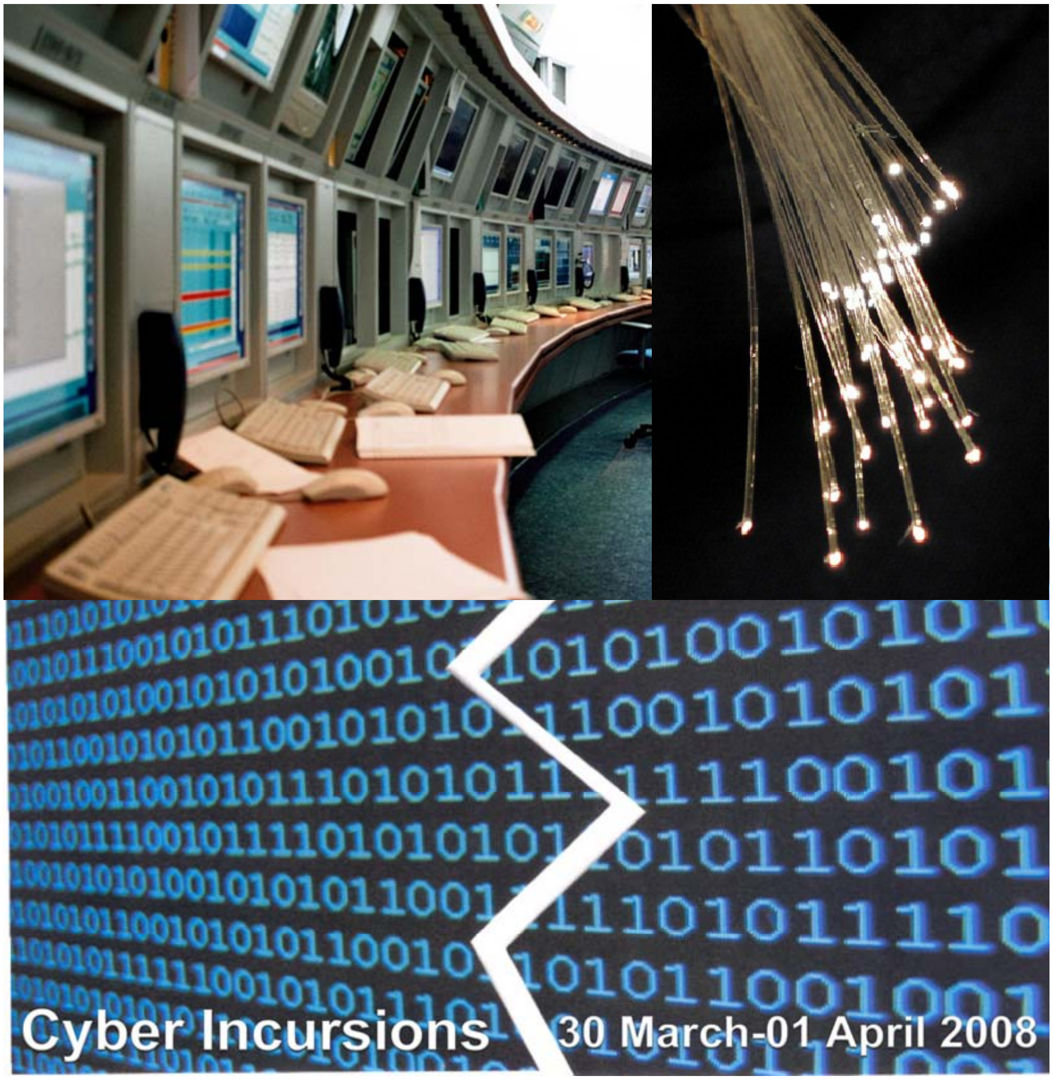
CIAG
Critical Incident Analysis Group



Cyber Incursions 30 March-01 April 2008

CYBER INCURSIONS:

Erosions of Security and Social Trust?

SHAUN WATERMAN
ANITA JONES
GREGORY SAATHOFF

CYBER INCURSIONS:
EROSIONS OF SECURITY AND SOCIAL TRUST?

Critical Incident Analysis Group
Summary, Eleventh Annual Conference
University of Virginia
March 30 – April 1, 2008

University of Virginia, PO Box 800657, Charlottesville, Virginia 22904-4764

Written and Edited by:
Shaun Waterman
Anita Jones
Gregory Saathoff
Sabrina Rissing

Design: Patrick Walsh
Printing: University of Virginia

Cover Photography and page 28 photography available in the Public Domain.
Conference Photography by Jim Carpenter, Gitchell's Studio, Charlottesville, Virginia

CIAG
Critical Incident Analysis Group

The simple truth is we do not protect cyber space to the same degree we protect our physical space.

– ROBERT S. MUELLER

Science fiction does not remain fiction for long.
And certainly not on the internet.
– VINTON CERF

Contents

Robert Mueller, Director of the FBI, speaks to the dinner group at The Rotunda.

Shawn Henry, Deputy Asst. Director of FBI Cyber Division, addresses the panel.

David Kestenbaum, NPR, John Lord Alderdice, Amit Yoran, NetWitness Corp., and James Schlesinger, MITRE Corp., participate in the conference's public session.

Foreward

Remarks Delivered by
Robert S. Mueller, III
Director, Federal Bureau of Investigation
at the Critical Incident Analysis Group
Eleventh Annual Conference
University of Virginia Rotunda
Charlottesville, Virginia
31 March, 2008

Good evening, I am honored to be here.

I want to express my appreciation for the work of the Critical Incident Analysis Group, and its executive director, Greg Saathoff.

Since its first conference in 1998, CIAG's partnership with the FBI has indeed been a fruitful one. We have confronted some of the critical topics of our time — threats to symbols of democracy, bioterrorism, radicalization — and now, cyber threats.

Throughout, the CIAG has been a tremendous support to, and partner with, the FBI, and we are most grateful to you.

As you may know, fighting cyber crime is among the FBI's highest priorities, just after counterterrorism and counterintelligence. Every day, our cyber agents and analysts investigate computer fraud, child exploitation, theft of intellectual property, and worldwide computer intrusions.

Tonight, I want to talk about cyber threats to our national security, and what the FBI is doing to meet those diverse dangers.

I recently watched a video on YouTube about the impact of the Internet. And for anyone here under the age of twenty-five, yes, those of us over a certain age are allowed to access YouTube. According to this video, entitled "Did You Know," the average twenty-one year-old has sent and received more than 250-thousand e-mails and instant messages. More than seventy percent of four-year-olds in the United States have used a computer at least once. And Internet users query Google nearly three billion times every month.

The Internet has become the primary means by which we conduct business, store data, and connect operating systems, from air traffic control to power grids. But that widespread use has also left us vulnerable to attack from hostile foreign powers, hackers, and even terrorists.

The Internet is not only the means by which attacks may be planned and executed; it is also a target in and of itself.

Just imagine a country experiencing a "cyber blockade." Wave after wave of data requests from computers around the world shut down banks and emergency phone lines, gas stations and grocery stores, newspapers and television stations, even the President or Prime Minister's office.

