FEBRUARY 2005
VOLUME 3, NUMBER 7

THE CIP REPORT

Cyber Crime

CIP Program Staff

John McCarthy, *Director / Principal Investigator*

Jerry Brashear, *Associate Director, National Capitol Region Project*

Emily Frye, *Associate Director, Law and Economics Programs*

Rod Nydam, *Associate Director, Private Sector Programs*

Dr. John Noftsinger, *Executive Director, JMU Institute for Infrastructure and Information Assurance*

Ken Newbold, *JMU Outreach Coordinator / JMU CIP Program Liaison*

Contact: cipp01@gmu.edu
703.993.4840

If you would like to subscribe to *The CIP Report* please click here.

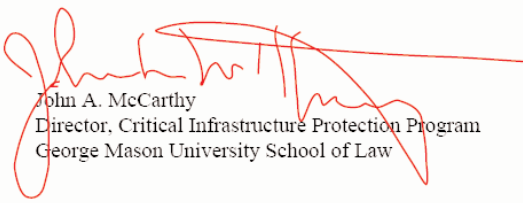
Director's Message

This issue of *The CIP Report* focuses on cybercrime and the initiatives underway to combat the many and complicated manners in which criminal activity is conducted within cyberspace. The term cybercrime is extremely broad, and growing more so everyday as new illegal activities are discovered, and currently covers everything from hacking, to denial of service attacks, identity theft and creative phishing schemes. These crimes, while perpetrated through the hazy anonymity of the Internet, have enormous and measurable economic impacts and are resulting in a growing number of prosecutions.

The CIP Program has seeded research on a variety of international issues related to cybercrime, one of which, dealing with Romania, is highlighted in this month's issue. While international legal impediments continue to challenge the prosecution of this activity, new and ongoing dialogue has removed some barriers towards a more cross-jurisdictionally functional international regime. In an effort to help practitioners deal with this challenge, CIPP will be hosting an international conference next fall dedicated to cybersecurity issues and best practices in the international arena. In addition to this conference, the CIP Program will also be holding another "Critical Conversation" event dedicated to cybersecurity issues and examining the urgency of the threats we face. As the event approaches, we will provide details and registration information in upcoming editions of *The CIP Report.*

In addition to this glimpse into the international issues of cybercrime, we have also included information on FBI Cyber Unit initiatives yielding strong results, Operation "Web Snare" and "Digital PhishNet". We also highlight the National Cyber-Forensics and Training Alliance (NCFTA), the first partnership between public and private sectors of this nature. Both of these programs have yielded practical results indicative of the innovative efforts underway to adapt to and combat the constantly changing nature of crimes committed within cyberspace.

On the political front, we have provided a brief overview of the proposed legislation by Representatives Zoe Lofgren (D-CA) and Mac Thornberry (R-TX) to create an Assistant Secretary for Cybersecurity position within the Department of Homeland Security's Information Analysis and Infrastructures Protection Directorate. This legislation would, if passed, provide the Assistant Secretary position primary authority within DHS for all cybersecurity-related critical infrastructure protection programs of the Department, including policy formulation and program management.



John A. McCarthy
Director, Critical Infrastructure Protection Program
George Mason University School of Law

Romanian Cyber Crime: A Summary

Stephen Bowers, Ashley Derrick, & Lauren Zangardi
William R. Nelson Institute, James Madison University

Contemporary Romania is a fusion of East and West. The collapse of Ceausescu's communist regime in 1989 opened the door for democracy and created wider access to computer technologies, thus creating the necessary environment for a technologically based market system. Yet, it simultaneously revealed troubling contradictions about the role of technology in Eastern Europe and the inherent difficulties of transition, calling into question basic assumptions about law and technology.

Eastern Europe's stagnant economy, coupled with a lack of adequate legislation, created an environment suitable for the proliferation of pirates and hackers. Cyber crime and cyber terrorism changed the landscape of law enforcement. Attacks on computer systems, whether for monetary gain or the disruption of critical infrastructure, are in a relatively new realm of criminal activity where norms and standards have yet to be established, in part due to the scope of activity.

