-electronics world of IEEE 802.11.

Passive countermeasures

Passive countermeasures can be highly effective and depending on the realistic threats and security objectives, may be most appropriate. They can range from free to very expensive and for this reason the following passive countermeasures have been organized according to approximate cost.

Vendor enhancements

Most IEEE 802.11 equipment comes integrated with security enhancements that are beyond the scope of the specification. One of the most common is medium access control (MAC) address access control lists (ACLs), which allows connections to be restricted to devices broadcasting a permissioned MAC address. Unfortunately, MAC addresses are relatively simple to both discover and mimic. Other vendor enhancements include "cloaked" or non-broadcasting service set identifications (SSID)—a technique in which the SSID is not broadcast with beacon information, meaning that a user or device must know the SSID in order to associate with the AP. Unfortunately, SSIDs which are not included in beacons can be easily sniffed from ProbeRequests coming from legitimate users. A further genre of vendor enhancement are variations on WPA and IEEE 802.11i which were implemented so early that they are barely recognizable are specification derivatives. A technique introduced in late 2000 known as "fast packet keying" is an example of a proprietary vendor enhancement which rotated WEP keys automatically. [12]

The most important thing to be aware of with vendor enhancements prior to deploying them is interoperability. While the first two enhancements (MAC ACLs and cloaked SSIDs) will generally not impact interoperability of equipment across vendor solutions, while the third type of enhancement (proprietary key management) will likely disallow intra-vendor interoperation. This is especially true in the case of Temporal Key Integrity Protocol (formerly WEP2) (TKIP) which, confusingly, is implemented differently in WPA than in Cisco products which are not necessarily WPA-enabled.

Signal crafting

Signal crafting involves the integration of low-cost ($100's) antenna systems with off the shelf WLAN equipment to "shape" the coverage area.

> ***Disclaimer****—It is not possible to completely contain or obscure radio signals without drastic measures, such as a Faraday cage, which would severely limit the mobility and usefulness of an IEEE 802.11 network. Additionally, with the right equipment the techniques we discuss in this section could be rendered moot.*

"Signal crafting" is a term referring to the ability to partially control the range and extent of radio signals such that they are less likely to be perceived by a low or moderately resourced threat agent. One of the greatest security problems with IEEE 802.11 equipment is that is it generally tuned to broadcast at maximum power in all directions often resulting in the availability of network data far beyond the required range of the application.

Three primary techniques can be employed to contain the signal—to shape or "craft" the signal. They are as follows—

- **Access Point (AP) placement**—All access points are intended to radiate signal in an omni-directional pattern, therefore wherever possible, the AP should be placed in the center of the intended usage range. Similarly, APs should not be located next to exterior walls or walls shared with other building occupants. The idea being to simply try and only cover the required areas with radio signals, and avoid placing network information into areas you don't physically control.

- **Transmission (Tx) power management**—Following the same theme as above, many equipment vendors allow for the Tx power to be adjusted, normally through ambiguous descriptions of the power (high/medium/low) or sometimes the intended size of the coverage area (large/medium/small). In all cases, it is best to only use as much Tx as is required for the coverage area. Figuring out what is "enough" Tx will be a matter of trial an error, turning the Tx up and down while a device at the intended range limit reports signal quality. Generally speaking, 10 dbi of signal is the minimum to maintain a useful IEEE 802.11 connection.

- **Directional antennas**—Many APs allow for the attachment of after-market antennas to the on-board radios. Normally, when an external antenna is connected, they override the built-in antennas. This provides the opportunity to adjust the omni-directional characteristic of the build-in antennas. For instance, there are a variety of antennas in the 2.4 Ghz and 5 Ghz frequency range available off-the-shelf, which direct signal in a wider or narrower elevations and azimuths (horizontal plane). By selecting the correct directional antennas, WLAN administrators can further reduce the propagation of radio frequency (RF) into uncontrolled areas. One thing to note—directional antennas are not like laser beams in their accuracy. There will also be a certain amount of signal going out in the unwanted directions as "side-lobes" and "back lobes." However, the better the antenna the smaller the amount of undirected. Similarly, the effect of signals bouncing off objects, "multi-path," will also degrade the effectiveness of a directional antenna.

Wireless intrusion detection systems (and network analysis)

This third class of passive countermeasure is fairly new and will range in price from several thousand to several tens of thousands of dollars per site.

Intrusion detection systems (IDS) are still relatively new in the fixed-line world but have already been extended to the IEEE 802.11 world. An IDS monitors network activity looking for traffic that indicates an attack in progress or tell-tales signs of a compromised system. Typically, an IDS would be deployed either on the outside of a firewall (facing the Internet) or possibly on a subnet dedicated for external facing services (e.g., demilitarized zone). The concept is that if you can detect the attack once it starts, you are less likely to be compromised because you can initiate a countermeasure before the attacks succeeds. There are several companies offering variations on this theme in the wireless world, [13] with the primary objective being the early detection of either rogue IEEE 802.11 stations or APs. These companies are both pure-play wireless IDS vendors and sometimes vendors of broader, network analysis tools that can be used for IDS-like purposes.

Typically, an IDS functions by sitting on the network and observing all network traffic without actually sending any data. In the process of this "observation," all the data packets, including headers and payloads, would be put through an analysis process. This process can be more or less detailed and intrusive, but in all cases will be looking for tell-tale patterns of an attack, abuse, or compromise. For fixed line networks, higher level details such as source, destination, port, protocol, payload size, and payload content might all be considered in an IDS logic system. Wireless IDS systems would go down to lower network levels that fixed-line systems, into the MAC levels of IEEE 802.11, but typically leave the higher level analysis described above to fixed-line IDS systems.

An example of a rogue station would be an unauthorized IEEE 802.11 laptop trying to associate with the corporate AP. This could be hacker, or a misconfigured laptop or just a benign visitor in the reception area. A rogue AP is generally a more serious and less commonly seen phenomena. A rogue AP implies an authorized network that has been established inside or close to the corporate facilities such that its signal is perceptible by legitimate wireless users. Rogue networks require immediate countermeasures for the following reasons—

- A rogue AP set up by a misguided employee (or threat agent) is often a back-door directly into corporate network

- A rogue AP with a strong signal may very well attract legitimate internal users to its signal, by virtue of the fact that the IEEE 802.11 specification predisposes a device to associate with the strongest signal, after which time it transmits internal information through the rogue AP unknowingly.

- A rogue AP, if not actually compromising users, could interfere with the legitimate wireless systems to the point of executing a denial of service attack.

Third-party VPN and access control

This last class of passive countermeasure is the most diverse and comprehensive in functionality. VPN and Access control solution for IEEE 802.11 will range in price from the low tens of thousands of dollars to mid tens of thousands per site.

There are well over a dozen companies offering IEEE 802.11 security solutions that essentially fall into two camps—virtual private network (VPN) and access control. [14] The VPN camp layers in varying strengths of encryption into either the transport or session layer of the WLAN communications. Often the solution is the Internet Protocol Security (IPSec) or an IPSec derivative, [15] and results in an encrypted tunnel being formed between the station and the AP. Sometimes the "tunnel" transverses the AP entirely and terminates on a server located in the fixed-line LAN somewhere. An alternate approach is a very granular access control scheme that requires stations to be authenticated prior to joining the network with the authentication system referring to a sophisticated back-end server that controls possibly dozens of APs at once. Most third-party vendors offer both VPN and access control at once, and are original equipment manufacturer (OEM) versions of larger vendor's equipment with proprietary add-ons to support the VPN/access control functionality.

Active countermeasures

The difference between active counter-measures and passive counter-measures is the difference between attempting to cope with a problem versus eliminating a problem.

This difference is critical because while VPN and access control can be used to effectively cope with issues of confidentiality, they do little or nothing for availability and integrity. As long as a rogue device is operating within range, it can inflict (intentional or accidental) denial-of-service (DoS) attacks. An unaddressed rogue can also continue penetration attempts unimpeded, bait users into traps.

In the world or WLANs and active countermeasures this means precision, location finding capabilities, or possibly techniques to simply neutralize the rogue devices pending investigation. Unlike the previous section, solutions will not be presented according to cost. Solutions will be presented in the order of their entrance into the market, which in all cases is less than one year.

Location finding

Location finding of IEEE 802.11 devices is one of the newest adjunct capabilities to be developed for security purposes. Location-finding has an obvious security function—find the rogue device and shut it down before it can cause harm. Location finding using IEEE 802.11 has many other applications outside of security too, such as stock management and personnel tracking. The results of this dual-use are two primary approaches to location-finding in IEEE 802.11. The first approach is based on "traditional" techniques of signal-strength direction finding, while the second is an evolving family of triangulation techniques.

Direction finding

Signal-strength direction finding involves the use of specially developed directional antennas coupled with signal processing software. The antennas display a dramatically weaker perceived signal when not pointed directly a the source of the signal thereby leading the operator to the source by watching signal strength increase and decrease as they alter the direction of the antenna. It should be noted that the efficient usage of direction finding equipment is an acquired skill and not a mean feat—signals reflect, refract, and generally misbehave. Much of the effectiveness of an IEEE 802.11 direction finding security tool will have to do with the user interface and equipment ergonomics.

Two companies have developed specialized tools for IEEE 802.11 direction finding with security in mind—Peel Wireless and BV Systems. Between the two, Peel Wireless offers a more sophisticated and accurate antenna system and software interface, while BV Systems offers a more portable solution.