As you may know, this scenario is not the stuff of science fiction. These very events occurred just last April in Estonia. Although the source of this attack has not been confirmed, the effect was real, and left all of us aware of the potential risk we face.

We see this effect on a smaller scale every day. Computer intrusions are becoming more and more commonplace. And studies show that computers in the United States are attacked at a rate ten times that of other countries.

Today, botnets are the weapon of choice. Botnets are considered the Swiss Army knives of cyber crime. You name it, they can do it, from attacking networks, sending spam, and collecting data, to infecting computers and injecting spy ware.

Botnets do not require highly technical skills, yet the national security implications are broad. A botnet could shut down a power grid, flood an emergency call center with millions of spam messages, or disable a military command post. The possibilities are endless, and that is what is makes it so daunting.

Take, for example, an operation we initiated last June called "Bot Roast" (I don't know where we come up with these code names, but it was called "Bot Roast"). Together with the Department of Justice, the Computer Emergency Response Team (CERT) Coordination Center at Carnegie Mellon, private sector companies such as Microsoft, and Internet service providers, we identified more than one million infected computers and shut down several bot-herders, as they are called.

In a second phase of "Bot Roast," cleverly-named "Bot Roast II," completed last November, an individual used botnets to make off with some $20 million dollars as part of a phishing scam.

It is clear that computer intrusions can also have large-scale implications for our economy and our national security. There is no shortage of countries that seek our information technology, our innovation, and our intelligence – information we have spent years and billions of dollars developing.

The simple truth is we do not protect cyber space to the same degree we protect our physical space. We have in large part left the doors open to our business practices, our sensitive data, and our intellectual property.

The espionage game once pitted spy versus spy, country against country. But today, our adversaries sit on fiber optic cables and wi-fi networks. Hackers are using sophisticated techniques to steal sensitive intelligence, scientific research, and communications data. They are difficult to identify and track because they move in and out of international systems at will, and they leave no visible trail.

A member of our cyber team describes it as having an invisible man in the room, standing over your shoulder, seeing and hearing everything you do, watching every word you type. And you may never know he is there, who he represents, or how much damage he has done.

We are concerned not only with loss of data but also with corruption of data. Such manipulation can cause electronic devices to fail and networks to freeze. It can alter critical air temperatures in laboratories and shut down safety systems in nuclear power stations.

There are also those who seek to block access to our own information, for political, financial, or ideological gain. If we lose the Internet, we do not simply lose the ability to email or to surf the web. We lose access to our data. We lose our connectivity. We lose our intellectual property. We lose our security.

And the threat is not limited to hackers on the outside. Insiders present a significant problem. Contractors may take the appropriate security measures, but what about those with whom they subcontract and their subs? And what of those who may take advantage of open access to research and development facilities on campuses such as this?

One case especially underscores this insider threat. In November 2001, a man named Li Sun (Lee Suhn) told FBI agents in Palo Alto that he believed his business partner had stolen trade secrets from his employers.

One week later, Fei Ye (Fay Yeh) and Ming Zhong (Jong) were arrested at the San Francisco airport, just moments before boarding a flight bound for Shanghai. FBI agents and Customs officials seized several hard drives and thousands of proprietary documents and electronic media from two major semiconductor companies.

They found these two men had planned to start a semiconductor company in China, using this proprietary information. They had requested funding from a Chinese government program dedicated to acquiring and developing science and technology. They had received more than two million dollars in start-up funds, from city and provincial Chinese government agencies.

In December 2006, these two pled guilty to economic espionage to benefit a foreign country. Each faces up to thirty years in prison.

The intersection between cyber crime and terrorism is also becoming increasingly evident. We know terrorist organizations have the interest and intent to attack American cyber networks. And there are thousands of extremist websites, comprising everything from propaganda to blogs.

In the past six years, al Qaeda's online presence has become pervasive. For terrorists, the Internet has become a marketing tool, a moneymaker, a training ground, and a virtual town square, all in one.

In July of 2007, three men in Britain were the first to be sentenced to prison for using the Internet to incite terrorism. One of these men, Younis Tsouli, went by the moniker "Irhabi Double Oh Seven" – which translates in Arabic to "Terrorist Double Oh Seven." He was a loner living in a London basement apartment with no previous connection to al Qaeda, yet he became a key part of its propaganda campaign.

Tsouli posted thousands of files online, from videos of beheadings to detailed instructions for building car bombs. He hacked into servers around the world to gain additional bandwidth.

But he did more than merely act as an al Qaeda webmaster. He was a hub of communication between terrorist plotters in Canada, Denmark, Bosnia, and the United States.

He and his colleagues stole thousands of credit card accounts through phishing schemes. They ran up charges of more than $3 million dollars for items they thought fellow extremists might need, from night vision goggles to GPS devices. And they laundered money through more than a dozen Internet gambling sites.

At the time of his arrest, Tsouli was just a twenty-two year-old student. Today, he is a guest of Belmarsh Prison in the U.K. But he is hardly the end of the line; many more cyber-savvy extremists hope to carry on where he left off.

The FBI has the authority to handle these varied threats from start to finish. We have cyber squads in each of our fifty-six field offices across the country. These agents, intelligence analysts, and computer experts mesh technological expertise with investigative experience. They run complex undercover operations to catch computer hackers and child predators the world over.

They also investigate threats to both companies and consumers. And they teach their law enforcement counterparts – at home and abroad – how to work cyber investigations.

Our capabilities are strong, but they rely on key partnerships with other federal agencies, law enforcement, private industry, and academia – indeed, many of you here tonight.

But we do not limit our operations to the United States. Increasingly, cyber threats originate outside of our borders. And as more people around the world gain access to computer technology, new dangers will surface. For this reason, global cooperation is vital.

To that end, we have sixty-one Legal Attaché offices around the world. We are working with our partners in Romania, Russia, Poland, Hungary, Italy, and Estonia, amongst others, to investigate international cyber threats.

Just last month, cyber agents arrested more than one hundred individuals across the globe who had been trading and distributing roughly 400,000 files of child pornographic material over a period of some fifteen years. These individuals used sophisticated encryption technology to elude detection. We worked with our counterparts in Australia, Germany, and the United Kingdom to bring these individuals to justice.

We also understand that we must continue to work closely with all of you – members of the private sector and the academic community.

Through the FBI's InfraGard program, members from a host of industries – from computer security to the chemical sector – share information about threats to their own companies and communities through a secure computer server.

To date, there are nearly 24,000 members of InfraGard — individuals from Fortune 500 companies to small businesses.

We are also reaching out to academia by way of the National Security Higher Education Advisory Board.

The Board provides a forum to discuss issues that affect not just the academic community but the country, considering issues such as campus security, counterterrorism, espionage, and cyber crime. This Board allows university presidents and chancellors from across the country to share their concerns and their collective expertise.

There is an old saying that all roads lead to Rome. In the days of the Roman Empire, roads radiated out from the capital city, spanning more than 52-thousand miles. The Romans built these roads to access the vast areas they had conquered. But, in the end, these same roads led to Rome's downfall for they allowed the invaders to march right up to the city gates.