Demonstrating an ironic ability to equal their Western counterparts, young Romanians have earned a reputation for their ability to capitalize on the vulnerabilities of modern information technology systems. In partnership with other computer criminals in Western Europe and the United States, Romanians have been able to steal millions of dollars each year from Western companies doing business on the Internet.

These thefts are accomplished in several ways. First, by creating phony Internet companies Romanian criminals are able to defraud customers who believe they are making purchases from legitimate vendors. Second, hackers frequently engage in extortion by entering systems, stealing information and threatening to use that information against businesses that refuse to pay cash for protection. Finally, thousands of young Romanians have mastered the art of creating computer viruses. By offering programs to defeat the virus, they have turned this dubious skill into a marketable talent. Romanian universities unwittingly provide a training ground for skilled students who first, target fellow students, and later, graduate to wider Western markets for their services. Despite a variety of criminal cyber-activity, the most common occurrence linked to Romania is auction fraud. Auction fraud can be a consistently lucrative business. Most victims loose about $500 to $600, often twice the average monthly salary in Romania. It is not necessary for every instance to yield a large sum when, basically, any amount provides a decent supplement to an average Romanian income.

As late as 2000, Czechoslovakia and Poland were the only Post-Communist states to have partially updated their computer legislation. All the other states in the region had failed to take even the first steps toward meeting this new legal challenge, according to a McConnell International study. Realizing Romania was quickly becoming blacklisted as a hotbed for hackers, U.S. officials stepped in to help remedy the situation. The FBI officially opened a Legal Attaché (Legat) office in Bucharest on August 24, 2000. One aspect of its function is to train international law enforcement personnel in methods of intercepting international crime. This collaboration between Romanian and U.S. officials resulted in the formation of a computer crime task force in 2003.

Romania did not have the proper legal parameters for punishing online criminal activity until the government enacted National Law 161, known as the Romanian Cyber Crime Law, on April 19, 2003. This law became the basis for the prevention and countering of computer related crimes. The *(Continued, Page 11)*

Representatives Zoe Lofgren and Mac Thornberry Reintroduce Cybersecurity Legislation

In early January, Representatives Zoe Lofgren (D-CA) and Mac Thornberry (R-TX) reintroduced bipartisan legislation to create an Assistant Secretary for Cybersecurity position within the Department of Homeland Security's Information Analysis and Infrastructures Protection Directorate. The legislation, also known as "the Department of Homeland Security Cybersecurity Enhancement Act of 2005" was first introduced in the second session of the 108th Congress. The establishment of a new Assistant Secretary position was ultimately approved by the House as part of H.R. 10, the House-passed version of last year's intelligence reform bill, but was not included in the final intelligence reform legislation approved by Congress and signed by the President.

"It is imperative that Congress work with a sense of urgency to revisit this bill to elevate the position of Assistant Secretary for Cybersecurity, so we can make sure that the top government cybersecurity personnel has the access and authority to get the job done," said Rep. Lofgren. "The creation of this position will also help protect our physical and converged physical-cyber infrastructures by hopefully putting experts - not bureaucrats- in charge."

Rep. Thornberry said, "At the same time that our Nation is growing more dependent on the reliability of various computer networks, the number of cyber attacks is also growing. Creating an Assistant Secretary is far more than just an organizational change. It is an essential move to assure that cybersecurity is not buried among the many homeland security challenges we face."

If passed, the legislation would allow for the Assistant Secretary to have primary authority within the Department for all cybersecurity-related critical infrastructure protection programs of the Department, including policy formulation and program management.