Triangulation

Triangulation as a location-finding technique involves the use of perceived signal strength of a target device from at least three distinct observing devices. However, most of the "triangulation" techniques actually involve many observing devices all reporting and comparing observations (we are referring to this technique as "triangulation" for convenience only). This system operates on the basis that perceived signal strength and distance are related and predictable through the physical laws [16] around "free space loss" and signal decay. If the positions of the observing devices are known, then using the perceived differences in signal strength from the target device it is possible to calculate the position this device. There are at least three companies pursuing variations on this theme—Ekhau [17], Newbury Networks [18], and IBM (a project they are calling Wireless Security Auditor which is not out of the lab yet). [19]

Triangulation in a security context has several serious problems. First, the technique will often rely on knowing certain characteristics about the target device in order to correctly calculate position, such as its transmission (Tx) strength. Many IEEE 802.11 devices have varying Tx strengths, or manually adjustable strength. Second, significant processing power is required for the calculations, possibly more than is suitable for anything other than a desktop machine. This means that two operators are required to track and locate a device—one to work the desktop and relay instructions/position changes to the second operator who is trying to visually locate the target. Third, the accuracy of these systems is not granular enough. Remember, we are tracking something no larger than a laptop. One square meter accuracy is the best claim made, but these claims should be accepted with caution. Three to five square meters is more likely in the field. When you add in a third (vertical) dimension, you have an area of 27 to 125 cubic meters of space to search. This could span multiple floors and be full of obstacles and hiding places.

In the end, signal-strength direction finding is the most appropriate for IEEE 802.11 security applications because it is a relatively simple, rugged solution that can be operated by security personnel on the spot.

Automated neutralization

Automated neutralization is the latest form of countermeasure and involves disabling an IEEE 802.11 station or AP through a variety of manipulations of the IEEE 802.11 specification—specifically the manipulation of "frames." A "frame" is a unit of information in the IEEE 802.11 world. Frames can be management frames, control frames, or data frames. Management and control frames are used to support the MAC and data link layers (i.e., access to and performance of the wireless network). Data frames carry the information payload for all higher-level services and applications. [20] By fabricating and broadcasting specialized management and control frames, it is possible to exert significant control over an IEEE 802.11 device. For instance, forcing it to stop transmitting or make it "disconnect" from the network.

One example of such a manipulation of the IEEE 802.11 specification is a disabling attack using "disassociation" management frames. To understand how we can manipulate these frames for security purposes, we should understand a little about the "legitimate" purpose of a disassociation frame. In IEEE 802.11, a disassociation frame is for an AP to tell a station to disconnect because it is about to shut down, thereby allowing the station to maintain network connectivity by forming a new association with another AP within range. Alternately, a station might be roaming and wishes to break off a connection with one AP to form a stronger connection with a closer AP. In this case, the AP that is being left behind needs to know that the station no longer requires its services, so the new AP can take over the wireless traffic. Without these management frames there would be horrendous problems of latency time-outs and data collisions. In a security context, disassociation frames can be used to disable an unauthorized device. By telling it to leave the network every time it tries to join.

Peel Wireless [21] has developed a solution for monitoring and controlling unauthorized IEEE 802.11 devices. Part of this solution is a countermeasures device that can be configured to automatically disable unauthorized devices using techniques, like the one described above. The idea behind this product is that any unknown device is assumed hostile, and is treated as such until administrative personnel can locate and identify the device. Alternately, the device is denied any sort of IEEE 802.11 transmit capability until it registers with a local administrator.

Conclusion

This article has discussed native IEEE 802.11 security and different counter-measure solutions. Counter-measures themselves have been described as passive and active, and we have attempted to outline the capabilities and characteristics of both varieties. The appropriateness of native security over different countermeasures is highly subjective and involves considerations around the requirements of confidentiality, availability, and integrity of WLAN resources. In an ideal world it would be possible to deploy both varieties of countermeasure to protect resources. Generally speaking, an active countermeasure requires more effort to employ, while a passive measure can run on auto-pilot. Alternately, the more sensitive or valuable the data on the organizational network, the more imperative it becomes to eliminate a threat as opposed to "living with it." Similarly, native 802.11 security will provide enough of a barrier to allow well managed, active countermeasure to take effect.

Finally, there is one sort of IEEE 802.11 threat that no countermeasure can provide defense against—pure, passive "sniffing." If the intent is to simply observe and record the network traffic without trying to engage the network in anyway—it is virtually impossible to detect such activity. If your organization cannot live with this reality, even with good countermeasures in place, then prohibit them altogether. Just be sure to back-up your prohibition with compliance monitoring, such as a wireless IDS tuned to alert on any signal. ■

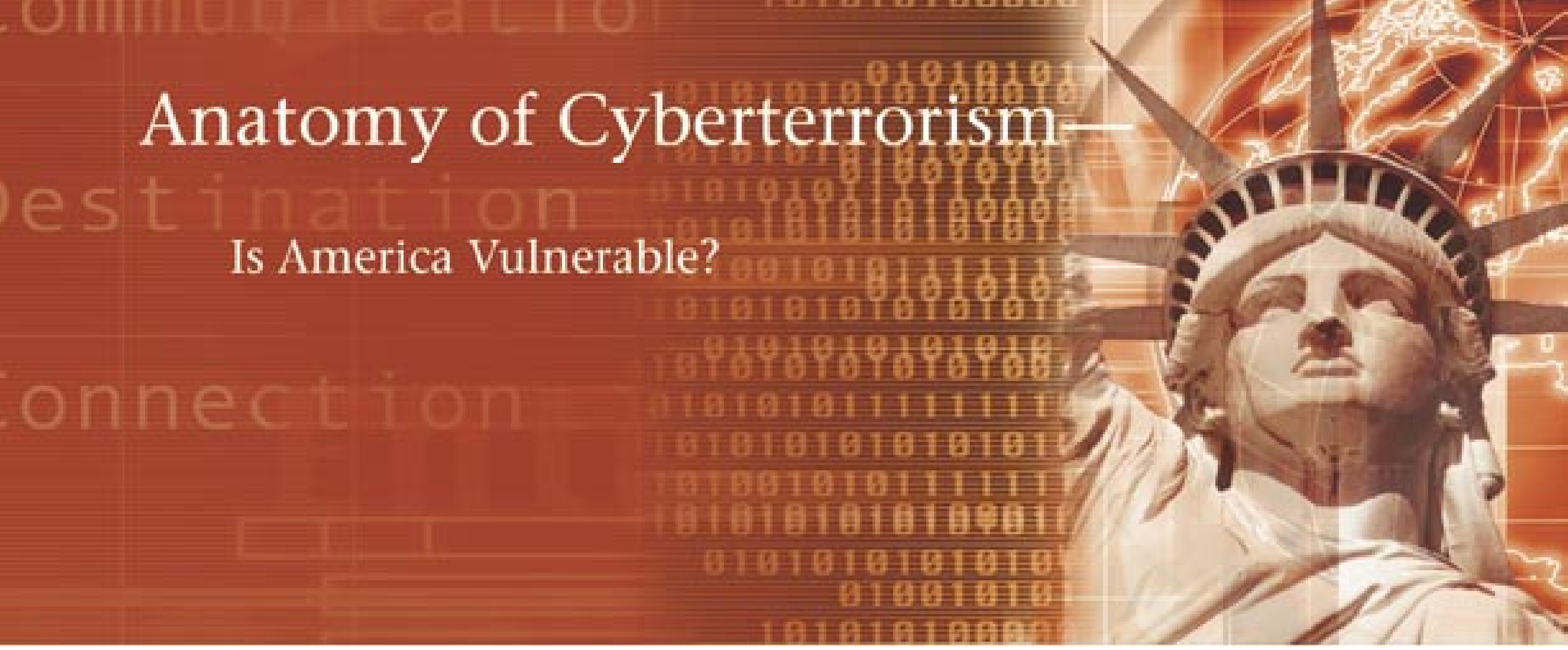
About the Author

Tyson Macaulay

Mr. Macaulay is co-founder of Peel Wireless, an IEEE 802.11 security firm, where he holds a part-time position as Chief Technology Officer (CTO). On a full-time basis, Mr. Macaulay holds a Director position in a Canadian defence contractor specializing in public key infrastructure (PKI), wireless security, and business process security. After completing his university education in Political Science in 1992, he started his career building the first generation of Internet services as a developer and system administrator from 1992 to 1996. From 1996 to 2001, he worked as CTO in a security company he co-founded where he acted as prime security architect for PKI implementations in both public and private sector institutions, working on projects from conception and development to implementation. Mr. Macaulay's first company was successfully acquired by a larger industry player in 2001. His work has covered business strategy, needs assessments, threat risk assessments, operational policy development, authentication processes, security architecture, and application design. Project work and speaking engagements have been conducted around the world involving international governments and multinationals as both stand-alone clients and in multi-lateral, collaborative projects, and forums. He may be reached at tyson@peerwireless.com.