The Internet has opened up thousands of new roads for each of us – new ideas and information, new sights and sounds, new people and places. But the invaders – those whose intent is not enlightenment but exploitation and extremism – are marching right down those same roads to attack us in many ways.

We have a much greater chance of staying safe if we stand together. We must continue to safeguard our systems and our data. We must continue to share intelligence. Most importantly, we must continue to stay connected.

The enemies, as they say, are at the gates, and we must rely on our agility, our resourcefulness, and our resolve to stop them, together.

Thank you again for having me here tonight and God bless.

CIAG
CIAG
James Schlesinger

Introduction

Society now depends upon the Internet as a communications infrastructure. But, it is routinely a conduit for attacks on individuals, corporations, and governments. Managers of other infrastructures, such as rail systems, water delivery systems, electrical grid, phone communications, air traffic controls, 911-emergency help, and road traffic control systems, are all held to a standard of safety and reliability. Users should be assisted, not threatened, by their infrastructures. It is for this reason that the Critical Incident Analysis Group (CIAG) chose cyber incursions as the topic for its 2008 Annual Meeting at the University of Virginia from 30 March to 1 April.

This document discusses the key themes of discussion from the meeting. It is organized topically, rather than chronologically, as discussants returned to key issues repeatedly. This summary is organized into four parts: *Part One: Framing the Problem of Cyber Incursions* sets the context for the following sections; *Part Two: Case Studies of Cyber Incursions* discusses three case studies (Europe, Middle East, and Asia) of recent major cyber incursions; *Part Three: Uncharted Territory* summarizes selected issues raised in the plenary discussions; and *Part Four: Some Ways Forward* describes some of the observations from the conference and presents a list of recommendations for the government, the private sector, and academe. These recommendations were not voted on and consensus around them was not achieved at the meeting. We simply offer them for consideration.

Due to the sensitivity and universal applicability of the incursions discusses in these case studies, this document is deliberately non-specific in regards to certain significant and detailed matters. In general, these matters would only add color to the issues; nowhere has this non-specificity prevented a lucid account of major issues.

Although we do not attribute specific comments to individuals, we have used direct quotations where a particular phrase was delivered with eloquence and authority. Those who were present will likely remember to whom the credit is due for these quotations.

This document represents an attempt to provide a timely summary of the key issues discussed at the conference. It presents a synthesis of the multidisciplinary discussions of an international group of professionals from business, academe, and government. Their expertise ranged from medicine and behavioral sciences to justice and law enforcement to cyber security as viewed from an international, homeland, corporate, and research perspective.

John O. Marsh, Jr., Secretary of the Army (1981-1989), provides lunchtime remarks.

Anita Jones, Prof. of Engineering and Applied Science at UVa, and Bill Wulf, former President of the National Academy of Engineering, speak with Marge Sidebottom, Director of the UVa Office of Emergency Preparedness.

Chuck Robb, Prof. of Law and Public Policy at George Mason University, offers his comments while George Terwilliger, senior partner with White & Case LLP, listens.

Technology... is a queer thing. It brings you great gifts with one hand,
and it stabs you in the back with the other.
– C.P. SNOW

I

Framing the Problem of Cyber Incursions

"Smoking keyboards are harder to find than smoking guns."

Cyber incursions are a problem that is directly related to the degree to which an individual, organization, or the global community depends upon information technology networks. Over time, society has increased that dependence. Today, all organizations, including militaries, businesses, and governments, depend substantially upon these networks. Indeed, over the past few decades most elements of society have deliberately altered their routine functioning procedures to incorporate more information networks, increasing their reliance on such networks. They offer a maximally efficient way to store and transmit information. Many organizations now depend upon the real-time, multilateral communications and data flows that information networks provide. And were they to lose the Internet, most institutions would be unable to function because they no longer support the old manual processes. But these information networks not only facilitate the productivity of so many organizations, they also provide the means to disrupt and impair governments and militaries as well as financial, manufacturing, retail, and service industries.

There are four major properties that characterize the Internet. Each one contributes to its value, yet at the same time is a basis for vulnerability. The first property is *accessibility*. The majority of data on the Web gain value for the very reason that they are accessible. A vast amount of data is equally available to all users of the Internet; easy and rapid accessibility is part of the basic architecture of both the Web and the Internet. Even in more secure and relatively closed sub-networks (connected to the Internet or not), information is easily and rapidly accessible to legitimate users. It is, however, extremely difficult to monitor and control the avenues of access while maintaining open communications, in general-use and in restricted-access networks. Almost by definition, the easier it is to communicate over a network, the more accessible it will be to potential intruders. When discussing accessibility, it is important to note that, while the networks are simply and rapidly traversed, end-point computers – personal computers to servers that hold data and willingly perform processing as a result of messages sent – are part of the accessible network. Illustrating this point, the National Security Agency in a wry but forceful gesture displayed a brick in a glass case with this description: "The only secure computer."

"The threat will grow with the number of attackers and their ambition increasing."

The second property is *anonymity*. Internet protocols do not assure a recipient of a message that the sender is actually the person or site from which the message purports to come. A sender may masquerade as someone else.

The third property of information networks is *decoupled locale*. There is no notion of physical location of a user. A message sender may have an Internet address. That address may be designated in a message, but people and computers are mobile. That Internet address does not tie to a latitude-longitude physical location. And, of course, the sender may "spoof" the recipient by writing in the message any possible address.

Fourth, the *speed* of the message communications on the Internet is orders of magnitude faster than the speed of human reaction; that speed means that events happen in virtual space at a pace with which humans cannot easily match.

These attributes are not weaknesses. They are properties of the Internet architecture, and each one contributes to useful functioning of the Internet. The problem is that each one also contributes to its vulnerability.

The organizers of the conference debated over the title. Should the term "cyber war", "cyber attack", "cyber incursion", or "cyber intrusion" be used? The question illustrates that society does not yet have good mastery of the distinctions among these terms, and the case studies reinforced this confusion. Those who presented alternately used several of the terms. Developing another question: Were some of these incursions actually acts of war?

Following accepted terminology, we use the term *cyber security* to mean the provision of assurance that information will be accessed and used only in accord with the intension of the owners of that information. The level of cyber security that a computer system or a network of systems can deliver is a result of the architecture implemented by the software, hardware, and interconnections used by individuals.

This need for cyber security and precaution has not been acted upon: "We do not protect cyber space as well as we protect our physical space. We have left the doors open." These open doors provide enormous opportunities to attackers who can steal, destroy, and corrupt data on networks. As some participants noted, "Although we can increase the difficulty of penetration, there is no way to make systems impenetrable." This threat to cyber space is not simply theoretical: successful intrusions into sensitive but unclassified US government systems have been well-publicized; less well reported, but just as extensive, are the breaches of private sector networks. Increasing the difficulty in preventing penetration is the often suboptimal education of less-sophisticated whose actions in cyber space can be exploited.

But, we must remember that physical space is not absolutely safe from intrusion either. Door and window locks of a typical home will not long deter a skilled burglar or an individual prepared to apply massive force. One can secure a physical space with barriers and guards. But that comes at an immense cost in dollars, time, and in the functionality. Similarly, a skilled cyber attacker can penetrate the security defenses of most information systems, unless they are protected in a costly and function-limiting way.