The legislation touts strong support from the technology, education, and financial sectors. ❖

Congresswoman Zoe Lofgren has consistently been recognized as a leader of high tech issues since she was first elected to Congress in 1994. As Representative of California's 16th District, which includes the Silicon Valley, high tech issues are on her doorstep every day. The list of initiatives, programs, and legislation she has sponsored and co-sponsored for the benefit of the high tech industry is staggering. She is a member of the House Select Committee on Homeland Security, where she serves as Ranking Member on the Subcommittee on Cybersecurity, Science, Research & Development. The Cyber Security Industry Alliance recently spoke with Congresswoman Lofgren about cybersecurity.

What is the biggest vulnerability we face in cybersecurity today?

Our economy and infrastructures are dependent on the durability of our computer networks and systems. This interdependence makes our economy and security vulnerable to cyber attack. We are also vulnerable to a cyber attack that is combined with a physical attack.

Unfortunately, both within and outside the government, we are not adequately prepared. Systems and technologies were, and continue to be, deployed without giving sufficient consideration to security.

The Department of Homeland Security is failing to provide the leadership necessary to protect cyberspace. This is due to the de-prioritization of cybersecurity by the current *(Continued, Page 4)*

Lofgren *(Cont. from Page 3)* administration. Two years ago, the government's top advisor on cybersecurity sat in the White House. Today, the position is buried four levels down in the Department of Homeland Security bureaucracy.

Congressman Mac Thornberry and I listened to the experts in technology, banking, business, and academia and introduced legislation to remedy this problem by creating an Assistant Secretary of Cybersecurity. I hope we can reintroduce this bill in the coming Congress so we can make sure that the top government cybersecurity personnel has the access and authority to get the job done.
The creation of this position will also help protect our physical and converged physical-cyber infrastructures by hopefully putting experts - not bureaucrats - in charge.

Incredibly, when I recently reviewed California's list of critical assets and resources in the National Asset Database, many if not most of what should be assessed and protected had not even made it onto the list. State and local law enforcement, which are our first responders, do not even know about the lists. The Department cannot possibly conduct meaningful analysis if it is using incomplete and inaccurate data as a foundation.

What do you believe is the role of government (Executive Branch/Congress) in cybersecurity?

The U.S. Government has an important leadership role to play in the cybersecurity arena. The majority of the nation's cyber-infrastructure is in private hands.

The Department of Homeland Security must work with the private sector to identify vulnerabilities and encourage cybersecurity improvements. The Department and other parts of the Executive Branch also lead by example and secure their own systems and networks. If the government simply employed better procurement and internal security practices, it would be making significant progress. Today, government systems are so insecure that many in the private sector fear sharing information with the government lest that information be compromised.

In Congress, we must conduct vigorous oversight of the Department of Homeland Security to make sure that the job is getting done. We must also encourage the private sector - from large companies to the home-user - to make cybersecurity a priority. One way to do this is to work with the private sector in understanding insurance and incentives options that could aid in this effort.

Government also has an important role to play in research and education. Congress can assist this effort by providing sufficient funding to existing programs, especially those created by the Cybersecurity Research and Development Act.

One thing we should not do is be overly prescriptive and regulatory. The technology is moving too fast to attempt to legislate prescriptive solutions. The code writers are faster than the legislative process!

What are the responsibilities of the private sector in supplying good software? What are the responsibilities of the end user?

The old cliché: "You are only as strong as your weakest link" comes to mind. Everyone has a role to play. We are all interconnected - from the government to the producers of hardware and software to the corporate enterprise to the home user - so we must work together to protect our cyber infrastructure. I suspect that in the end we are also going to continue to have a greater involvement by *(Continued, Page 11)*

Fighting Cyber Crime at the FBI

The FBI plays two very important roles in cyberspace. First, it is the lead law enforcement agency for investigating cyber attacks by foreign adversaries and terrorists. The potential damage to the United States' national security from a cyber-based attack includes devastating interruptions of critical communications, transportation, and other services. Additionally, such attacks could be used to access and steal protected information and plans. The FBI also works to prevent criminals, sexual predators, and others intent on malicious destruction from using the Internet and on-line services to steal from, defraud, and otherwise victimize citizens, businesses, and communities.

