International Computer Crime Conference
"Internet as the Scene of Crime"

Oslo, Norway
May 29-31, 2000

Remarks of James K. Robinson

Good Morning. My name is Jim Robinson. I am the Assistant Attorney General for the Criminal Division at the United States Department of Justice in Washington, D.C. I supervise approximately 450 federal prosecutors in Washington who enforce a diverse set of laws, including those that deal with organized crime, fraud, child pornography, terrorism, narcotics, money laundering, and computer crime. We also serve as the primary point of contact for assisting federal and state prosecutors who work with our international law enforcement partners concerning extradition and requests for mutual legal assistance. We also work closely with the 93 U.S. Attorneys' offices and over 4,000 federal prosecutors located throughout the United States.

I want to thank our colleagues from the Norwegian government for all their hard work in making this event possible. They have expended an enormous amount of energy and resources. My government is extremely grateful to them. I especially want to thank ØKOKRIM and the Norwegian Ministry of Justice who have contributed greatly to the success of this Conference.

I am honored to be here. In this room are the experts and professionals - both investigators and prosecutors - who are working to ensure that law enforcement agencies around the world are equipped to combat computer crimes.
Computer crime is global in scope. That 33 nations are represented at this conference attests to this fact. This conference provides us a valuable forum to discuss how our nations can cooperate to address the challenges and policy issues created by computer crime.

TYPES OF COMPUTER CRIMES

In February of this year, many of my nation's most prominent Internet commerce sites were temporarily crippled by a malicious computer attack. These "Denial of Service Attacks" shut down such sites as Yahoo, CNN, E-Bay, and several others. Just a few months later, the "I Love You" and "New Love" viruses struck, damaging computers around the world and potentially causing a tremendous amount of financial losses. These attacks demonstrate how dependent the world has become on computers and computer networks.

We have entered the Information Age, where information technologies have been integrated into virtually every aspect of business and society. This integration is posing new challenges for all of us in law enforcement. Law enforcement agencies in the

United States, and I'm sure in your nations as well, are seeing computers being used for criminal behavior in three ways.

. First, a computer can be the target of an offense. When this occurs, a computer's confidentiality, integrity, or availability is attacked. That is services or information are being stolen, or victim computers are being damaged. The denial of service attacks that were experienced by numerous Internet sites earlier this year and the recent proliferation of the "I Love You" virus and its variants are but a few examples of this type of computer crime.

. Second, a computer can be used as a tool for committing criminal behavior. This category includes those crimes that we in law enforcement have been fighting in the physical world but now we are seeing with increasing frequency on the Internet. These crimes includes child pornography, fraud, intellectual property violations, and the sale of illegal substances and goods online.

. Third, a computer can be incidental to an offense, but still significant for our purposes as law enforcement officials. For example, pedophiles might store child pornography and drug traffickers and other criminals may store business contact information on their computers.

TECHNICAL, LEGAL, AND OPERATIONAL CHALLENGES

All three types of crimes involving computers are creating challenges for all 33 of our nations, as well as the rest of the world. In the United States we are devoting significant resources to identifying these challenges and formulating a sound legal and policy framework in which to address them. This past March, Attorney General Janet Reno released the report "The Electronic Frontier: The Challenge of Unlawful Conduct Involving the Use of the Internet," which was drafted by President Clinton's Working Group on Unlawful Conduct on the Internet. This extensive report highlights the significant challenges created by cyberspace for law enforcement - not only in the United States, but throughout the world. If you are interested in reading the report, it is available on the Internet at www.cybercrime.gov . As the report states, the needs and challenges confronting law enforcement "are neither trivial nor theoretical."

I see the challenges that law enforcement agencies face in our battle with cybercrime generally being divided into three categories:

1) Technical challenges that hinder law enforcement's ability to find and prosecute criminals operating online;

2) Legal challenges resulting from laws and legal tools needed to investigate cybercrime lagging behind technological structural, and social changes; and

3) Operational challenges to ensure that we have created a network of well-trained, well-equipped investigators and prosecutors who work together with unprecedented speed - even across national borders.

Private Sector & Consumer Involvement

Before I discuss these challenges in more detail, let me say that governments, even if we all work together, will not be able to meet these challenges alone. We need the private sector to be involved. In fact, the private sector must take the lead in certain areas, especially in protecting private computer networks, through more vigilant security efforts, information sharing, and, where appropriate, through cooperation with government agencies. The private sector has the resources, the technical ability, and the trained personnel to ensure that, as technology continues to develop and change rapidly, the Internet is a safer place for all of us. As such, the private sector must take the lead on improving security practices and the development of a more secure Internet infrastructure.