The very accessibility of data and information services that makes actions easy for the legitimate user exacerbates the difficulty of providing cyber security. When an intruder is physically remote, possibly a continent away, all the tools for physical defense and law enforcement are not available. Because an intruder's actions may take place at electronic speeds, the time window within which security defenses can be deployed is very short. To complicate the difficult situation for the cyber defender, network protocols permit attackers to masquerade as someone else or to be anonymous. And the technical and legal tools to "give chase" are weak to non-existent. The situation is "stacked" to favor the intruder and disarm the defender.

The sophistication of exploits increases as novice attackers, using sophisticated tools, have more successes. As a result, cyber threats will only increase in number. In order to protect vital systems, increased security measures and greater precautions should be implemented. Currently, many systems do not deploy powerful enough security measures. And cyber defense tools can be weak. For example, a typical anti-virus package recognizes viral software based on a signature, a pattern of bits in the virus. Such a tool will fail to recognize a new software virus or even one that is able to dynamically rearrange its bits, thus avoiding ever having a predictable signature.

Because "the ambition of attackers is increasing," new and improved security measures must be developed and more detailed information on proper usage should be disseminated to those using these systems.

One of the most important infrastructures currently under attack is the US government. It faces continual attacks from a spectrum of would-be intruders, ranging from the incompetent amateur to those whose sophistication and resources suggest an international adversary. According to the Department of Homeland Security, there were 37,000 attacks on US government networks in 2007, a significant increase from the 24,000 that occurred the previous year.

But, the US government is just one of the many important institutions suffering from extensive attacks. It and other high value targets can be protected to an extent, but "we must avoid the illusion of a perfect defense." We must understand that protection, even imperfect protection, is expensive. Helping decision-makers understand the need for public and private security measures is a difficult and nuanced problem, especially when resources are scarce. Participants felt that the situation will further deteriorate. New attacks will rapidly emerge.

The publicly available information about compromised US government networks relates almost exclusively to unclassified domains. In fact "most of the successful attacks have been against unclassified networks," suggesting that more appropriate security measures are in place for classified networks. Although this statistic is comforting, one participant observed that, "they are going after the unclassified networks with the B-Team; the A-Team is going after the classified ones."

"We do not protect cyber space as well as we protect our physical space. We have left the doors open."

Attacks on information networks occur continually. Cyber attackers seek to perform traditional acts of espionage and crime using cutting edge technology. The government and the private sector has, however, not always responded in kind but have often been "casual and amateurish" in handling this growing threat. Most attacks are nationally insignificant, but personally or institutionally harmful. There are, however, cyber events with the potential to inflict enormous harm. The government needs to have a clear response plan in place for there are cyber attacks that could realize such potential.

There are a number of hurdles preventing the development of such a response. As two of the case studies demonstrate, one of the major impediments to the development of policy responses is the difficulty in identifying the source of attacks. Because of the open nature of networks and systems, attackers can easily act across multiple national boundaries, remaining anonymous by masking their identities and utilizing multiple intermediaries. Even the most complete and technical forensic trails lead only to a computer and not to an individual.

This anonymity of the attacker, as well as the unpredictable nature of cyber attacks, makes the threat of cyber attacks strikingly similar to that of terrorist attacks. Like those involved in counter-terrorism, the people defending networks have very limited information from which to develop strategies of prevention or by which to trace a culprit. Even once a cyber intruder has been identified, it is difficult to determine the scope of the intrusion. Forensics are difficult to perform and legal recourse for prosecution and justice are weak.

In the end, the greatest security vulnerability is the user who controls their networks' accessibility. Cyber security is not just technological; it is also sociological—individuals are responsible for protecting their computers and limiting access to their networks. In considering information networks, there is an inverse relationship between usability and security, and in the past, both individuals and institutions have sacrificed security for usability. Discussants at the conference asserted "accessibility cripples security". One way to manage cyber threats is to reverse this relationship, placing the emphasis on security, not on usability and accessibility.

There is a balance to be struck between "usability", "accessibility", "productivity," and "security". Participants wondered whether users could be convinced to increase security at the cost decreasing the others. Some advocated a new balance so that the "need to share" has an equal position with the "need to know" in order to increase security.

Arguing that demands for productivity and that the reliance of current and upcoming generations of the workforce on Web collaboration, some believe that usability will remain the priority. Others contend that more stringent security policies and increased security awareness, developed by public outreach and corporate/institutional training, could improve user behavior resulting in strengthened cyber security.

In order to protect critical public and private infrastructures and organizations, a multi-pronged strategy needs to be developed which will not only address issues concerning the development of technological security measures but will also educate users as to the need for increased precaution.

Ed Meese
IQIC

The internet is the first thing that humanity has built that humanity doesn't understand, the largest experiment in anarchy that we have ever had.
– ERIC SCHMIDT

II

Case Studies of Cyber Incursions

Three case studies were presented by individuals who had encountered, defended against, and actively fought major cyber incursions; these studies were characterized by the presenters' profound knowledge of cyber defense and their insights for future defense systems.

Case Study I: The Asian Case

In 2007, a highly developed attack on governmental networks in a small Asian nation was intercepted and halted. Prior to the direct attack, three networks belonging to government agencies were penetrated by attackers. The attackers deployed more than 100 personal computers by using a sophisticated, three-stage methodology that exploited both technical and sociological vulnerabilities in the government systems.

The attackers used multiple layers of "stepping stone" servers and Internet Protocol addresses to conceal their identities. They were able to route stolen data through compromised computers and to provide new instructions for these computers during the attack without detection. The attack plan had three parts:

- *Case the Target.* The attackers cased the target and collected data by probing the target networks with both host and port scans. The attackers used NSLookUp, WHOIS, Traceroute, and other Internet tracking and identity services to identify target Internet Protocol addresses.[1] They also

[1] The cryptic names are of specific utility programs that deliver information useful to the attackers.

collected electronic mail addresses of the targeted networks' users to exploit in a later step.

- *Gain Privileges on Compromised Machines.* On systems with firewalls, e-mail attachments, which exploited so-called "zero day" (newly discovered and unpatched) vulnerabilities[2] in popular applications like Word or PowerPoint, were used to install software that gave attackers control over the personal computers' operating system and access to any files or folders imported to it through devices such as USB thumb drives or memory sticks.
- *Maintain Privileges and Install Software.* Once the attackers had established privileges on the compromised personal computers, they were then able to install software that collected passwords, analyzed communications, logged keystrokes, and gave attackers the ability to monitor and manage the compromised personal computer remotely.

Once the attackers made initial contact and compromised a computer within the network, they were able to exploit connections between that computer and others. At least one of the penetrated systems with a firewall in this case was compromised by a friendly neighbor system without a firewall, which the attackers had already infiltrated.