The mission of the Cyber Division is to:

- coordinate, supervise and facilitate the FBI's investigation of those federal violations in which the Internet, computer systems, or networks are exploited as the principal instruments or targets of terrorist organizations, foreign government sponsored intelligence operations, or criminal activity and for which the use of such systems is essential to that activity;

- form and maintain public/private alliances in conjunction with enhanced education and training to maximize counterterrorism, counter-intelligence, and law enforcement cyber response capabilities; and

- until such time as a final decision is made regarding the future role and location of the National Infrastructure Protection Center (NIPC), the FBI will direct and coordinate the Center's mission to protect the Nation's critical information infrastructure and other key assets.

Operation "Web Snare"

Operation Web Snare represents a coordinated initiative targeting an expansive array of Cyber Crime schemes victimizing individuals and industry worldwide. This initiative highlights numerous investigations that have been successfully advanced through cooperation and coordination of law enforcement, and a growing list of industry partners.

Cases included in Operation Web Snare exemplify the growing volume and character of Cyber crimes confronting law enforcement, and also underscores the continuing commitment of law enforcement to aggressively pursue Cyber criminals, both domestically and abroad. Focused efforts to pursue Cyber criminals internationally, has led to the development of enhanced proactive capabilities in several countries, and numerous investigative successes highlighted within this initiative. The development of international resources is closely coordinated with the DOJ, the U.S. State Department and a growing list of E-Commerce industry partners.

Criminal schemes included in this initiative include: criminal spam, phishing, spoofed or hijacked accounts, international re-shipping schemes, Cyber-extortion, auction fraud, credit card fraud, Intellectual Property Rights (IPR), Computer Intrusions (hacking), economic espionage (Theft of Trade Secrets), International Money Laundering, Identity Theft, and a growing list of "traditional crimes" that continue to migrate on-line.

The substantial accomplishments captured in this initiative are attributable to the growing number of joint Cyber-crime task forces established across the U.S. Over the past year, more than 50 such task forces have either been established or significantly augmented with resources from numerous federal, state, and local agencies. Substantial industry partnerships developed in coordination with associations such as the Direct Marketing Association (DMA), the Merchants Risk Council (MRC), the Business Software Alliance (BSA), and the Software and Information Industry Association (SIIA) also contributed significantly to the success of this initiative. Operation Web Snare has been coordinated at the Federal level with the Department of Justice, the Federal Bureau of Investigation, the Internet Crime Complaint Center (IC3), the U.S. Postal *(Continued, Page 6)*

AN UNPRECEDENTED CYBER PARTNERSHIP: "Digital PhishNet" Is Reeling In Cyber Crooks

You're checking e-mail and up pops a message. It looks legit-like it's from your bank, Internet Service Provider (ISP), or another business you deal with all the time. But, it's asking for sensitive financial information-your credit card information, social security number, passwords, etc. "Just click on the link below," the message says. But you're suspicious. Is it a ruse? Have you been "phished"?

Chances are you have.

Over the past year, tens of millions of Americans have been targets of bogus e-mails, web pages, and pop-ups seeking personal financial data, making "phishing" one of the fastest growing cyber crimes around. A word to the wise: err on the side of caution. Don't respond to unsolicited e-mails asking for your financial secrets.

What's being done to stop these scams and find the culprits? Plenty. In fact, the FBI and its partners recently launched a proactive, groundbreaking operation called "Digital PhishNet."

The team includes more than 50 cyber experts from:

- Five major e-commerce and technology companies (like Microsoft and VeriSign).
- Four top ISPs (such as AOL and EarthLink).
- Nine of the top 10 U.S. banks and financial service providers.
- Key federal law enforcement agencies: the Secret Service, the Federal Trade Commission, the U.S. Postal Inspection Service, and the FBI.
- And the National Cyber-Forensics & Training Alliance (NCFTA) in Pittsburgh, which also serves as Digital PhishNet's home base.

