Keynote Address by

U.S. Attorney General Janet Reno on

High-tech and Computer Crime

Delivered at the Meeting of the P-8 Senior Experts' Group on Transnational Organized Crime

Tuesday, January 21, 1997

Chantilly, Virginia

P R O C E E D I N G S

ATTORNEY GENERAL RENO: Thank you, Mark. I'm very touched by that introduction and I hope I can live up to it. I want to welcome you all to the United States for this first Plenary session of 1997. I am very pleased to be with you today.

Not only is this meeting the first P-8 meeting under the U.S. Presidency, it is the first multilateral meeting of President Clinton's second Administration.

As you know, yesterday the President took the oath of office for his second term. His re-election brings with it the opportunity for me to continue to work with international and domestic law enforcement to bring security to the citizens of our countries, and I consider this a very special privilege.

Besides the historic significance of

this day, I want to share with you the excitement and the enthusiasm I feel about and toward the P-8. I view this group like no

other: The P-8 countries are a special group made up of the world's most powerful democracies. We are global leaders in so many ways -- economically, technologically, legally, and politically. Our small number allows us to act quickly, and our unique membership offers an opportunity to lead the world community that is rarely found in our history. And we are often on the cutting edge -- for example -- in responding to international terrorism, to international money laundering, to precursor chemicals. This group has so much promise. Through your work, giant strides are being made in several critical areas that have significant global implications.

No area of criminal activity is more on the cutting edge or has greater global implications than crime involving technology

and computers. The importance of emerging technologies and the significance of global computer networks cannot be overstated. If properly developed and properly protected, they

will be used in virtually all personal communications, financial transactions, information sharing, medical care, and a myriad of other applications. It is, indeed, a very exciting time.

But while new technologies allow us to do things that were previously impossible, they can also be misused in creative ways to threaten public safety and national security. The same technologies that facilitate lightning-fast and ultra-reliable transactions between computers can be misused by hackers, that is, by those who access computers without or in excess of authority. They can access confidential information, steal economic data, disrupt telephone networks, and interfere with the delivery of government and other vital

services.

So while the information age holds great promise, law enforcement has a responsibility to ensure that the users of networks are not victimized in new ways.

To protect honest, law abiding citizens, law enforcement must keep pace with advances in computer and telecommunications technologies. We must work to ensure that the international law enforcement community can keep pace with the criminals. This is especially true in the case of computer offenses, which differ from traditional crimes in a number of ways and, as a result, create new and very challenging problems:

First, international computer crimes are easier to commit. Hackers are not hampered by the existence of international boundaries, since information and property can be transmitted covertly via telephone and data networks. A hacker needs no passport and

passes no checkpoints. He simply types a command to gain entry. And there is little need for manpower since a sole hacker, working alone, can effectively steal or erase as much information as he can read, or he can cause extensive damage to global networks.

Secondly, until recently, computer crime has not received the emphasis that other international crimes have engendered. Even now, not all affected nations recognize the threat it poses to public safety or the need for international cooperation to effectively respond to the problem. Consequently, many countries have weak laws, or no laws, against computer hacking -- a major obstacle to solving and to prosecuting computer crimes.

Thirdly, law enforcement faces new procedural challenges, many of which are impossible to address without international consensus and cooperation. Consider, if you will, merely locating a hacker whose

transmission passes from his computer to a local service provider, then through a telephone network, then crosses an ocean via satellite, and then passes through a university computer on its way to a corporate victim. To make matters worse, this hacker could be in his car, using wireless communications. How do we

go about finding this individual? How do we collect the evidence and preserve it in a way that will be useful at trial?

Fourth, law enforcement will be faced with significant technical challenges, such as the widespread use of encryption. In such cases, we will have to find innovative and effective ways to preserve government access to the plain text of encrypted data. We can do this, in part, by supporting international efforts and national policies which promote the development of the emerging key management infrastructure and the use of products which allow for data recovery, as well as by

assisting each other in this very difficult area.

I think that these threats and these problems call for the particular experience and the expertise of this group. While important work in the high-tech area is being done under the auspices of other organizations, one thing that sets the P-8 apart from other multilateral

groups is its common-sense focus on practical solutions.

And the great thing about practical solutions is that they usually produce real results. Since computer crime is so important to all of our interests, there are several areas that I hope P-8 Experts will address. First, we need adequate laws which will allow us to prosecute hackers and other computer criminals. Second, we need the technical ability to find these individuals, wherever located. Third, we must develop legal procedures that permit timely cooperation in

the collection of evidence. And fourth, we need to train law enforcement personnel and devote these technically literate experts to the task at hand.