The attack exhibited a high degree of sophistication, both in this social engineering used to package malicious electronic mail attachments and in the technical expertise demonstrated by the software used within them. Employing a complex electronic mail hacking system, the attackers invaded networks establishing contacts in multiple computers. Harmless e-mails with a downloadable image were sent to users of targeted networks. The downloadable image was a blank line that was invisible to the recipient. If the user opened the e-mail, however, his computer would contact a server designated by the attackers. This contact informed the attackers that the there was indeed a computer at that address and that that particular user might open an e-mail message loaded with malicious software. When the attackers later sent e-mails that contained malicious attachments, they falsified the addresses so that messages appeared to come from someone that the

"They are going after the unclassified networks with the B-Team; the A-Team is going after the classified ones."

[2] A zero-day attack exploits unknown, undisclosed, or unpatched computer application vulnerabilities. Zero-day exploits are deployed before the vendor releases a patch to remove the vulnerability. Zero-day exploits generally circulate through the ranks of attackers before finally being disclosed on public forums. The term derives from the age of the exploit.

target user communicated with regularly or from someone else within the target network.

This e-mail strategy was only one avenue of the attackers' highly sophisticated penetration system. Between April 2004 and July 2007, the attackers utilized seven different zero-day exploits in popular applications. Attack software installed itself at the root of the operating system, which gives the software the ability to take any action whatsoever on the computer. Once the malicious software was established, it initiated encrypted communication with the attackers' command and control servers. Because this software generally did not contain the signatures for which anti-virus software packages scan, they were rarely detected at any stage in their penetration. Attackers also employed worms that spread through removable media, automatically installing themselves on any external drive; this covert and automatic installation quickly compromised other computers in the network.

Since discovering the attack, the defenders have attempted to reconstruct the attacks in an attempt to understand how the penetrations were performed and who was behind them. A technical solution that they developed was an automated e-mail and document analysis system, dubbed Honey Bear, designed to search for malicious software based on its behavior. Another developed solution, Honey Net—a fake system designed to attract attackers to expose them—failed as no attackers were deceived by the falsified system. Thus far, there is very little information about the source of attack because of the care and sophistication of the attackers.

Because the attackers routed information that they were stealing through a series of "stepping stones" or storefront Internet addresses and often used computers or servers that had already been penetrated, their trail was almost impossible to follow. There are, however, some aspects of the attackers' trail that have been uncovered due to "store and forward" techniques, which left a trail because the servers saved copies of the stolen data packets and kept records of where they were sent. These records unfortunately, do not provide enough information to trace the origins of the attack, as there are large gaps in the trail. The attackers also used "connection re-direct" techniques that left no record of what information had been sent or where it had been sent. Even with their extensive investigation, the authorities "have no evidence about where these attacks originate." Despite the paucity of technical forensic evidence, there are several facts about the attacks that identify at least one potential suspect.

"We must avoid the illusion of a perfect defense."

Key observations from the Asian case

- Too many personal computer users do not observe good security practices and become pawns of cyber attackers.
- It is critical that vendors release security patches rapidly and that users apply those patches.
- Good e-mail discipline is required.
- It is extraordinarily difficult to identify attackers using only technical forensic data.
- There is little (stored data) memory in the "middle" of the network, through which messages transit, that can be used in forensic analysis.
- The defense needs to adapt continuously to attackers' changing strategies.
- The attacker has not been indisputably identified.
- While the attack was sophisticated, the number of attackers was probably small.

Case Study II: The European Case

In 2007 a small European country experienced a large-scale Distributed Denial of Service (DDOS) attack, as well as multiple Web site defacements. These attacks and defacements were correlated with a larger crisis involving violent street demonstrations and ethnic conflict. It had been decided to re-locate a controversial monument, which had become a highly contested symbol of national meaning, representing to some oppression and to others freedom. Rumors about what was going to happen to the monument triggered both physical and cyber protests. The most notable of these cyber protests was an attack conducted in three waves, one of which was on a scale "almost impossible to create without a well-coordinated group and a chain of command."

The command and control of the group was distributed among several organizations and across national boundaries. Attackers used various strategies from grassroots to hierarchical power structures to coordinate their attacks. Much of the control was exercised through nationalistic chat rooms and Web forums where participants posted instructions for attacks and coordinated timing. Many of those who participated in these forums were from a large neighboring country and were involved in a nationalistic youth organization. Upon investigating this attack, some observers have detected the hand of the intelligence services of the large neighbor, which carries troubling implications. The largest single set of attacks came from a bot-net, or robot network, of compromised computers being used without the knowledge of their owners. The bot-net was rented from a criminal syndicate.

Although a many of the bogus requests to the targeted systems that constituted the DDOS attacks came from Internet addresses belonging to the neighboring country's government, it remains unclear whether this attack was an official act. It is possible that the government's employees were acting on their own in response to nationalistic calls for action or that the employees were themselves the victims of hackers using their machines to launch attacks. But, because the government of the neighboring country declined to cooperate with efforts to investigate the attack, the attack's source and motive may never be known.

This cyber attack inflicted no significant damage to critical infrastructure nor did it permanently compromise any data. Instead the Web servers of some government and private sector entities were overwhelmed by high volume of DDOS requests; they were bombarded with millions of falsified requests until they crashed or were taken off-line. This cyber attack was mirrored in a physical demonstration in which protesters drove their cars at extremely low speeds through the center of the capital to grid-lock traffic. This protest acted as a physical analogue to the DDOS attacks which in effect grid-locked the cyber avenues and channels of communication.

"It was more like a cyber riot than an act of war."

Although the country's Internet was shut down for a significant amount of time, the people's attitudes toward the Internet have not changed appreciably. The Internet is still used for banking, financing, and other important transactions despite the recent breaches.

Without international cooperation and in the absence of an international legal framework that might compel such cooperation, tracing the source of the attacks was nearly impossible. Even with cooperation—voluntary or compelled—such an investigation would take a great deal of time, straining the policy options for timely response.

While the European nation did receive some international assistance, political boundaries affect law enforcement. In this case, lack of cooperation impeded forensics and justice.

Key observations from the European case

- The character of the crisis emphasizes the degree to which cyber attacks, like many contemporary forms of conflict, blur established distinctions between nation-state warfare, insurgency, and other forms of rebellion, ethnic conflict, protest, or crime. This would especially be true if the large neighboring country was actually involved in the attacks.

- Tracing attackers who can easily act across national boundaries and effectively conceal their origins and location is difficult.
- Attackers can multiply their numbers by using open forums to "rouse the rabble."
- The absence of international legal frameworks under which attackers can be traced and prosecuted leads to problems of apprehension and indictment of cyber criminals.
- Crime syndicates now use and offer resources for sale.
- Cyber and physical disruptions can reinforce each other.
- The Internet was essentially inoperable during the attack, but it rapidly returned to functioning after the attack.
- The public's trust in current digital systems appears, at least in this case, resilient.