The hallmark of Digital PhishNet? Real-time information sharing and analysis.

It works like this: Members of private industry or law enforcement get wind of a scheme. They quickly forward the details electronically to the Digital PhishNet team. The team digs further and makes a preliminary intelligence assessment. Then, it prioritizes the attack based on the universe of threats, comes up with a proactive targeting strategy, and refers the case to appropriate law enforcement agencies. An investigation is launched, with other partners pitching in as needed.

It all happens at lightening speed ... because it has to. Phishers often create and take down these phony sites over the course of just a few days. Since many phishing schemes are launched overseas, the FBI is also working with its international partners. That includes cyber training for law enforcement in places like Nigeria and Hungary, with more planned in the Far East and other areas.

The bottom line? Phishing is already becoming a more dangerous sport. Thanks to Digital PhishNet, arrests have been made in the U.S., Eastern Europe, and South America. Stay tuned to www.digitalphishnet.org for more! ❖

FBI *(Cont. from Page 5)*
Inspection Service, the U.S. Secret Service, the Federal Trade Commission, and the Bureau of Immigration and Customs Enforcement. Numerous state and local law enforcement agencies contributed significantly to this initiative as well. State and Local participation in this effort was amplified in coordination with The National White Collar Crime Center (NW3C).

Operation Web Snare includes more than 150 investigations, in which more than 870,000 victims lost more than $210 million dollars. Through these investigations more than 300 subjects were targeted, resulting in 100 arrests/convictions, 116 indictments, and the execution of more than 130 search/seizure warrants. Although significant in number, these investigations represent only a fraction of the Cyber crime problem, underscoring not only the need for sustained law enforcement focus, but the continuing development of expanded industry partnerships as well. ❖

Extra Territoriality and International Cyber Crime

Kenneth Geers
Naval Criminal Investigative Service

Investigating international cyber crime poses many problems to U.S. law enforcement. Some of these will be very difficult ever to overcome entirely. One of the biggest challenges is the fact that a high degree of anonymity is not difficult to achieve on the Internet. When attribution of an international cyber crime is found, there is often a significant time lag involved. Criminal evidence needs to be secured as quickly as possible, but you can imagine how obtaining evidence for a crime that originated in Russia, but was routed through Nigeria, cannot take place overnight. Compare this to the crime itself, which may have only taken a few milliseconds to commit!

Ideally, we would examine in detail every Internet data packet that crosses our borders, but when they arrive at well over a billion per second, that thought is quickly ruled out. When there is little hope of individually interviewing every person who crosses our borders each day, it is clear that there is not a chance of evaluating each Internet communication either.

When a real Internet crime has been discovered, and the log data exists to prove it (the combination of which is fairly rare), the tedious process of tracing the hack back to its point of origin begins. The obstacles for an international investigator begin to multiply quickly here. Cultural, linguistic, and political barriers can prove insurmountable.

Let's assume that your assiduous network administrators can prove that your network has been cracked, and further that they can point to an Egyptian Internet Protocol (IP) address as the clear source of the heist. What is your next step? Do you pick up the phone and call Cairo, or do you call the FBI? Either way, someone is going to have to speak with a network administrator who may not speak English very well. What are the chances that they will have accurate log data, the expertise to read the logs, the willingness to share it, and the extra time during their work day for your case? By some miracle, let's say that all this works out, but now the trail leads to an Internet connection made to the ISP from China. Ouch. At this point, the process starts all over again.

In this context, it is important to understand that digital evidence is notoriously time-sensitive, and that it can be relatively easy for a smart hacker to quickly destroy the evidence of their crimes. Once your investigator has gone from Cairo to Beijing and back, if only by e-mail and telephone, how long has it been since your company's hack took place?