In addition, we need the assistance of the consumer, the everyday user of computer systems, to ensure that safeguards are taken and that sound practices are followed. The best infrastructure and most secure means of electronic commerce will be ineffective if the users of the technology, that is, all of us, don't follow the basic "rules of the road."

That being said, even if companies and consumers do everything they can do to protect the Internet, law enforcement must be properly equipped, trained, and organized to fight cybercrime. There is little doubt that there will be instances where the practices and safeguards fail. As we all know, criminals rob banks even though banks use effective security measures. When practices and safeguards fail, we must be ready - ready to investigate and ready to prosecute cybercriminals - so that we can stop their criminal activity, punish them, and deter potential cybercriminals.

Technical Challenges

When a hacker disrupts air traffic control at a local airport, when a child pornographer sends computer files over the Internet, when a cyberstalker sends a threatening e-mail to a school or a local church, or when credit card numbers are stolen from a company engaged in e-commerce, investigators must locate the source of the communication. Everything on the Internet is communications, from an e-mail to an electronic heist. Finding an electronic criminal means that law enforcement must determine who is responsible for sending an electronic threat or initiating an electronic robbery. To accomplish this, law enforcement must in nearly every case trace the "electronic trail" leading from the victim back to the perpetrator. Tracing a criminal in the electronic age, however, can be difficult, especially if we require international cooperation, if the perpetrator attempts to hide his identity, or if technology otherwise hinders our investigation.

When I first became a federal prosecutor over twenty years ago, law enforcement rarely needed to be concerned about fighting crime across international borders. This is no longer the case. Those of us in this room know too well the daily challenges we face when combating criminals that do not respect national borders. As networked communications and e-commerce expand around the globe, businesses and consumers become more and more vulnerable to the reach of criminals. The global nature of the Internet enables criminals to hide their identity, commit crimes remotely from anywhere in the world, and to communicate with their confederates internationally. This can happen in nearly any type of crime, from violent crime, terrorism, and drug-trafficking, to the distribution of child pornography and stolen intellectual property, and attacks on e-commerce merchants.

Criminals can choose to weave their communications through service providers in a number of different countries to hide their tracks. As a result, even crimes that seem local in nature might require international assistance and cooperation. For example, a computer hacker here in Oslo might attack the computers of a corporation located only a few miles away. Yet, it is very possible that the ØKOKRIM might have to go to U.S., French, or Danish law enforcement officials for help in finding this criminal. This would happen if the hacker routes his communications through providers in New York, Paris, and Copenhagen before accessing his victim's computer.

Naturally, criminals like these, who weave communications through multiple countries, present added complexities to governments trying to find criminals. Mutual legal assistance regimes between governments anticipate sharing evidence between only two countries, that is, the victim's country and the offender's country. But when a criminal sends his communications through a third, or fourth, or fifth country, the processes for international assistance involve successive periods of time before law enforcement can reach data in those latter countries, increasing the chances the data will be unavailable or lost, and the criminal will remain free to attack again.

At the same time, the global nature of the Internet makes it easy for a criminal armed with nothing more than a computer and modem to victimize individuals and businesses anywhere in the world without ever setting foot outside his or her home. The February denial of service attacks serve as a good example of how easy it can be for cybercriminals to commit crimes across borders, as well as how technical and infrastructure challenges have made international cooperation a necessity.

In those attacks, I am happy to say, U.S. law enforcement was able to reach out after hours to our Canadian counterparts and receive timely and expert assistance. I believe our joint investigation, which culminated in charges against a Canadian citizen, will serve as a model in other cases where international cooperation is necessary.

Even with our success in the denial of service attacks, I recognize that our nations face many international challenges in the battle against computer crime. While the Internet may be borderless, national boundaries exist for law enforcement and we must respect the sovereignty of each other's countries. We increasingly are dependent on mutual cooperation from other countries in investigating and prosecuting computer crimes. Simply stated, cybercriminals know no national boundaries, and the multi-jurisdictional nature of cybercrimes requires a new multilateral approach to investigations and prosecutions.

We saw this in the February denial of service attacks and we are experiencing it again in the investigation of the dissemination of the "Love Bug" virus. This virus, wreaked havoc on computers around the world, probably in most of our nations, and caused tremendous damage. Within a day or so, international law enforcement agencies, as well as high-tech companies in the private sector, began focusing their investigations on the Philippines.