Case Study III: The Middle Eastern Case

In the Middle East, a key US ally has found that al Qaeda networks are using the Internet to recruit, train, fundraise, and communicate. Through the Internet, al Qaeda can disseminate extremist interpretations of Islam to young people, indoctrinating them with terrorist ideology. By posting videos and texts that promote terrorist activities and provide instructions for them on the Internet, al Qaeda spreads terrorist techniques and tactics. Al Qaeda communicates through the Web, planning and coordinating operations electronically. Through direct means and fronts, terrorist organizations use the Internet to raise funds and gain supporters. The Internet has become a critical element to al Qaeda's international operations and will continue to be so. Al Qaeda owns and operates satellite communications technology, voice-over-IP techniques, and social networking sites. Extremists have established and currently maintain between 4,000 to 6,000 Web sites, including password-protected forums to which thousands of active al Qaeda supporters belong.

> ***"The network capabilities that [al Qaeda] has access to are currently insufficient for [cyber] attacks."***

In 2004 an individual on one of these forums caught the attention of security services. Known by the screen-name Irhabi007 (*Irhabi* is Arabic for terrorist), this individual was arrested last year by British police after acting as a key cyber facilitator for al Qaeda. For two years, Irhabi007 eluded a multi-national manhunt that included a special CIA unit established to identify him. During this time, Irhabi007 taught incursion techniques, propagandized al

Qaeda online through videos and other media, and facilitated al Qaeda communications.

Individuals are not al Qaeda's only ties to the Internet; the Global Islamic Media Front is another example of how al Qaeda has incorporated cyber operations into its basic organization, linking leaders to terrorist cells as far away as North America. When one of the Global Islamic Media Front's leaders was arrested last year, authorities seized a forty-gigabyte hard disk and multiple flash drives, which held "information [that] has proved very useful" to investigations.

Al Qaeda clearly uses the Internet for recruitment, planning, and fundraising. Beyond these communicative elements, it seems that al Qaeda also has a high level of technological sophistication, demonstrated by their employment of "military grade" encryptions and other high-level knowledge and technical developments.

Although al Qaeda has been calling for a cyber jihad—the use of hacker skills against their enemies—since 2000, there has been no sign of efforts by al Qaeda to launch cyber attacks on specific targets. Instead of planning cyber attacks when they sought to attack a government database, al Qaeda planned a physical attack that was foiled. Some believe that al Qaeda may lack the resources to stage such an attack at the moment: "The network capabilities that al Qaeda has access to are currently insufficient for these types of attacks." Although they may currently lack the resources for such attacks, potential al Qaeda cyber attacks should be considered a long-term threat, and decision-makers should be cognizant of the fact that a single volunteer can quickly bring al Qaeda across this technological threshold.

Key observations from the Middle Eastern case

- Al Qaeda calls for hackers to use their cyber attack skills against their enemies.
- The absence of such attacks could be interpreted as a lack of volunteers or resources at the present time, which can change dramatically and quickly.
- Al Qaeda uses the Web as a vital logistical and communicative tool.
- Terrorists' use of the Internet can create opportunities for intelligence and law enforcement exploitation.

David Wennergren, Deputy Asst. Sec. of Defense for Information Management, Integration, and Technology provides remarks.

ABOVE: Rolf Mowatt-Larssen, Director of Office of Intelligence and Counterintelligence, Department of Energy.

LEFT: Anita Jones, Prof. of Engineering and Applied Science at UVa.

Information on the Internet is subject to the same rules and regulations as conversation at a bar.
– GEORGE LUNDBERG

III

Uncharted Territory

Reaching an equilibrium position with respect to cyber security is a work in progress. Society lacks clear definitions with which to make distinctions between cyber threats, cyber incursions, and cyber warfare. Currently, the terms used to describe a crime or threat depends upon knowing the attacker's identity—information that is nearly impossible to ascertain. When might a cyber attack escalate to cyber warfare? The boundaries between different forms of cyber threats and intrusions are hazy, creating problems for law enforcement and for policy makers.

Categorizing a cyber threat in order to take the appropriate measures to prevent future attacks is difficult when hackers are anonymous. A cyber attack aimed at a critical US infrastructure like a power grid could be defined in multiple ways: as an act of war if it was initiated by a nation-state; as an act of terrorism if it was conducted by extremists; or as a criminal act if it was designed by an organized crime syndicate or independent hackers. Compounding the importance of attacker identity is the fact that responses depend upon perpetrators. In the US, criminal and terrorist acts fall under the FBI's jurisdiction, but the military responds to attacks from nation-states. Without knowing the attacker's identity, appropriate and prompt responses can be impeded.

Just as an attack on critical infrastructure could be the act of alternative organizations, so too, could the defacement of private sector Web sites. Such defacement could be the result of individual vandalism; direct cyber action if done by an organized group seeking publicity; corporate foul-play if encouraged by a competitor; or terrorism or war if done to distract information security staff from a more serious attack. Again, with varied possible perpetrators, it is hard to appropriately address the attack.

"More cooperation from currently recalcitrant nations may result when they see their citizens victimized by online criminals."

Identifying perpetrators is not the only element in this equation that presents problems; determining whether, and at what scale, an attack is being waged can be nearly impossible. Currently, as several participants observed, there are no clearly defined "tripwires" or warning mechanisms that, with certainty, indicate that a cyber attack is in progress. Although both the public and private sectors have a paucity of such measures, the private sector is significantly lacking in this arena. Although the US Computer Emergency Response Center and the IT Information Sharing and Analysis Centers try to identify new types of threats and to notify potential targets, there are still very few mechanisms for real-time reporting of potential attacks. There is even less time for law enforcement response because the time-scales of attacks are measured in seconds and minutes today whereas a decade ago they were measured in hours and days.

It is not simply the classification and ascription of legal responsibility to prosecute that can impede the government's attempts to prevent the spread of cyber incursions but also the balance of risks. The government needs to share information with the public, but when the government publicizes an exploit or a technique for an attack, it invites other attackers to attempt it. Thus, the government and private sector corporations must make difficult decisions about public disclosure in order to maintain security.

Beyond Borders and Beyond Perimeter Defense

The key terms in the vocabulary of cyber security—firewall, gateway, intruder, penetration, access control—imply that there is a perimeter to be defended. The notion of perimeter defense, the dominant paradigm for cyber security, originated in a time when mainframes were kept in locked rooms. As one participant put it, "perimeter defense is the Maginot line of cyber security." Perimeter defense has never worked in the physical world. For example, the Maginot line that was designed to keep the Germans out of France was by-passed in days; it serves as a good example of the failure of defensive perimeters. There is no reason to believe that perimeter defense will be effective in virtual space. Firewalls can always be breached by an attacker who is persistent and determined, and they are quite ineffective against insiders who act in a hostile fashion. Although no network security system is impenetrable, there are better methods than static defensive barriers such as firewalls.

"Perimeter defense is the Maginot line of cyber security."

Almost by definition, software security is weak. The millions of lines of code in modern software make effective security audits impossible. Moreover, the exploitation equation is weighted heavily in the intruder's favor—he only needs to find a single flaw; the defender must protect or try to fix all flaws. Because it is difficult to specify the correct behavior of these complex systems, it is very hard to identify a flaw. In one survey it was found that more than half of all security exploitations were based on manipulating a correctly functioning feature of the software. The author of the software specification just never envisioned such manipulation.