References

1. IDC WLAN market forecast 2002–2006.
2. 802.11 Planet http://www.80211-planet.com/tutorials/article.php/953691
3. Investigations conducted by the author show approximately a 20 percent deviation in the "population" of access points available from a urban business, location on a week to week basis.
4. Netsumbler, WLAN export.
5. The author has planted "wireless honey pots" at client sites in Ottawa, Canada to obtain this statistic.
6. http://www.eyetap.org/~rguerra/toronto2001/rc4_ksaproc.pdf
7. http://wepcrack.sourceforge.net/
8. Ibid.
9. http://www.drizzle.com/~aboba/IEEE/
10. Bernard Aboda, IEEE 802.11i TWG
11. http://www.wi-fi.com
12. http://www.wi-fi.com/opensection/pdf/wi-fi_protected_access_overview.pdf
13. http://www.wired.com/news/business/0,1367,56350,00.html
14. http://www.inetdevgrp.org/20020618/WLANSecurity.pdf
15. RSA Security.
16. Peel Wireless, Air Magnet, Wild Packets, ISS, Air Defence , Network chemistry, Airwave/3eTI.
17. Colubris Networks, Fortess Technology, Filanet, Red M, Vernier Networks, Reefedge, Airdefense, Meetinghouse Data Comm, Bluesocket, Funk Software, Excino, Chantry Networks.
18. "Simplify PKI with Hybrid Auth and Xauth" http://www.nwfusion.com/news/tech/2000/0828tech.html
19. Friis Free Space Equation http://stewks.ece.stevens-tech.edu/EE683/WebNotes/Chapter4Home/FriisMod/friis-basic.html
20. http://www.ekahau.com/
21. http://www.newburynetworks.com/
22. http://www.research.ibm.com/gsal/dwsa/
23. IEEE 802.11 Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications http://standards.ieee.org/getieee802/
24. http://www.peelwireless.com



Anatomy of Cyberterrorism—

Is America Vulnerable?

by Col (Select) Bradley K. Ashley, USAF

Editor's Note—The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the U.S. Government or the Department of Defense (DoD). In accordance with U.S. Air Force Instruction 51–303, it is not copyrighted, but is the property of the United States Government.

The United States is vulnerable to attacks from cyberterrorists. A "Digital World Trade Center Attack," killing thousands and costing billions of dollars, is quite plausible today.

The events of 9/11 caught us by surprise. We cannot afford to discard the cyber threat and be caught by surprise by a major cyber assault. Unless we take the appropriate steps to protect ourselves against cyber attacks now, America will surely suffer tragic cyberterrorist attacks that will include loss of life.

> *There is nothing more difficult to take in hand, more perilous to conduct, or more uncertain in its success, than to take the lead in the introduction of a new order of things.*
>
> *Machiavelli*

The global media is buzzing with reports of American Military systems under relentless electronic assault from computers in the Middle East. The latest media buzz term is "cyberterrorist." An unknown adversary controls logistics, transportation, administration, and accounting systems essential to deploying troops just as troops begin deploying to the Persian Gulf to enforce Iraqi compliance with United Nations inspections. DoD debates the pros and cons of removing all its Internet connections. Many of America's largest commercial Web sites are flooded with connection requests rendering them inoperative and paralyzing significant portions of the Internet. Deadly viruses begin to infect computers and data around the globe including many Military systems. Both Government and private sector networks are destroyed. Over 60 million computers are affected costing billions of dollars. [1] The timing of the cyber attacks is so accurate—the attacks are interpreted as a first wave of subsequent attacks by a hostile nation or group.

Web sites spring up like weeds calling for an electronic war and providing training on nuclear, chemical, biological, cyber attacks, and explosives. People around the globe are invited to join in electronic attacks simply by clicking on a Web site button to begin a flooding campaign. Osama bin Laden calls for a cyber Jihad on an Afghanistan hosted Web site. Computers at American infrastructure sites, like airports and dams, are infiltrated. Over one million liters of raw sewage are released into rivers and coastal waters. Agents tied to Al Qaeda buy useful information to penetrate DoD computer networks. Power grids in California are infiltrated and held captive for weeks. Vigilante American hackers strike back at government computers of several suspected countries in the Middle East who may have initiated the original attacks. Cyber security experts testify before Congress that there is a high probability of further cyberterror attacks. The stock market is closed early due to computer problems after a record setting one-week loss. Americans are alarmed at the devastation, cost, and results of these cyber attacks coming on the heels of the World Trade Center tragedy. The competitive media help spread the panic throughout the nation.

Does this scenario sound like science fiction? Is this a realistic scenario or panic filled rhetoric and hype? I assure you that it is 100 percent plausible because each one of the events described above has already occurred. Fortunately for us, these events took place at different times over the past several years. But could they happen in an orchestrated fashion in a short time frame in the future?

My model describes the anatomy of cyberterrorism. It is descriptive and should not be confused as a prescriptive model. In order to fully understand cyberterror, one must first understand the cyberspace environment and its unique attributes. Then by analyzing the various components of the cyberterror anatomy, we can grasp the answers to basic questions: who, what, how, where, why, and when. Only after one understands these basic pillars, can one fully understand the whole of cyberterrorism.

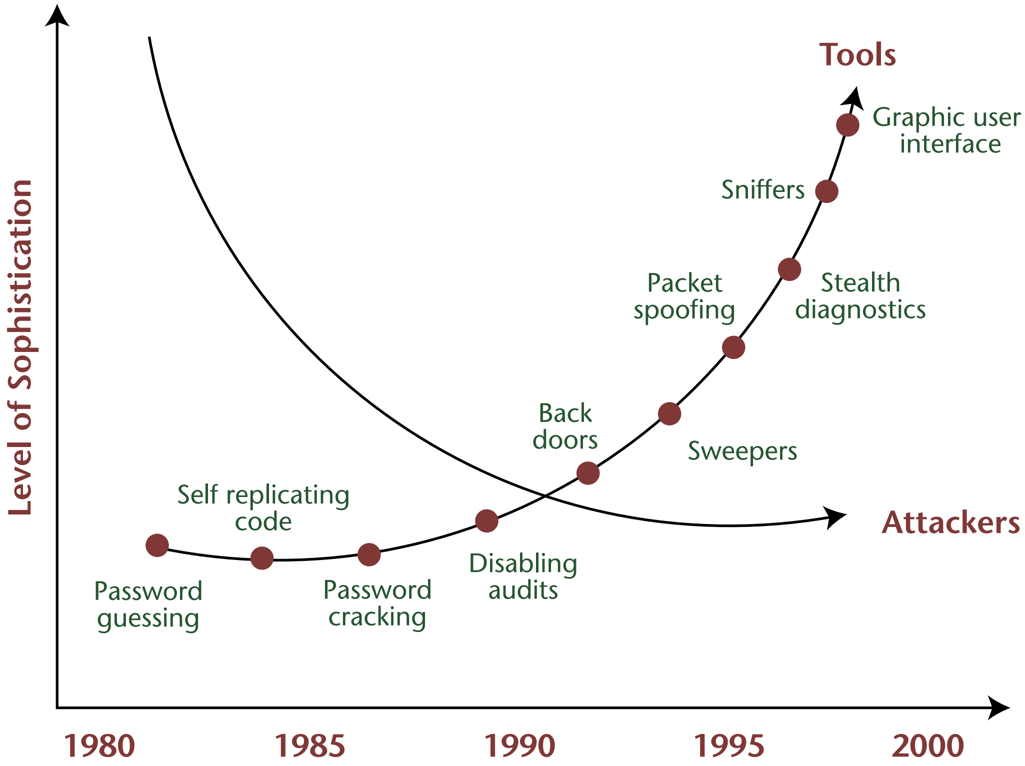


Figure 1. Level of sophistication over time

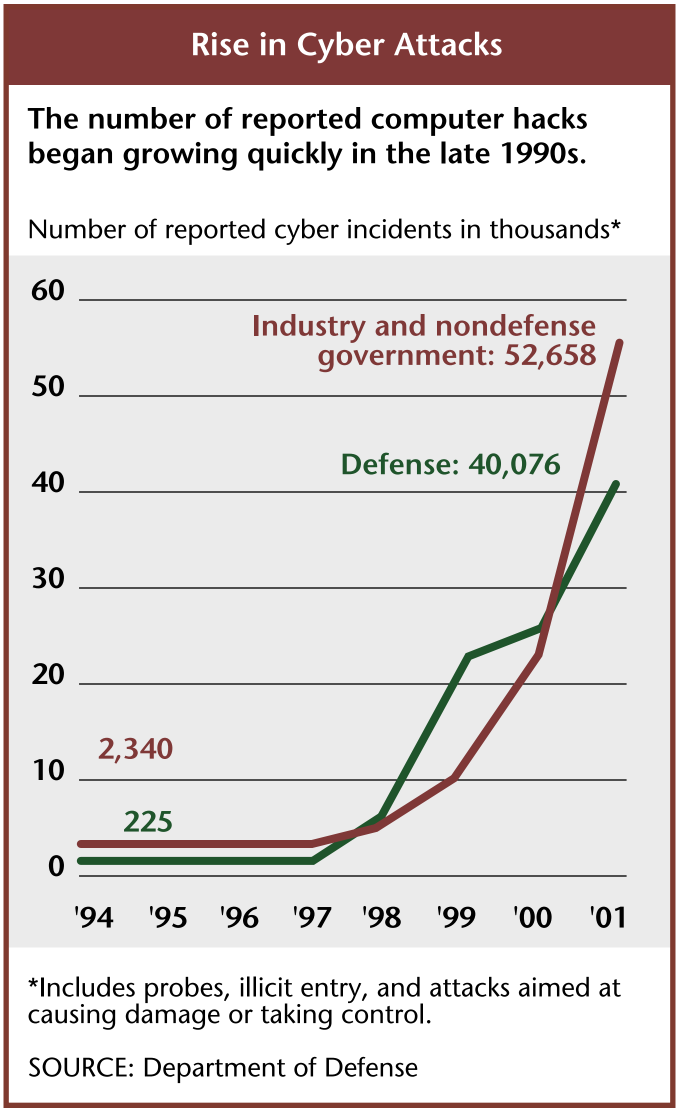
Tools and techniques—what?