The Philippine National Bureau of Investigation, assisted by the U.S. Federal Bureau of Investigation, is pursuing several leads. While I cannot comment directly on the ongoing investigation, I can say that the United States, as I am certain is the case for other nations that were victimized by the virus, stands committed to assisting the Philippine government and to ensuring that the perpetrators of this crime are brought to justice.

To succeed in identifying and tracing global communications, we must work across borders, not only with our counterparts throughout the world, but also with industry, to preserve critical evidence such as log files, e-mail records, and other files, and we must be able to do so quickly, before such information is altered or deleted. If we cannot get this information quickly, the investigation may grow cold.

At the same time, we often need to trace transmissions in real time, during an actual communication. This can be technically difficult, since many communications technologies are not designed to facilitate tracing. The victim's computer often only receives the address of the computer connected directly to it, not the address of the communication's source, and this address can be false or temporarily hijacked. The infrastructure of the Internet does not normally provide an automated mechanism for identifying the true source. Therefore, investigators will often need to contact individually each communications provider in the chain, to determine the source of the prior connection. When these investigations cross national borders, they often cross time zones as well. This often means that it is nighttime in at least one jurisdiction, and critical personnel may not be at work.

While less sophisticated cybercriminals may leave electronic "fingerprints," more experienced criminals know how to conceal their tracks in cyberspace. With the deployment of anonymous software, it is increasingly difficult and sometimes impossible to trace cybercriminals. At the same time, other services available in some countries, such as pre-paid calling cards, lend themselves to anonymous communications. All of these technologies make identifying criminals more difficult, even though they have other benefits.

There are countless other technical challenges we face, like those stemming from Internet telephony, strong encryption, and wireless and satellite communications. The technological advances in electronic commerce and communication that have led to the explosive growth of the Internet have also made it possible for international criminals and terrorists to target victims in all our countries in unprecedented ways. In an age of anonymous, wireless, and encrypted communications, how is law enforcement to identify and prosecute those who would do harm to our citizens and businesses? What do we do when criminals located domestically use satellite and wireless communications that travel exclusively through gateways located in other countries?

Legal Challenges

The second type of challenge we face as investigators and prosecutors is in the legal arena. Deterring and punishing computer criminals requires a legal structure that will support detection and successful prosecution of offenders. Yet the laws defining computer offenses, and the legal tools needed to investigate criminals using the Internet, often lag behind technological and social changes, creating legal challenges to law enforcement agencies. In addition, some countries have not yet even adopted computer crime statutes.

All nations must take the threat of cybercrimes seriously. Hacking and virus-writing and proliferation are not simple pranks, but injuries that have significant security and financial consequences. At a time when the number of crimes carried out through the use of computer technology is increasing at an alarming rate, it is especially important that law enforcement officials around the world demonstrate that such crimes will be punished swiftly and with an appropriate degree of severity. When one country's laws criminalize high-tech and computer-related crime and another country's laws do not, cooperation to solve a crime may not be possible. Inadequate regimes for international legal assistance and extradition can therefore, in effect, shield criminals from law enforcement. As France's President Jacques Chirac stated at a G8 cybercrime conference in Paris a few weeks ago, "what we need is the rule of law at [an] international level, a universal legal framework equal to the worldwide reach of the Internet."

For those countries that do have computer crime statutes, they must also have appropriate procedural laws in place to investigate crimes. We must recognize that technology is constantly changing and that procedural laws need to be updated. For example, tracing criminals online in real time can be difficult in some countries because they have not yet adopted mechanisms to obtain traffic information in real time.

In certain cases, countries might want to reconsider both their substantive and procedural laws. For example, some countries have laws that require telecommunications carriers and ISPs to routinely delete data that may be critical to an investigation. These countries may want to review these laws to determine how these deletion requirements balance against the need to provide a safe and secure Internet.

Operational Challenges

In addition to technical and legal challenges, law enforcement agencies around the world face significant operational challenges. The complex technical and legal issues raised by computer-related crime require that each jurisdiction have individuals who are dedicated to high-tech crime and who have a firm understanding of computers and telecommunications. The complexity of these technologies, and their constant and rapid change, mean that investigating and prosecuting offices must designate investigators and prosecutors to work these cases on a full-time basis, immersing themselves in computer-related investigations and prosecutions.