There is one highly effective security tool that does not rely on perimeters and that is encryption. It is described as an "end-to-end" mechanism because the security of the encrypted data relies only on the encryption algorithm and the secrecy of the keys involved. There is no "perimeter" around the encrypted data as it is transmitted from one place to the other. Public key encryption uses a pair of "matched" keys. One is made widely public, by being posted openly on a Web site. The other is kept private. A message encrypted with one key can be decrypted with the other. This permits a user to create a pair of keys and publicize the public key. Anyone receiving an encrypted message that purposes to be from this user can simply decrypt it with that user's public key. If the decrypted message makes sense, then it can only have come from that user. Although public/private key encryption is slow, it permits any user to distribute keys without the need for a trusted courier to carry keys. This method is one basis for authenticating a user.

> ***"There is no technological 'silver bullet' for cyber security."***

Participants agreed that there is no technological "silver bullet" in part because of fundamental characteristics of the current Internet architecture. Many people assume that the Internet protocols are a "given" and cannot be changed. While they work extraordinarily well, it is possible to revise those protocols to provide fundamental building blocks so that those who desire more security can build it. In particular, if the Internet protocols provided functionality so that those users who wish greater security could be assured that a message is authentic, that is that it was authored by the source from which it claims to come, it would be possible to have assured authenticity of messages – but at some cost. Further use of encryption is a possible augmentation for safeguarding data, even on insecure networks.

Legal Safeguards

There have been attempts to create uniform and legal frameworks through which to analyze cyber activity. The 2001 Council of Europe's Cybercrime Convention provides some legal framework for cross-border investigation and the prosecution of intruders, hackers, and other cyber criminals. However, many countries, particularly some that are considered to be hubs of cyber crime because of their laxer laws on cyber activity, have failed to sign it.

Perhaps, as more countries begin to experience the effects of cyber incursions, they will become increasingly aware of and concerned by the absence of an adequate legal framework for combating and prosecuting cyber incursions. Currently, the US suffers from cyber incursions at a significantly higher rate than other nations; US computers are attacked at ten times more often than computers in any other country. But, that ratio is changing. Other countries are starting to appreciate the negative consequences associated with the absence of an adequate legal framework for the investigation and prosecution of cyber incursions. More cooperation from currently recalcitrant nations may result when they see their citizens, businesses, and governments victimized by online criminals.

As other countries, currently disinterested in entering into international legal agreements, become more wired, they become more dependent upon cyber space and therefore more vulnerable to attack. This trend could lead to a political paradigm similar to the threat of the "Mutually Assured Destruction" scenario. This possibility increases the attractiveness of deterrence as a policy, much as it did with nuclear weapons.

The Public Health Analogy

Given the shortcomings of the current law enforcement or war-fighting models as ways of understanding cyber incursions, several participants suggested that a more helpful paradigm might be provided by public health. The appropriation of public health terminology allows cyber incursions to be approached with some nuance. And the analogy is apt: not only are cyber incursions sometimes called viruses, but also the best means of controlling these viruses lies in prevention.

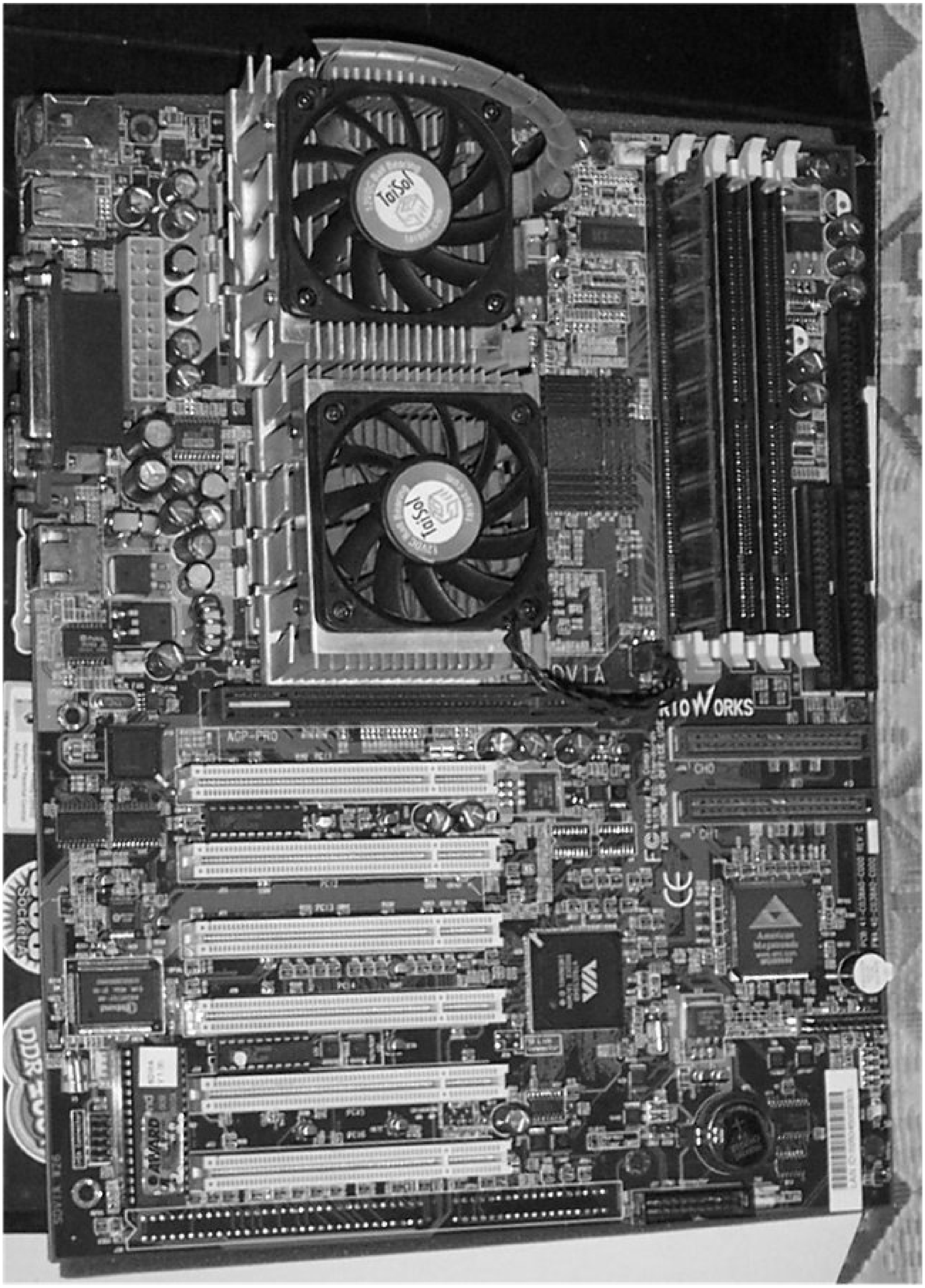
"With this form of cyber incursion, people who allow their computers to become infected are part of the problem."

Through spam e-mails, cyber criminals launch millions of so-called Trojan horse viruses. These viruses enable them to seize control of computers that are poorly patched or have careless users. Once they have gained access to these computers, the intruder can link the computers in huge nets or herds that can then be used for distributed denial of service attacks, spam, or other purposes.