It is getting easier

Over time, the level of sophistication required to hack into an information system has dramatically decreased. At the same time, the quality, quantity, and availability of hacking tools has dramatically increased. This creates an environment where teenagers successfully infiltrate DoD and U.S. Government systems. This creates a very dangerous target-rich and low-risk combination. Statistics show cyber attacks are on a dramatic rise.

Cyber weapons are often readily available for download on the Internet. Unlike the tools of conventional warfare, the tools of this trade require no long-term acquisition, training, and fielding process to mount an attack. As the typical PC has become more powerful and easier to use, so has the sophistication of the weapons that information adversaries have at their disposal. A comparatively low technology adversary with minimal funding, training, manning, and defense infrastructure is capable of employing these weapons on short notice from anywhere in the world. One key advantage afforded the information warrior is freedom from the burden of time and money needed to field and project a conventional force.

One common method to gain unauthorized access is through the normal log-on process from the command line prompt of a telnet or remote login session. User names and passwords may be gleaned from any number of methods. Free password cracking software is available on the Internet


Rise in Cyber Attacks

The number of reported computer hacks began growing quickly in the late 1990s.

Number of reported cyber incidents in thousands*

*Includes probes, illicit entry, and attacks aimed at causing damage or taking control.

SOURCE: Department of Defense

Figure 2. Cyber Attacks on the Rise

for anyone wishing to test the security of (or break into) networked systems. Once logged onto a system as a valid user an attacker may read, copy, delete, substitute, and modify data and programs on the host. Other computer vulnerabilities are easily found on the Internet to include corresponding exploitation tools.

Why are attacks on the rise? Several factors go into this equation: the growth of the Internet raises the number of both attackers and targets, vulnerabilities of new software version releases continue to grow, and sophisticated hacking tools are readily available.

There are countless actions an intruder could take after gaining access to an information system. However, these acts can be summarized into four general categories—modification, fabrication, interception, and interruption.

Modification

Modifying data is also known as “spoofing.” Unauthorized users who gain access to data can add, modify, or delete data. If done properly, this method can go unnoticed for a long period of time. Imagine the havoc caused simply be replacing all the “1s” with “7s” in an Air Tasking Order or Deployment Order (see Figure 3).

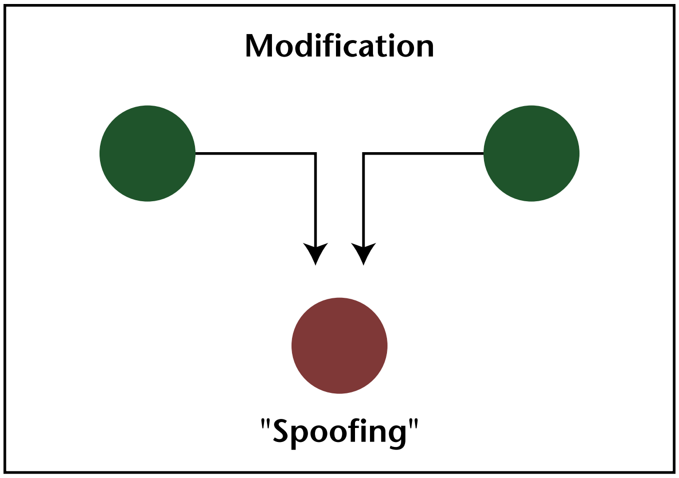


Figure 3. Modification

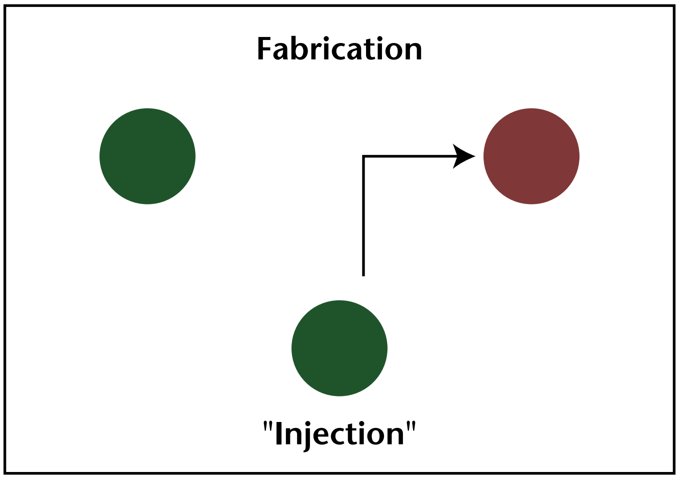


Figure 4. Fabrication

Fabrication

Fabricating or “injecting” data into a command and control system can wreak havoc on a system. Loss of confidence in the entire network can result. Imagine injections of new sorties into an Air Tasking Order or cancellation of needed logistics. This method requires experience in or knowledge of the attacked system in order for the injected messages to appear credible and authorized (see Figure 4).

Interception

Interception or “Intelligence gathering” is the least intrusive technique. Simply monitoring or copying data for the purposes of gaining valuable intelligence on an enemy is very valuable to our adversaries. Imagine the impact of an enemy having a copy of our Air Tasking Order in advance. Targets could be relocated, defenses could be adjusted, counter-air could be waiting in ambush (see Figure 5).

Interruption

Interruption or denial-of-service (DoS) is probably the most intrusive technique. There is little doubt to a skilled adversary that the enemy is “inside the wire” and they are undergoing an attack when a DoS attack occurs. Surprise

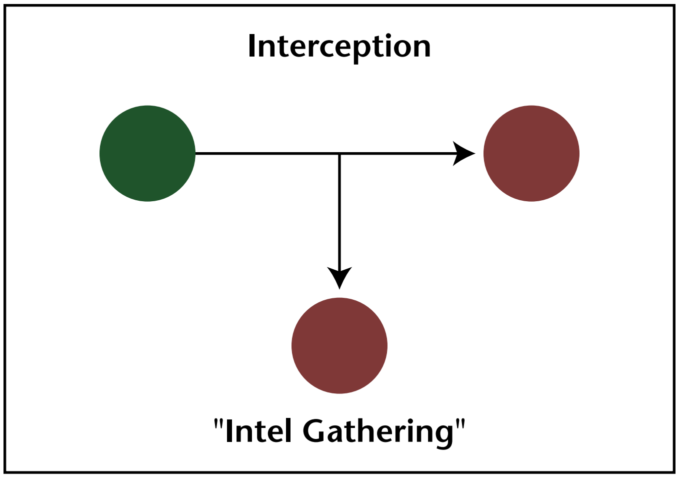


Figure 5. Interception

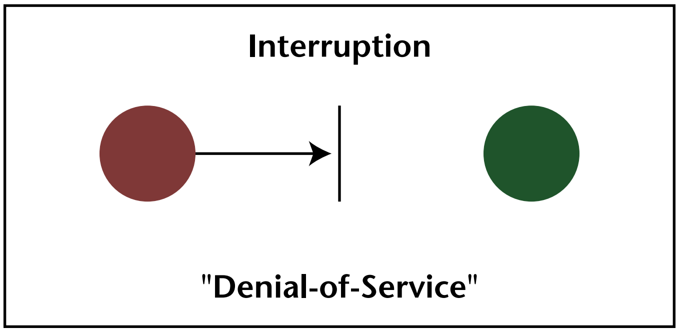


Figure 6. Interruption

is lost and future access to the target system may also be jeopardized. Timing is everything with DoS attacks. Imagine the potential impact of a DoS attack on a command and control system that coincides with a major Military offensive (see Figure 6).

Cyber tactics, techniques, and procedures (TTPs)—how?

For decades, the world has witnessed unauthorized intrusions and Web hacks from a myriad of actors: teenagers, industrial espionage experts, hacker groups, and nation states. Newcomers to this area have infiltrated very sensitive systems with relative ease. There are many TTPs utilized by these actors.

Polymorphic viruses/code

Polymorphic viruses or polymorphic code changes its fundamentals with each replication in order to preclude detection, filtering, blocking, or anti-virus software. Polymorphic viruses take on many forms. Some insert junk code into the virus source code, while others insert random numbers or extra line feeds. More sophisticated versions change their virus code variable names with each replication. This tactic is intended to make detection much more difficult and allow viruses to proliferate further without restraint. [2]

WM95.Slow was the first true polymorphic macro computer virus. More recent ones include: Nasty, Zevota, and Jug.A. These viruses vary in several ways and further the ongoing "cat and mouse game" of virus authors, anti-virus software, and network defenses. Detection of polymorphs is extremely difficult and poses a real concern for the future. [3]

Worms

Worms are independent programs that replicate themselves to congest networks. They can be very malicious and destroy valuable data. The Nimda worm caused an estimated $530 million in damages worldwide. [4] The Code Red worm (July 2001) infected a quarter million computers in nine hours and was labeled "a real and present threat to the Internet" by the National Infrastructure Protection Center. The Slammer Worm infected more recently 75,000 hosts in less than 10 minutes. [5] Code Red caused an estimated $2.6 billion dollars in damages. [6] Worms are very costly and are serious threats.

Viruses

Viruses also cause a great deal of damage and are proliferating at ever-increasing rates. The I Love You virus (May 2000) infected millions of computers worldwide and caused billions of dollars in damages in just 5 hours. It had over 80 variants and was traced back to one individual. The Melissa virus set records with its unprecedented rapid spread around the world and set new standards for the world.