One of the leading efforts to effect a sea change in this area is the European Cybercrime Convention. European Union (EU) politicians, police and business leaders have billed this as the first comprehensive international treaty to address the commission of electronic crimes. At present, forty-one countries have signed the treaty (including the United States and Russia) and nine have acceded to it through formal ratification. The ultimate goal of the treaty is to harmonize cybercrime laws all over the world. These run the gamut: fraud, child pornography, data protection, and even cyber terrorism. That something needs to be done on the issue of cyber crime is indisputable. The amount of damage done every year easily runs into the billions of dollars, and the problem is an acutely asymmetric one. Take the case of Germany. There, criminal activity committed on the Internet is officially pegged at only one percent of recorded crimes. However, Internet crime is also thought to be responsible for over fifty percent of total financial losses!
(Continued, Page 8)

Kenneth Geers is an Intelligence Specialist in the Cyber Department of the Naval Criminal Investigative Service

Int'l Cyber Crime *(Cont. from Page 7)* The rules of the European Cybercrime Convention (ECC), however, are controversial. At best, they will be difficult to implement. The convention calls on all signatories to cooperate with each other. This includes those countries that have historically had poor relations with one another. Many governments worry that this would leave their citizens' personal information vulnerable to abuse by foreign governments, and that this abuse could occur with inadequate oversight. Privacy groups fear for their civil liberties as well. Internet service providers (ISPs) fear that unwieldy strictures and obligations will be placed upon them.

Beyond these misgivings, will the treaty, if implemented, aid international investigators? In short, only if the treaty works as its authors envisioned. The governments must have the capacity and the desire to work with one another, and in a timely manner. But even then, there will be countries that choose not to participate in the scheme. In effect, those outliers will create major headaches for the Treaty members, because they will be safe-havens for criminals in cyberspace. Member states will be forced into using various forms of coercion in order to get them to cooperate.

The ECC fails to authorize any type of unauthorized cross-border digital searches or seizures, even in the case of hot pursuit. All cooperative scenarios foresee consultation with host-nation officials before any examination or seizure of computer data. While politically palatable, this rule runs the risk of giving cyber criminals the valuable time they need to hide their point-of-origin.

When a real Internet crime has been discovered, and the log data exists to prove it (the combination of which is fairly rare), the tedious process of tracing the hack back to its point of origin begins. The obstacles for an international investigator begin to multiply quickly here. Cultural, linguistic, and political barriers can prove insurmountable.

The rationale for governments to keep their information security affairs in-house is easily understood. The protection of national sovereignty - as well as the privacy rights of a country's citizens (and voters) - almost never needs a vigorous rhetorical defense. The Foreign Relations Law reads thus: "It is universally recognized, as a corollary of state sovereignty, that officials in one state may not exercise their functions in the territory of another state without the latter's consent." Inter- national law prohibits what is known as "extraterritorial jurisdiction," and this includes criminal investigations.

There is sure to be tension, however, between a government's desire to guard its national sovereignty and its desire to prosecute foreign cyber crimes that take place on its own territory. Unauthorized cross-border searches and seizures are likely to be upheld in certain circumstances because it will be seen to have been the only way that certain types of evidence could feasibly have been acquired.

The argument that remote search and seizure is not consistent with international law holds up only to a point. There are analogies to other disciplines, like espionage, that help to shed light on this problem. There are many ways that governments keep track of what is going on inside foreign territory without physically entering that territory that are commonly accepted as normal. Binoculars, surveillance aircraft, satellites, personal interviews and mass media are a few that immediately come to mind. All governments practice these techniques to the extent that they can, and there is no feasible way to stop them. You make the call: are remote searches and seizures of digital evidence closer to a physical intrusion into the territory of another state, or are they closer to satellite pictures taken from a now commonly available remote sensing device?