Many of these infections could easily be avoided if communities acted responsibly, using up-to-date systems and virus software and following a few basic behavioral precautions, such as not automatically opening attachments. As with hand-washing and other basic hygiene measures that help conquer viral epidemics, “there isn’t any other way to deal with this except to get the public to understand how these infections spread and then get them to act appropriately.”

The health care paradigm emphasizes the importance of public outreach and awareness. Individuals and corporations must learn to look after their own security to an extent—just as families have to take responsibility for vaccinating their children. The government cannot protect the Internet or other privately owned networks, any more than it can filter germs out of the air.

Viruses, whether they are biologic or cyber, can stigmatize their hosts who may be too concerned with their reputations to report their infections; some organizations would rather deal with invasions privately than publicly announce their compromised systems. This failure can establish a fertile environment for propagation. Failure to report incursions weakens the community by lessening its appreciation for the magnitude of the threat; by limiting constructive communications among governments, corporations, and individuals who are being victimized; and by emboldening the attackers. In public health, doctors are required to report some kinds of cases that they see. This alerts the health authorities to activate defenses. This approach might work well with cyber space, allowing officials to act proactively and preventatively.


TaiSol
TaiSol
SDVIA
RIOWORKS
AGP-PRO
CH0
CH1
AWARD
DDR 266

Sed quis custodiet ipsos custodes?
[Who watches the watchers?]
– JUVENAL

IV

Some Ways Forward

Throughout the conference, participants discussed ways in which to prevent and to cope with cyber incursions. One suggestion was to think in terms of mission assurance: determine which elements needed the most protection before and during attack, and which elements would need to be reconstituted and how rapidly. Prioritization is central for both security and mitigation for, "if you try to protect everything, you can't protect anything." The first step is to prioritize assets, based on their value to mission assurance. Because prioritized response requires an ongoing assessment of the seriousness of the attack, metrics to estimate the scale of cyber incursions are needed. Ideally, such metrics would be the basis for rapid and accurate evaluation the scale and potential damage of the attack. There also needs to be a new vocabulary with which to describe the risks in more precise terms.

"Prioritization is central in planning both security and mitigation, for, 'if you try to protect everything, you can't protect anything.'"

Some participants believe that encryption is an important tool for protecting data while being transmitted across networks. Encryption does not depend upon perimeters, but only the actions of the senders and receivers at the ends of the data transmission path. Encryption can also protect (not-in-use) data—whether stored in permanent or temporary files—against unauthorized access even with intruders present in the system. Widespread use of encryption for the purpose of authenticating message senders would require a protocol that supported carrying some identity information, sufficient to suggest the public key of the sender. Currently, computer nodes on the Internet place their Internet address in each message. If instead or in addition, the message carried information that identifies the sender's identity, authentication could be achieved – for those users that want it. Such modest protocol adaptation may strengthen the security safeguards.

But, if the past is any example, new technological advances and methods must also be paired with user instruction, for human error and carelessness invite these attacks. Today, many individual users do not take the risk of cyber incursions seriously. Because "ninety percent of the vulnerabilities are between the chair and the keyboard," efforts should be taken to sensitize and train the users. One proposal was to institute "continuous training" to reinforce the need for security awareness amongst users and to keep information technology specialist up-to-date with developments. Several of the participants pointed out that it would be most effective to teach children proper Web usage. Others focused their attention on behavioral issues, trying to pinpoint ways to keep network users honest, suggesting prohibitions on the downloading of certain vulnerable or threatening software.

"Ninety percent of the vulnerabilities are between the chair and the keyboard."

Participants asserted that people across national boundaries need to develop international laws and treaties regarding safe and acceptable use of the Internet. Various international bodies could be influential. For example, the International Telecommunication Union, based in Geneva and associated with the United Nations, was mentioned as an existing international institution that should be considered to be a model. And many thought that if more countries signed the 2001 Cybercrime Convention, then progress could be made in the effective regulation of the Internet.

There is enormous difficulty in ascertaining the source of cyber attacks especially across national boundaries without international cooperation. Some suggested the development of an authoritative international institution that would "investigate, assess, and allocate responsibility" for major cyber incidents. The feasibility of such efforts, however, was not explored. The feasibility of changing the Internet protocols so that sources could be traced was also not explored.

Although most of the participants felt that legislative action needed to be taken, there was some discussion about the wisdom of legislating. Most participants seemed to agree that Congress could easily do as much harm as good through poorly-drafted legislation. There was also some discussion about the structure of congressional oversight, with some feeling that there was "a diffusion of authority" over cyber issues because too many committees have claimed jurisdiction.

Other approaches to control cyber incursions that were considered included: conventional intelligence techniques to analyze stolen data in an attempt to deduce who would want it; and traditional law enforcement techniques that have proved successful against other forms of organized crime. One way or another law enforcement organizations can no longer avoid making accusations. They must have the political courage to say who they think the attackers are; "naming and shaming" is crucial in the effort to de-legitimize cyber attackers. Correct attribution and a clear stance on cyber crime is key to deterrence. Today, the US has no clear doctrine about cyber attacks.

A number of participants asserted recommendations for action by the government, the private sector and academia. Some of these recommendations had strong support from participants, but there was no attempt to assure consensus. We offer them for consideration:

Key Options – Government

- Increase disclosure about cyber incursions – when and how they happen, their source, and what evidence there is for this attribution.
- Use international venues to de-legitimize cyber incursions, by pressuring nations to sign the Cybercrime Convention or by initiating or joining other efforts to promote an international framework for the investigation and prosecution of cyber incursions.
- Continue to build partnerships with state and local law enforcement, and with the private sector to improve situational awareness and facilitate coordinated responses.
- Improve public awareness of incursions.
- Train the public how to prevent cyber incursions through public outreach and K-12 education.
- Develop ways of communicating about cyber risks, both to the public and internally in the government.
- Prioritize risks; protect and plan to mitigate attacks based on that prioritization.
- Encourage public debate about the risks, potential counter-measures, and the costs of action and inaction against cyber incursions.
- Create and fund basic research to improve computer security.

Key Options – Private Sector

- Develop computer products that enforce user security discipline through the configuration management and other "door locks," and that offer options for the user to choose how to balance security and usability.
- Deploy new, non perimeter-based security technologies, e.g. document and traffic analysis and enhanced encryption.
- Enhance training and security awareness as a technique to lessen (not eliminate) the threat of incursions.

- Adopt methods to deal with disclosure of attacks, employing e.g. the public health model to raise awareness about the need to share information concerning incursions, so as to maximize situational awareness and coordinate responses.
- Improve collaborative partnership with government, law enforcement, and private companies.

Key Options – Academia

- Develop more powerful encryption-based solutions.
- Design, prototype and evaluate a more secure Internet architecture.
- Develop new frameworks and metrics, and the accompanying vocabulary, to distinguish between and characterize cyber incursions and other threats.
- Encourage and participate in a public debate about the risks, potential counter-measures, and the costs of action and inaction against cyber incursions.