DoS attacks

DoS attacks are characterized by intruders obstructing access to a computer system from one or more authorized users. The damage done to national security interests by such attacks depends on the functions of the actual system attacked.

October 2002 marked the most coordinated attack on the Internet itself seen to date. Attackers sent floods of traffic to the Internet's 13 core domain name servers. These devices serve as the Internet's phone book properly routing traffic to its destination. Nine of the 13 were taken off-line. DoS floods of this type have been predicted for over two years. This attack demonstrated both the intent and capability to potentially take down the Internet. [7]

Categories of information targets—where?

Recent discussions by experts before Congress have included targets such as: the Centers for Disease Control, financial networks, water supplies, major cities, electrical grids, dams, the Internet, telephones, air traffic control, rail, and public transportation systems. [8]

The President's Commission on Critical Infrastructure Protection (PCCIP) divided our national infrastructures into five sectors—

1. Information and communication
2. Physical distribution
3. Energy
4. Banking and finance, and
5. Vital human services.

Motives—why?

Physical attacks are the simplest. Nuclear, chemical, and biological attacks require very specific skills, knowledge, and materials and may be much more difficult to

Table 1. The five sectors of our national infrastructures as defined by the Presidents Commission on Critical Infrastructure Protection (PCCIP) [9]

Information and Communications	This sector includes the public telecommunications networks, the Internet, and millions of computers at homes, business, industry, and government.
Physical Distribution	This sector includes our interconnected network of highways, rail lines, ports, pipelines, airports, mass transit, and trucking companies.
Energy	This sector includes industries that produce and distribute electrical power, oil, and natural gas.
Banking and Finance	This sector includes banks, financial services companies, mutual funds, securities, and commodities exchanges.
Vital Human Services	This sector includes water supplies, emergency services such as police and fire, and critical government services such as social security and unemployment payments

implement. In an asymmetric world, terrorists will look for alternate methods to spread terror. The cyber world may prove to be the simplest and quickest alternative to traditional physical attacks.

Motives of cyber attacks vary greatly: intimidation, coercion, retaliation, influence, power, specific objectives, revenge, induce fear or panic, decrease public confidence in infrastructures, spread ideology (religious and/or political), or financial gain. Terrorists motives will likely be the same as physical attack motives. The dilemma in the cyber world is to not only detect who is attacking you (individual, group, nation) but understand why.

Effects/results

Terrorists will likely seek: financial impact, ransom, disruption, decreased military capability, fear/panic, publicity, news impact, decrease confidence in critical infrastructures, psychological operations, great physical damage, and/or loss of life. There are many distinct advantages to cyber attacks: cheap, fast, tough to trace, low risk, no martyrdom required, no handling of explosives, no border crossings, low probability of detection, easy to hit and run, detection and trace actions are difficult, borders do not have to be crossed, logistics requirements are low, remote, anonymous, can operate from anywhere on the globe and be mobile, range, appeals to younger generations, and are stealthy.

There are also disadvantages: takes resources, new skills for many terrorists, could possibly be traced, takes lead time to gain accesses, hard to control, less drama and emotional appeal, may not try new methods until old ones are inadequate or protected against, controlling systems can be complex without the right skills. The cyber world is relatively new in the terrorist world. However, future generations that grow up computer savvy may see this as the future's perfect asymmetric attack method.

Timing is critical—when?

Stand alone/isolated attack

Cyber attacks, whether stand alone or coordinated attacks, occur at the time and choosing of the adversary. They are inherently stealthy and can be used at critical periods such as when U.S. forces deploy, take actions, a critical point in a war, retaliation for trials, prosecutions, sentencing, or for specific events. Terror attacks are often randomly timed and sporadically targeted in order to maximize the aspect of surprise. Cyber attacks have the same characteristics.

Coordinated/compound attack

> *What I fear is the combination of a cyber attack coordinated with more traditional terrorism, undermining our ability to respond to an attack when lives are in danger.*
>
> *Representative Jane Harman, Democrat, California*
> *House Intelligence Committee Panel on Terrorism and Homeland Security*

It is likely that cyber attacks will accompany physical attacks to enhance the impact and reduce our response capabilities. Complimenting physical attacks with cyber attacks magnify their impact and limit first responders and assistance. This type of attack could serve as a force multiplier for the terrorists. Initial destruction followed by limited timely response capability could significantly magnify the end effect of the attacks.

Al Qaeda's use of cyber world

Today, Al Qaeda is America's number one terrorist adversary. Would terrorists actually use the cyber world? Is this a realistic concern? Let's take a closer look at how Al Qaeda has used cyber technology thus far. Al Jazeera reported that senior aides to bin Laden described the instructions for the 9/11 attacks were transmitted to Mohammed Atta via encoded E-mail. [10] Many Al Qaeda supporters and sympathizers are establishing Web sites (alneda.com, jehad.net, aloswa.org) to show their support for bin Laden. These extremists have found shelter on the Internet. [11] Sites such as 7hj.7hj.com teach surfers the art of computer attack and trains hacking skills to serve Islam. This has global appeal to young Muslims who can enter the fight without traveling to Afghanistan and risking their lives in service to the cause.

Al Qaeda terrorists are using the Internet to research infrastructure information on American water and wastewater systems. The FBI released bulletins that said, "U.S. law enforcement and intelligence agencies have received indications that Al Qaeda members have sought information on Supervisory Control And Data Acquisition (SCADA) systems available on multiple SCADA-related Web sites." SCADA systems allow utility companies to monitor and direct equipment at unmanned facilities from a central location. [12] Computers of bin Laden associates were found to include structural engineering data and programs related to dams and other water retaining structures. Other infrastructure related information, available on the Internet, is being accessed from sites around the world. [13] Lamar Smith, Representative from Texas, said that Congress has been briefed on Al Qaeda operatives probing the electronic infrastructure in search of ways to disrupt or disable power, phones, and water supplies. They are especially interested electrical systems in California. [14] Researching SCADA systems demonstrates a high level of sophistication.

Ramzi Yousef, the original World Trade Center bomber, stored detailed plans to destroy American airliners on encrypted files on his laptop computer. [15] Terrorist groups are also using the Internet to recruit like-minded people to their cause. A recent term has emerged called "hacktivists" which includes cyber protests, floods, DoS, and hacks for a political cause. We have seen a rise in actions taken immediately following real-world events. We saw several new viruses and Web server attacks following 9/11. These included the W32.Nimda.A@mm virus and the attacks of Iranian and Taliban Web sites. [16] Khalid Ibrahim is a member of a Pakistani terrorist group (Harkat-Ul-Ansar) and a bin Laden supporter. He is known to use death threats and social engineering to gain information on how to hack U.S. Military networks. He sent certified checks in the mail to potential informants within the US. He is seeking retaliation on U.S. strikes against Al Qaeda.

Al Qaeda has not been known to use cyber attacks in the past. However, bin Laden has suggested that he has the expertise to use the computer as a weapon. Bin Laden was quoted by the Ausaf newspaper after the 9/11 attacks, "hundreds of young men had pledged to him that they were ready to die and that hundreds of Muslim scientists were with him and who would use their knowledge in chemistry, biology and ranging from computers to electronics against the infidels." This statement implies bin Laden is threatening computer attacks against America. [17]

The CIA is already alert to the possibility of cyber warfare by Al Qaeda and describes this group as becoming "more adept at using the Internet and computer technologies." Al Qaeda are believed to be developing cyberterrorism plans. [18] The Washington Post and CBS news have reported that Al Qaeda prisoners have informed interrogators about their intent to use cyber attack tools. Captives said Al Qaeda is on the threshold of using the Internet as a direct instrument of bloodshed. It is a question of when, not if. [19]

Damage/death via a cyber attack

A terrorist must go beyond Web page defacements, simple hacks, or pranks and "attack people." In order to gain the publicity for his cause that he seeks, he must cause widespread damage, destruction, and death.

In 1998, a 12-year-old hacker broke into the SCADA computer systems that run the Arizona's Roosevelt Dam. Federal authorities said he had complete control of the dam's massive floodgates. This dam holds back as much as 489 trillion gallons of water. He could have totally flooded the cities of Mesa and Tempe which have a combined population of nearly a million people. [20] Had the floodgates been opened, lives would have surely been lost. There are an estimated three million SCADA devices in use today.

Hackers affiliated with Al Qaeda are conducting suspicious surveillance of nuclear power plants, dams, and other critical infrastructures. Information about SCADA devices and hacking them were found on Al Qaeda computers seized in raids in Afghanistan. Al Qaeda prisoners have informed interrogators about their intent to use these methods to attack the U.S. to cause death and destruction. [21] If a terrorist group gained access to one of these critical infrastructure systems, it would not take a lot of imagination to develop a plan that could cause widespread damage and death. Examples include: opening flood gates on a dam, closing down a city's electrical grid, switching a passenger train to collide with a freight train, or turning off an air traffic control system during a winter storm. Given that this could be a successful strategy, do terrorists have the capabilities to carry out these type plans?

Terrorist capabilities assessed

How do we measure if a terrorist or terror group is capable? There is an accepted model within DoD that assesses threat based on several factors: existence, capabilities, intentions, history, and targeting. This model can be applied to the Al Qaeda to gain some insight on their assessed cyber threat.

This threat-analysis methodology is used by the Defense Intelligence Agency (DIA), the Joint Staff, and the unified and specified commands for assessing the level of threat. [22]

Let's take a closer look at Al Qaeda using the above assessment model and its five factors.