The year 2000 provides us our best illustration to date. The FBI was hot on the trail of Russian hackers *(Continued, Page 11)*

National Cyber-Forensics and Training Alliance

The National Cyber-Forensics and Training Alliance (NCFTA) began in 2002 as a logical outgrowth of the Pittsburgh High Tech Crimes Task Force, one of the first coalitions of federal, state, and local law high-tech forces established in the nation. A focal point of this project is the primary partnership established among the FBI, the National White Collar Crime Center, Carnegie Mellon University, and West Virginia University.

This core group conducted a survey of industry, government, and academia regarding vulnerabilities to current and evolving cyber threats. The survey results identified overlapping mission goals and resources among the respondents. These results form the basis for NCFTA's mission and directives.

The NCFTA has established an alliance between the public and private sectors. This alliance is comprised of Subject Matter Experts (SMEs) from industry, academia, and government. SMEs from each sector bring specific talents and experiences to the partnership. This allows the NCFTA to adapt itself to meet new threats through a steady influx of personnel and ideas.

The NCFTA is the first partnership of its kind in the nation. Future partnerships will be established in regions where interest exists to combine resources, intelligence, and expertise more effectively. These additional partnerships will be linked together, enhancing the resources fundamental to this project. This coordinated and decentralized approach will empower regional teams with vital information and expertise in a timely and efficient manner.

The NCFTA offers advanced training and degree certification programs, cyber forensics assistance, investigative best practices, and case management. The NCFTA provided key evidence in a Department of Justice sting last fall that led to 160 arrests. The alliance's annual budget of approximately $750,000 is underwritten by the federal government, private industry, and academia. ❖

Mission Statement: The NCFTA provides a neutral collaborative venue where critical confidential information about cyber incidents can be shared discreetly, and where resources can be shared among industry, academia and law enforcement. The Alliance facilitates advanced training, promotes security awareness to reduce cyber-vulnerability, and conducts forensic and predictive analysis and lab simulations. These activities are intended to educate organizations and enhance their abilities to manage risk and develop security strategies and best practices.

Hewlett Packard Announces New Security Software and Trials Conducted through CIP Program

Hewlett Packard recently announced the availability of new software designed to quickly control the spread of viruses across corporate networks and reduce the damage they cause during an attack.

HP also announced that HP Labs, the company's central research facility, has begun collaborating with two prominent partners to test new damage-containment security software aimed at simply and effectively preventing certain viruses from corrupting entire systems. One of these partners is the CIP Program, through which HP Labs is conducting trials of the new software within the School of Public Policy at George Mason University.

The full HP press release can be found at:
http://www.hp.com/hpinfo/newsroom/press/2005/050211a.html.

Investigating and Prosecuting Computer Crimes

(Excerpted from "Computer Security: A Summary of Selected Federal Laws, Executive Orders, and Presidential Directives" by John Moteff, Congressional Research Service)

The **Counterfeit Access Device and Computer Fraud and Abuse Act of 1984** (P.L. 98-473, Title II, §2102(a), 18 USC 1030, as amended) makes certain acts associated with the unauthorized access to computers a federal crime. For example, it is a crime to knowingly gain unauthorized access to a nonpublic federal computer or a computer used by or for the federal government. It is also a crime to knowingly gain unauthorized access to a computer and obtain national security information, financial or credit information, or any information from a protected computer. A protected computer is one used by or for a financial institution, the federal government, or one used in interstate or foreign commerce and communication. It is also a federal crime to knowingly transmit a program, information, code, or command that causes damage to a protected computer. While the Attorney General has the primary authority to enforce federal laws, the Act also specifically states that the United States Secret Service has the authority, as does any other agency with such authority, to investigate the computer-related offenses covered by this section of the Act.

The **USA PATRIOT Act** (P.L. 107-56, §506(a)) amended the above statute by adding that the Federal Bureau of Investigation (FBI) has primary authority to investigate offenses where espionage or national security is involved, except for offenses affecting the duties of the United States Secret Service. Such authorities are to be exercised in accordance with an agreement signed by the Secretary of the Treasury and the Attorney General.