We have taken this challenge seriously in the United States and have made specific efforts to create specialized investigative and prosecutorial offices at the federal level. At the Department of Justice, the cornerstone of our prosecutor cybercrime program is the Criminal Division's Computer Crime and Intellectual Property Section, known as CCIPS. CCIPS was founded in 1991 and has grown from five attorneys to twenty attorneys today. CCIPS works closely on computer crime cases with Assistant United States Attorneys known as "Computer and Telecommunications Coordinators" (CTCs) in each of our U.S. Attorneys' Offices located around the United States. Each CTC is given special training and equipment, and serves as his or her office's expert in computer crime cases. Increasingly, these prosecutors are working with state and local law enforcement as well.

On the investigative side, the National Infrastructure Protection Center was created in 1998 to coordinate the FBI's investigation of computer crimes. The NIPC currently has approximately 100 investigators, computer scientists, and analysts working on computer crime matters. In addition, the FBI has almost 200 agents located in FBI field offices through the United States who are assigned to investigate computer crimes.

I believe that every country should have dedicated high-tech crime units that can and will respond to a fast-breaking investigation and assist other law enforcement authorities faced with computer crimes.

Given the quickly evolving nature of computer technology, our nations must also continue to increase their computer forensic capabilities, which are so essential in computer crime investigations. Twenty years ago, a new police officer was given a gun, a flashlight, and a notepad. When that officer retired, the three items would be returned to the police department, and the only intervening equipment expenses would have been replacement bullets, batteries, and note paper. Today, keeping pace with computer criminals means that law enforcement experts in this field must be properly equipped with the latest hardware and software.

In addition, because of the speed at which communications technologies and computers evolve, prompting rapid evolution in criminal tradecraft, experts must receive regular and frequent training in the investigation and prosecution of high-tech cases.

CYBERETHICS

As we move to meet technical, legal, and operational challenges, we should not forget to educate our youth and others in society that computer hacking and virus dissemination is not only illegal, but ethically wrong. Regardless of which country we call home, most of us know that it is wrong to break into our neighbors' houses and steal things or damage their property. Yet, it doesn't seem that our youth today are being taught that the same principles apply to their behavior on computers and the Internet. Indeed, in certain instances, unethical online behavior has been glorified. In the United States, the Department of Justice is working with the private sector in an effort to rectify this situation. Approximately a year ago, in a joint private-public effort, we formed the Cybercitizen Partnership, an initiative designed to educate and raise awareness of computer responsibility. It is important for all countries to think about how they, too, can encourage ethical cyber-behavior among their citizens.

INTERNATIONAL EFFORTS

I noticed that included on our agenda for this week is a presentation about the efforts of the Council of Europe. The Council of Europe's Draft Convention on Cyber Crime breaks new ground in the area of computer crime as the first multilateral instrument drafted specifically to address the problems posed by the spread of criminal activity in computer networks. I understand that the draft Convention is now available to the public and the Council has invited comments from industry and others prior to the completion of drafting this December.

The United States Department of Justice welcomes the Council of Europe's efforts to improve mechanisms to expedite mutual assistance in the investigation of high-tech crimes, promote and harmonize policies and practices for improved Internet security, and to ensure that law enforcement agencies are empowered with the requisite procedural authority to obtain electronic evidence within their territory. These actions go far in assisting us in the investigation and prosecution of computer crimes.

In addition to supporting many of the efforts of the Council of Europe, the Department of Justice is interested and involved in high-tech discussions at the G8. Just two weeks ago, I headed the U.S. delegation at a meeting in Paris at which the governments and industry of the G8 nations, along with representatives of other nations and groups, sat down to discuss how we can work together to identify the source of criminal behavior on the Internet, as well as tracing those responsible for committing crime over the Internet.

Indeed, the G-8 nations have been interested in cooperation on cybercrime since at least December 1997, when the G-8 Justice and Interior Ministers met in Washington, DC and adopted 10 Principles and a 10-point Action Plan to fight cybercrime. When the Heads of State for the G-8 nations endorsed the Principles and Plans a few months later, it was the first time that a group of Presidents and Prime Ministers agreed to a joint plan to fight cybercrime.

One of the things that has come out of the G-8's efforts is the 24/7 network, which requires participating countries to designate a 24 hour, 7 day per week Point-of-Contact for the purposes of providing investigative assistance. Currently, almost 20 countries are participating in the network. We are working to further develop the network so that we are better prepared to address crimes committed using computer networks wherever and whenever they occur. If your country is not involved in the network, I encourage you to learn more about it and get involved with this worthy effort.

I know that the European Union also has turned its attention to high-technology and computer crime issues. The United States looks forward to increased dialogue with the EU on these matters.

CONCLUSION

The U.S. delegation looks forward to learning from the 33 other nations represented at this conference and to finding ways we can work together to reduce crime on the networks which have become too important to us all.