1. **Existence—Yes**
   A terrorist group is present, assessed to be present, or able to gain access to a given locale.

2. **Capabilities—Yes**
   The acquired, assessed, or demonstrated level of capability to conduct terrorist attacks.

3. **Intentions—Yes**
   Recent demonstrated anti-U.S. terrorist activity or stated and/or assessed intent to conduct such activity.

4. **History—Yes** for reconnaissance,
   No—For demonstrated cyberterrorist activity.

5. **Targeting—Yes**
   Current credible information on activity indicative of preparations for specific terrorist operations and/or specific intelligence that shows an attack is imminent.

Therefore, the overall assessment of the Al Qaeda cyber threat is—Severe.

A June 2002 survey of technology industry experts revealed that 74 percent thought it was nearly certain that there will be a cyber attack against America within one year. Fifty-nine percent said they expect a major cyber attack against the Federal Government within one year. These dramatic findings prompted a call for the creation of a Cyber Security Agency within the proposed Homeland Security Department. [23] Bin Laden has threatened the use of cyber attack but there is no documented history of

Explanation of Factors

Factor 1: Existence—A terrorist group is present, assessed to be present, or able to gain access to a given locale.

Factor 2: Capability—The acquired, assessed, or demonstrated level of capability to conduct terrorist attacks.

Factor 3: Intentions—Recent demonstrated anti-U.S. terrorist activity or stated and/or assessed intent to conduct such activity.

Factor 4: History—Demonstrated terrorist activity over time.

Factor 5: Targeting—Current credible information on activity indicative of preparations for specific terrorist operations and/or specific intelligence that shows an attack is imminent.

Threat Levels	
Severe	Factors 1, 2, and 5 are present. Factors 3 or 4 may be present.
High	Factors 1, 2, 3, and 4 are present.
Elevated	Factors 1, 2, and 4 are present.
Guarded	Factors 1 and 2 are present. Factor 4 may be present.
Low	Factors 1 and/or 2 may be present.

Figure 7. Threat level determination

Al Qaeda cyber attacks. However, with his vast finances, he certainly could develop or hire out this capability.

A February 2002 CIA Directorate of Intelligence Memorandum said Al Qaeda had "far more interest" in cyberterrorism than previously believed and contemplated the use of hacker for hire to speed the acquisition of capabilities. [24]

In order to successfully understand the world of cyberterrorism, we must study its components and analyze the who, what, how, where, why, and when questions. As a new dimension of warfare, the cyber environment must be thoroughly studied and analyzed. Hopefully, my cyberterrorism model contributes to this new body of knowledge.

The latest U.S. National Security Strategy document focuses on defeating global terrorism, preventing our enemies from threatening us, and denying new sanctuaries. The bulk of this document addresses the physical world; however, most of its major tenets and ideas apply to the cyber world as well. The cyber world is such a new "dimension" of national security that our policy and doctrine will take time to catch up to the possibilities of the technologies. Until that time, cyber space will remain much like the old wild west where the strong survive and rules are sporadically enforced, criminals run amuck and the rules of engagement continue to evolve.

> *Cyber space is essential to both homeland security and national security; its security and reliability support the economy, critical infrastructures, and national defense. [25]*

The strategy describes initiatives to secure U.S. information systems against deliberate and malicious disruption.

The national strategy definitely considers a cyberterrorist attack as a viable reality.

> *Though the U.S. possesses both the world's strongest military and largest national economy, these two aspects of the nation's power increasingly rely upon certain critical infrastructures, which include cyber-based information systems. As witnessed on 9/11, enemies of the U.S. (nations, groups, and indeed, even individuals) are prepared to strike in unconventional ways. These adversaries have explicitly stated the intention, not only to strike at U.S. citizens, but to attack the nation's infrastructures and cyber space—the pillars of the economy. [26]*

The President is expected to sign the National Strategy to Secure Cyberspace within a few months. The draft document calls for the development of a clear roadmap to protect critical infrastructures. The document states—

> *Cyber space is essential to both homeland security and national security; its security and reliability support the economy, critical infrastructure, and national defense…*

The events of 9/11 caught us by surprise. We cannot afford to disregard the cyber threat and be caught by surprise by a major cyber assault. Unless we take the appropriate steps to protect ourselves against cyber attacks now, America will surely suffer tragic cyberterrorist attacks that will include loss of life.

There are several key recommendations to improve the current U.S. cyber security posture—

- Accept cyberterrorism as a viable near-term threat
- Organize for success and establish the new Department of Homeland Security and its new Cyber/Infrastructure Division
- Debate the issues with Congress and the public to raise awareness
- Increase punishment for cyber crimes with terror or death as a motive

- Finalize the national cyber security plan and implement it
- Conduct Inter-Agency Cyber Exercises
- Commit Congressional funding to improve cyber security
- Commit manpower and training to implement the plan effectively

We must prepare for an inevitable and perhaps imminent cyberterrorist attack. It took a tragic event on 9/11 to improve the nation's physical security strategy. We should not wait for a similar cyber tragedy before we take action to improve our security. We know terrorists are pursuing this capability. Major cyberterror attacks against America will occur. It is a matter of when, not if. ■

About the Author

Col (Select) Bradley K. Ashley

Colonel (Select) Bradley K. Ashley has been selected to be the Deputy Group Commander at the 5th Combat Communications Group, Robins AFB, Georgia. Prior to this assignment, he was a student at the Air War College, Maxwell AFB, Alabama and more previously, was the Commander, 30th Communications Squadron (CS), Vandenberg AFB, California.

The 30th CS is the largest and most technically diverse unit of its kind in DoD, providing communications, computer, network, visual information (VI), and information management (IM) systems for the 30th Space Wing, Western Range (WR), and 47 tenants. He also served as the Senior Information Operations (IO) Policy and Doctrine Officer, Joint Staff, C4 Systems Directorate (J6), Washington D.C. In that position, he advised the Chairman, Joint Chiefs of Staff, and senior members of the Joint Staff, on issues related to information vulnerabilities to U.S. strategic systems.

Colonel (Select) Ashley enlisted in the U.S. Air Force in 1979 and served as an avionics technician. He completed Reserve Officer Training Corps at the University of Georgia in 1985. He has served in a wide variety of assignments including Base level, Major Command Headquarters, Squadron Commander, Air Staff and the Joint Staff. Key prior assignments included the Chief, Tactical Warning/Attack Assessment (TW/AA) Aerospace Defense Requirements and Program Element Monitor (PEM) for Cheyenne Mountain Upgrade, Deputy Chief of Staff for Plans and Operations (XO), Headquarters U.S. Air Force, Pentagon, Washington, D.C. He is a career communications and computer officer.

References

1. "National Strategy to Secure Cyberspace," Draft, September 2002
2. "Polymorphic Macro Viruses, Part One" at http://www.online.securityfocus.com/infocus/1635, October 23, 2002.
3. "Polymorphic Macro Viruses, Part Two" at http://www.online.securityfocus.com/infocus/1638, November 5, 2002.
4. "Cyber-Attacks by Al Qaeda Feared" at http://www.washingtonpost.com/ac2/wp-dyn/A50765-2002Jun26?start=48&per=16, October 30, 2002.
5. "Cyber Terror—Potential for Mass Effect" at http://www.iac.dtic.mil/iatac, Winter 01/02.
6. "Is Cyber Terror Next?" at http://www.ssrc.org/sept11/essays/denning_text_only.htm, October 30, 2002.
7. "Is a Larger Net Attack on the Way?" at http://www.msnbc.com/news/827209.asp?cp1=1, November 1, 2002.
8. "Cyberspace Full of Terror Targets" at http://www.usatoday.com/life/cyber/tech/2002/05/06/cyberterror.htm, September 11, 2002.
9. "President's Commission on Critical Infrastructure Protection", Appendix A, Sector Summary Reports.
10. "Cyber News, Virtual Soldiers in a Holy War" at http://www.ds-osac.org/edb/cyber/news/story.cfm?KEY-9026, September 27, 2002.
11. Ibid.
12. "FBI Issues Water Supply Cyberterror Warning" at http://www.online.securityfocus.com/news319, September 30, 2002.
13. Ibid.
14. "Al Qaeda Cyber Alarm Sounded" at http://www.fcw.com/fcw/articles/2002/0722/web-attack-07-25-02.asp, September 11, 2002.
15. "Cyber-terrorists Wield Weapons of Mass Disruption" at http://www.news.bbc.co.uk/1/hi/sci/tech/specials/washington_2000/648429.stm, September 11, 2002.
16. "Malicious Internet Activity Increases Following 11 September Attacks" at http://www.janes.com/security/international_security/news/jir/jir010925_1_jir010925_1_n.shtml, September 25, 2001.
17. "Report Warns of Al-Qaeda's Potential Cybercapabilities" at http://www.infowar.com/class3/02/class3010902aj.shtml, September 11, 2002.
18. CIA Identifies Cyber Terror Groups" at http://www.vnunet.com/news/1136404, October 30, 2002.
19. "Use of Web in Terror Attack Feared" at http://www.cbsnews.com/stories/2002/06/27/attack/main513582.shtml, September 11, 2002.
20. "Cyber-Attacks by Al Qaeda Feared" at http://www.washingtonpost.com/ac2/wp-dyn/A50765-2002Jun26?start=24&per=24, October 30, 2002.
21. US Fears Nuclear Cyber Terror Attacks, Nick Farrell, June 27, 2002.
22. "Intelligence, Counterintelligence, and Threat Analysis" at http://www.adtdl.army.mil/cgi-bin/atdl.dll/fm/3-19.30/appc.htm, October 23, 2002.
23. "Al Qaeda Cyber Alarm Sounded" at http://www.fcw.com/fcw/articles/2002/0722/web-attack--7-25-02.asp, September 11, 2002.
24. "Cyber-Attacks by Al Qaeda Feared" at http://www.washingtonpost.com/ac2/wp-dyn/A50765-2002Jun26?start=24&per=24, October 30, 2002.
25. "National Security Strategy to Secure Cyberspace," Draft, September 2002.
26. Ibid, pg 7.