Section 105 of the PATRIOT Act authorizes the Director of the United States Secret Service to develop a national network of electronic crime task forces, modeled on the New York Electronic Crimes Task Force, for the purpose of electronic crimes, including potential attacks against critical infrastructure and financial payment systems.

Section 816 of the PATRIOT Act also authorizes the Attorney General to establish regional computer forensic laboratories to provide forensic examinations with respect to seized or intercepted computer evidence related to criminal activity, to provide training and education to other federal, state, and local law officials, and to assist other federal, state, and local law officials.

Some of the ground-rules for investigating computer crimes are found in the **Electronic Communications Privacy Act** (P.L. 99-508, USC Chapters 119,121, 206). A number of these were modified in Title II of the USA Patriot Act. For example, prior to the amendments, tracking computer hackers via computer logs across jurisdictional areas required separate court orders from each jurisdiction. The USA Patriot Act allows investigators to get a single court order from any court of competent jurisdiction. ❖

Romania *(Cont. from Page 2)*
Romanian Cyber Crime law carries penalties of up to 15 years for violations. The new law, derived from the European Convention, is an indication of Romania's determined efforts to embrace the assistance and emulate the programs of other nations within the broader community of European states.

In light of future EU incorporation, computer crime demanded immediate attention. The creation of a U.S.-Romanian computer crime task force enabled officials to formally address the issue. By 2003, the Center for Expertise and Response to Security Incidents (CERIS or *Centrul de Expertiza si Raspuns pentru Incidente de Securitate*) was operational. Based within the Romanian Ministry of Communications and Information Technology, CERIS marked the first significant step to countering a problem that has threatened the country's future integration into the economies of the United States and Western Europe. ❖

Lofgren *(Cont. from Page 4)*
ISPs relative to home user security. Indeed, the steps taken in a recent month by some ISPs to integrate AV into their services shows this trend.

As you might expect, the technology sector is generally well ahead of other parts of the economy in caring about cybersecurity. However, "Old Economy" industries are, today, as reliant on technology as the companies in Silicon Valley, my home. Yet, many of the companies in these sectors appear to be less aware than they should be about their vulnerabilities. And, of course, successful attacks against them would have quite an important and adverse impact on our American economy as a whole. ❖

Int'l Cyber Crime *(Cont. from Page 8)*
who had cracked various computer networks around the country, including banks and ISPs, in order to steal credit card numbers. The point-of-origin was determined to be Russia, but Russian assistance in the investigation was not forthcoming. Therefore, the FBI decided to act on its own. With a U.S. search warrant in hand, it tricked one of the Russian suspects into traveling to Seattle, where it used a keystroke logger to gain his username and password to a secret stash back in Russia. The FBI then proceeded to log on and download highly incriminating evidence.

Said hacker gang was responsible for fraud on a massive scale, involving the theft and use of many thousands of American credit card numbers. In a case like this, in which the cost to U.S. citizens is substantial, and when there is no help offered by the foreign country, what should the response be? The two FBI agents were given the Director's Award for Excellence, and the FBI publicly praised its field office's first successful "extra-territorial seizure." ❖

The CIP Program is directed by John A. McCarthy, a member of the faculty at George Mason University School of Law. The CIP Program works in conjunction with James Madison University and seeks to fully integrate the disciplines of law, policy, and technology for enhancing the security of cyber-networks, physical systems and economic processes supporting the nation's critical infrastructures. The CIP Program is funded by a grant from The National Institute of Standards and Technology (NIST).

The CIP Report is published by Zeichner Risk Analytics, LLC on behalf of the CIP Program. ZRA is the leading provider of risk and security governance knowledge for senior business and government professionals. ZRA's vision is to be a consistent and reliable source of strategic and operational intelligence to support core business processes, functions, and assurance goals.

If you would like to be added to the distribution list for *The CIP Report*, please click on this link:
http://techcenter.gmu.edu/programs/cipp/cip_report.html.