Bibliography

AntiOnline, "Interview with Makaveli" at http://www.antionline.com, March 2, 1998.

Campen, Alan D., Col, USAF, "Information War Techniques Supersede Kinetic Weapons", SIGNAL, May 1998, pg 33-36.

Computer Security, Issues & Trends, Vol. IV, No.1, Winter 1998, Computer Security Institute, p. 1.

Defense Science Board Report, "Task Force on Information Warfare-Defense (IW-D)" at http://www.jya.com/iwd.htm, November 1996.

Denning, Dorothy, “Is Cyber Terror Next?” at http://www.ssrc.org/sept11/essays/denning_text_only.htm, October 30, 2002.

Department of Defense Directive S-3600.1, Information Operations, Washington, GPO, December 9, 1996.

Department of Defense News Briefing, OSD/PA Press Release, February 25, 1998.

GAO Report, ”Information Security: Computer Attacks at Department of Defense Pose Increasing Risks” at http://www.fas.org.irp/gao/aim96084.htm, May 22, 1996.

Glave, James, “Analyzer Nabbed in Israel?,” Wired News, March 16, 1998.

Glave, James, “DoD Cracking Team Used Common Bug,” Wired News, March 5, 1998.

Graham, Bradley, “11 U.S. Military Computer Systems Breached by Hackers This Month,” Washington Post, February 26, 1998, page 1.

Lardner, Richard and Pamela Hess, “Pentagon Looks for Answers to Massive Computer Attack,” Defense Information and Electronics Report, February 13, 1998.

Overholt, Matt, “Overview of Cyber-Terrorism” at http://www.cybercrimes.net/terrorism/overview/page1.htm, September 12, 2002.

Prepared Testimony of Jim Christy, AF Investigator before the Senate Government Affairs Committee Permanent Investigations Sub-Committee, June 5, 1996.

President’s Commission on Critical Infrastructure Protection Report, “Critical Foundations, Protecting America’s Infrastructures,” October 1997.

Reed, Dan, “Pentagon Hacker Suspect Tells of Plans for Retaliation”, San Jose Mercury News, March 3, 1998.

Szappanos, Gabor, “Polymorphic Macro Viruses, Part Two” at http://www.online.securityfocus.com/iforuc/1638, November 5, 2002.

United States Department of Army Memorandum. FORSCOM Network Security Improvement Program (NSIP) Action Plan (Draft), pg. 7.

United States Joint Chiefs of Staff, CJCS Instruction 6510.01B, Defensive Information Operations Implementation, Washington, GPO, June 30, 1997.

United States Joint Chiefs of Staff, Concept for Future Joint Operations, Expanding Joint Vision 2010, Washington, GPO, May 1997.

United States Joint Chiefs of Staff, JCS Pub 3-13, Joint Doctrine for Information Operations, January 28, 1998, page I-22 and GL-14.

United States Joint Chiefs of Staff, Joint Vision 2010, Washington, GPO, 1996.

United States Joint Chiefs of Staff, J39, Information Operations Division Briefing, IA-The Way Ahead, March 1998.

United States Joint Chiefs of Staff, J6K, Information Assurance Division Briefing, Rome Labs Case, November 1997.

Van Derbeken, Jason and Jim Doyle and Glen Martin, “Hacking Suspect Caught in Cloverdale”, San Francisco Chronicle, February 27, 1998.

…continued from page 7

and the impact of the Patriot Act in aiding law enforcement and counterintelligence activities related to CND. The 33rd Information Operations Squadron (IOS), Air Force Computer Emergency Response Team (AFCERT) presented an overview of the AFCERT. Highlighted was the speed of which the sensors can detect an incident and alert an incident handler to react. The AFCERT noted that information sharing of CND does not only occur at the higher levels (ASD, JTF–CNO) but also at the Service CERT levels. JFCOM presented information on Content Base Information Security (CBIS), which would allow information sharing between U.S./NATO and Coalition partners on one network. The afternoon session involved separating into different forums for discussions pertaining to senior management, operations, knowledge management, and technical issues.

Day three

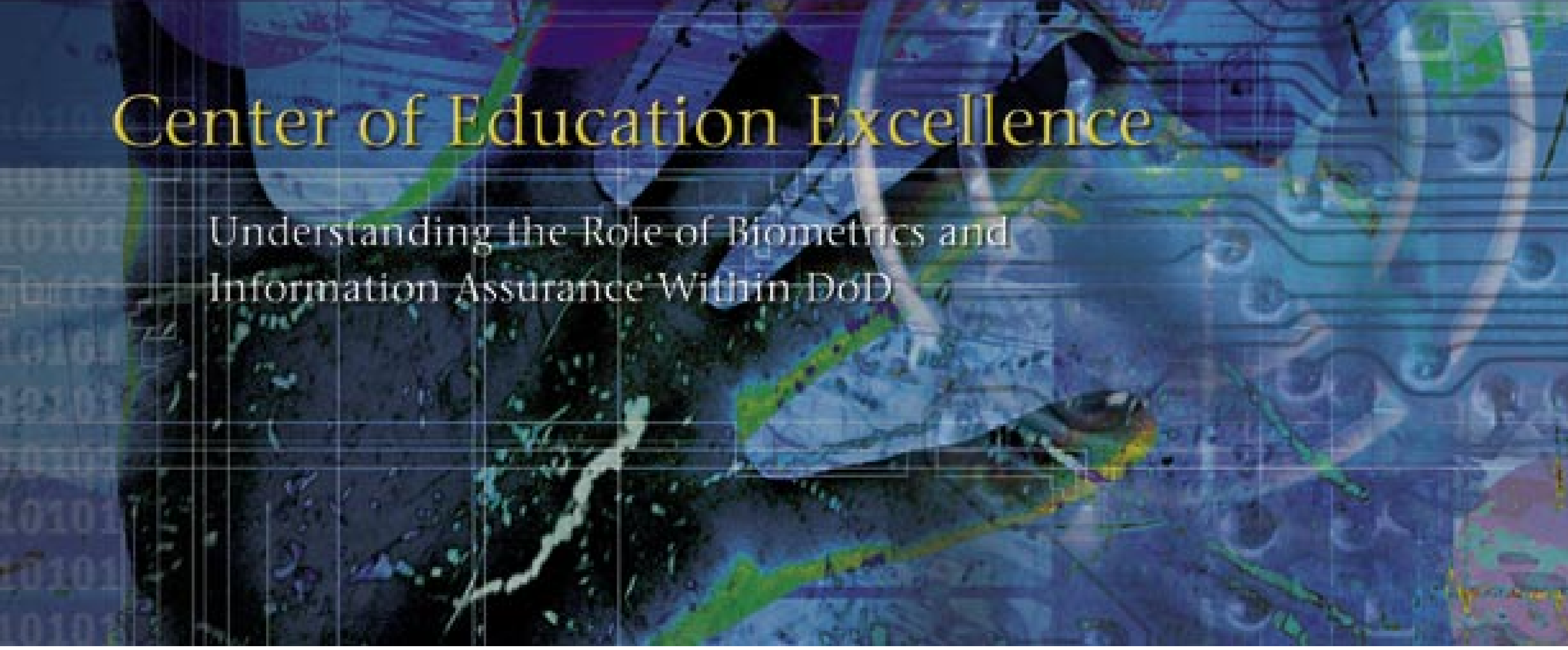
Mr. Erroll Schwartz discussed defending DoD networks from cyber attacks. The Defence INFOSEC Product Co-Operation Group (DIPCOG) UK presented a briefing on INFOSEC within COTS applications. The briefing was an overview of the DIPCOG and the approval process for COTS products. Other briefings presented included an IATAC overview, Information Security in a Modern Combined Air Operations Center (CAOC), and Open Source IDS Programs. Group forums met during the afternoon and gave a back brief of items discussed in the forums. As the conference drew to a close, the following were identified as milestone objectives for 2003—

- Draft standard operating procedure (SOP) inputs no later than the end of January 2003
- Ratify SOP at March International Coordination Cooperation Working Group (ICCWG)
- Exercise SOPs during JWID as required (June 2003)
- Conduct distributed ICCWG CND demonstration (September 2003)
- 5-Eyes CND Operational IOC (December 2003)

About the Author

James Peña

James Peña is a research analyst at the Information Assurance Technology Analysis Center (IATAC). Mr. Peña served in the Military for over 15 year with the U.S. Marines, U.S. Army, and U.S. Army Reserves. He has served in both the conventional and special operations units as a signals intelligence/electronic warfare operator. Mr. Peña has worked at the Joint Task Force Computer Network Defense (JTF–CND) and later in the Joint Task Force Computer Network Operations (JTF–CNO) in the J2, J3, and J5 directorates. Mr. Peña is currently pursuing a B.S. Degree in Computer Information Systems at Strayer University. He may be reached at iatac@dtic.mil.



Center of Education Excellence

Understanding the Role of Biometrics and Information Assurance Within DoD

by Walter McCollum, Ph.D.

Information assurance (IA) has long been a priority for the U.S. Department of Defense (DoD), and biometrics are playing an increasingly important role in protecting our country's assets. A vital security enabler, biometrics can be used in conjunction with, or in lieu of, passwords, personal identification numbers (PINs), and other tokens to add an additional layer of information or physical security by establishing positive access control to information and facilities. While DoD Agencies and Services look forward to enterprise-wide biometric implementation, they're taking a deliberate, conservative approach to ensure successful adoption. Meanwhile, educating these Agencies and Services on biometrics will go a long way in achieving this goal.

The DoD Biometrics Management Office (BMO), a member of the West Virginia University (WVU) Center for Identification Technology Research (CITeR), has partnered with WVU to educate government and information technology (IT) industry personnel in biometrics and IA. Spanning from basic principles to advanced technology integration, this joint venture has developed several different options for the beginner to advanced scholar in biometrics and IA.

Concepts in Biometrics Systems and Information Assurance 5-Day Short Course

The objective of the Concepts in Biometric Systems and IA 5-Day Short Course (5DSC) is to present an introduction to the principles of operation, design, testing, and implementation of biometric systems and the legal, social, and ethical concerns with their use. In addition, this will provide an overarching DoD biometrics educational framework that will be utilized to institutionalize biometrics education throughout the Services and Agencies. This is designed to be either the first course in the IAB Graduate Certificate Program (which will be brought up later in this article), or as a standalone professional development course for use by anyone in the DoD.

The 5DSC has been offered in various locations to include West Virginia, Northern Virginia, and California, and is becoming more popular as major commands are now showing interest and requesting the course. As a result, WVU's mobile training team will be taking the course to United States Pacific Command (USPACOM) in Hawaii this May.

Graduate Certificate Program

The Graduate Certificate program was designed to be a precursor for university students to enter into the Masters program with a concentration in IA and biometrics. It consists of 5 graduate level courses (15 credit hours) with the 5DSC as the first course. The goal of the program is to provide students with the following—

- A solid understanding of biometrics technology, system security principles, and their scientific foundations.
- An awareness of the social, psychological, ethical, and legal policies and requirements in the field of IA and biometrics.
- The ability to communicate with professionals in the wide range of public services, including law enforcement, military, science and who employ the principles and techniques of IA and biometrics.

Masters Program

The Masters Degree programs with emphasis in biometric and IA offered through WVU's Lane Department of Computer Science and Electrical Engineering will have three separate possible degree paths. Those degrees are—

- Master of Science in Computer Science with concentration in biometrics and IA
- Master of Science in Electrical Engineering with concentration in biometrics and IA
- Master of Science in Software Engineering with concentration in biometrics and IA

By using these three separate degree paths, WVU is able to offer the concentration in biometrics and IA to students with a variety of backgrounds and experience. For those with an undergraduate degree in computer science, the Master of Science in Computer Science degree is recommended. Those with an Electrical Engineering or Computer Engineering undergraduate degree would be best suited for the Master of Science in Electrical Engineering. Lastly, those candidates with and undergraduate degree in other disciplines and having a minimum of three years software development experience will be best served by the Master of Science in Software Engineering through a non-traditional student approach.

This diversity in the approach to graduate education in biometrics and IA allows the Department to service the needs of a broad range of DoD personnel and contractors.

Additional BMO Education Initiatives

Collaborating with the 36 Centers of Academic Excellence in Information Assurance, the BMO is providing insight to the value of integrating biometrics into the Center's IA curricula. To date, among the universities expressing interest in the integration include—

- George Washington University
- Idaho State University
- Iowa State
- Purdue University
- U.S. Air Force Institute of Technology
- U.S. Military Academy, West Point
- University of Idaho
- University of Texas, San Antonio
- University of Tulsa

The BMO initiative also oversees the Student Education Employment Program (SEEP) at the Biometrics Fusion Center (BFC), West Virginia. A program provided by the Office of Personnel Management (OPM) through an agreement between the BFC and WVU, SEEP provides Federal employment opportunities to students who are enrolled or accepted for enrollment as degree-seeking students taking at least a half-time academic, technical, or vocational course load in an accredited high school, technical, vocational, 2- or 4-year college or university, graduate or professional school.

The program is comprised of two components—the Student Temporary Employment Program (STEP) and the Student Career Experience Program (SCEP). STEP provides maximum flexibility to both students and managers because the nature of the work does not have to be related to the student's academic or career goals. However, SCEP provides work experience, which directly related to the student's academic program and career goals. Students in SCEP may be non-competitively converted to term, career, or career-conditional appointments following completion of their academic and work experience requirements.

The BMO is investigating the opportunity to integrate the 5DSC into computer-based training (CBT) within the next 12 months. The benefits of the integration presents a course delivered by CD–ROM where personnel can choose when and where to take the course. A CBT program can also be repeated until the student understands the material, or the student can cover the material once and proceed to the next topic. The BMO and WVU are also considering instituting a 3-Day Short Course—in lieu of the 5DSC—serving as a professional development course for DoD personnel who may not be interested in obtaining the IAB Graduate Certificate.

The BMO Education Program is currently marketed through various mediums across DoD. For information on Biometric Courses offered through the Biometric Management Office, please visit the U.S. Army On-line Catalog at: http://cpol.army.mil/train/catalog/toc.html. All Defense Agencies and U.S. Armed Services are encouraged to take advantage of the biometric educational opportunities. ■

About the Author

Walter R. McCollum, Ph.D.

Dr. McCollum oversees the Biometric Education Program in the Department of Defense Biometric Management Office. Dr. McCollum has over 15 years experience in instructional technology and is currently an adjunct professor at the University of Phoenix School of Management's Graduate and Undergraduate Programs. He earned his B.S. in Psychology from the University of the State of New York, Albany; his M.A. in Management from Webster University; and his Ph.D. in Applied Management and Decision Sciences with a specialization in Organizational Change and Leadership from Walden University. Dr. McCollum also served thirteen years in the U.S. Air Force in Information Management and Communication Air Force Specialties.

product order form

Instructions: All IATAC **LIMITED DISTRIBUTION** reports are distributed through DTIC. If you are not a registered DTIC user, you must do so **prior** to ordering any IATAC products (unless you are DoD or Government personnel). **To register On-line: http://www.dtic.mil/dtic/regprocess.html**.
The *IAnewsletter* is **UNLIMITED DISTRIBUTION** and may be requested directly from IATAC.

Name ________________________________

Organization ________________________________

Address ________________________________

____

____

DTIC User Code ________________________________

Ofc. Symbol ________________________________

Phone ________________________________

E-mail ________________________________

Fax ________________________________

Please check one: □ USA □ Industry □ USMC □ University □ UN □ DoD □ USAF □ Gov't □ Command □ Other

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

____

LIMITED DISTRIBUTION

IA Collection Acquisitions CD–ROM

□ Summer 2002 ed.

IA Tools Reports (softcopy only)

□ Firewalls (3rd ed.) □ Intrusion Detection (3rd ed.) □ Vulnerability Analysis (2nd ed.)

Critical Review and Technology Assessment (CR/TA) Reports

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

State-of-the-Art Reports (SOARs)

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

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

UNLIMITED DISTRIBUTION

Hardcopy *IAnewsletters* available

Volumes 4 □ No. 2 □ No. 3 □ No. 4

Volumes 5 □ No. 1 □ No. 2 □ No. 3 □ No. 4

Softcopy *IAnewsletters* back issues are available for download at http://iac.dtic.mil/iatac/news_events/ia_newsletter.htm

Fax completed form to IATAC at 703/289-5467

April

FSI's 18th Annual Federal Outlook Conference

April 2, 2003
McLean Hilton, Tysons Corner, VA
http://www.fedsources.com/elements/events/fsievents/con-outlook.asp

FOSE 2003

April 8–10, 2003
Washington Convention Center,
Washington DC
http://fose.rd10.net/r.asp?ZXU=10096&ZXD=6427403&source=E3IJEA

Knowledge Management Conference

April 14–16, 2003
Ronald Reagan Building, Washington, DC
http://www.egov.com/events/2003/km/

Network Centric Operations 2003

April 16–17, 2003
Sheraton Premiere, Tysons Corner, VA
http://register.ndia.org/interview/register.ndia?PID=Brochure&SID=_0V00JGYLQ&MID=3AF3

Fiesta Crow 2003

April 20–23, 2003
Gonzalez Convention Center, San Antonio, TX
http://www.fiestacrow.com

DISCEX III Exposition: The Third DARPA Information Survivability Conference and Exposition

April 22–24, 2003
Hyatt Regency Crystal City, Washington, DC
http://www.iaands.org/discex3/cfp.html

May

InfoSecurity Directors and Managers Symposium

May 6–8, 2003
Boston, MA
http://www.misti.com/northamerica.asp?page=4&disp=sym&region=1&subpage=3

PACOM Conference IA Conference

May 19–23, 2003
Honolulu, HI
http://www.iavents.com

National OPSEC Conference

May 19–23, 2003
Town and Country Resort & Conference
Center, San Diego, CA
http://www.iaevents.com

June

E-Gov Conference

June 9–12, 2003
Washington Convention Center,
Washington DC
http://www.e-gov.com/events/2003/egov/

Government Symposium on Information Sharing and Homeland Security

June 30, 2003
Philadelphia Marriott, Philadelphia, PA
http://www.federalevents.com

IATAC

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

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