When countries have inadequate legal structures to combat computer crimes, they provide safe havens for computer criminals, and they can create a major obstacle to obtaining international assistance in multijurisdictional

cases. As you know, in 1990, the Council of Europe recommended that European nations adopt harmonious computer crime laws. As a result, several P-8 countries have enacted new laws and joined international efforts to encourage other countries to enact or to strengthen their computer crime laws. However, much work remains to be done in this area.

We need to reach a consensus as to which computer and technology-related activities should be criminalized, and then commit to taking appropriate domestic actions.

This would also aid in providing the inevitable legal assistance required to investigate and prosecute these cases. I think it is also important to think about a global legal support regime, which could be used to avoid ad hoc approaches to multiple prosecutions. The unique nature of computer crimes and the unusual problems that can result would make such a regime very useful. Further, it would provide practical solutions as countries

determine the best place for a prosecution, the order of prosecutions in a case where multiple countries are affected, and the most fair way to vindicate interests when a crime affects a large number of nations.

When a hacker attacks, the first investigative step is to locate the source of the attack. To do so requires tracing the electronic trail from the victim back to the attacker. However, in today's communications environment, one telecommunications carrier

does not carry a communication from end to end. As in the example I mentioned before, a hacker's communication will pass through an array of carriers, often in less than a second, and tracing the electronic trail from victim back to attacker may be difficult or impossible unless the hacker is actually on-line.

One practical solution that our technologically advanced countries should pursue is maintaining access to source information for each link in the chain of

transmission. Some countries, including the United States, have required that technical standards be adopted which ensure that "call set-up information" for normal telephone calls is accessible, so that the source of the call can be identified. I think it would be productive for P-8 Experts to consider whether all carriers should carry this kind of information, whether other communications technologies should be similarly designed, and

what would be required for countries to share this information with one another. This is a critical time for this issue, as all of us are upgrading our telecommunications systems, because it is far easier to build such requirements into new machines rather than to retro-fit existing equipment.

Finding a criminal who plies his craft through an array of carriers becomes much more challenging when wireless communications are used. In the past, when a perpetrator used a phone to commit a crime, law enforcement

could easily find out the exact location that the call came from. They could find out the name of the person who was being billed for the phone line, because the caller would be physically attached to a telephone wire. But today, mobile phones can allow an individual to commit crimes while roaming around a city or even a country.

Even identifying the owner of a

particular mobile phone may be difficult, because mobile phones can be altered to transmit phony identifying information. Here, as in most of the areas we discuss, governments would be well-served to work on this problem with the help of industry. Our technical experts tell us that there are practical solutions to the problems created by wireless communications, such as encouraging the encryption of cellular electronic identifiers. I hope that P-8 Experts will work to see that law enforcement is not overtaken by technology in this area, but instead uses technology to

thwart crime.

As the globalization of computer networks continues, and as computer criminals become more sophisticated, law enforcement increasingly will need timely access to computer or telecommunications information in all our countries. Up until this point, our regime of mutual legal assistance has served

our countries well. But in a hacker case, the trail of evidence sometimes ends abruptly and permanently as soon as the hacker goes off-line. We should consider whether mutual legal assistance treaties and letters rogatory need to be supplemented with procedures that will facilitate the immediate collection and review of evidence, or whether other avenues should be explored. As mechanisms are developed, specially trained lawyers within countries' Central Authorities may be necessary to ensure rapid response to requests for assistance, particularly while a hacker is on-line. Again, the experience and the

expertise of the P-8 makes it well-suited to tackle these very difficult problems. Practical solutions are out there -- we must work together to find them.

One idea I believe worthy of consideration is formalizing international expedited procedures that protect electronic

evidence on foreign soil from alteration or destruction. These could be in the form of "preservation of evidence requests," or "protected seizures," whereby an international request freezes a scene until a domestic judicial search mechanism can be used. Just like technological advances are the product of creativity and ingenuity, our legal work in this area must likewise be imaginative and forward-leaning.

Also in the area of evidence collection, I encourage this group to address the issues involved in analyzing electronic evidence -- evidence which can be easily altered or destroyed. We must be able to

analyze this evidence in ways that preserve its integrity and make its authenticity irrefutable, both for purposes of domestic prosecution and international cooperation. The ease with which digital evidence can be manipulated has already led to the development

of scientific protocols for searching computers and for analyzing data. But we now must strive to ensure that such procedures are internationally accepted.

None of the advances I have discussed are possible without ensuring that law enforcement personnel are capable of addressing high-tech crime by understanding two emerging and converging technologies simultaneously: Computers and telecommunications. The complexity of these technologies, and their constant and rapid change, suggest that countries need to designate investigators and prosecutors to receive appropriate and ongoing training. They, in turn, need to work these cases on a full-time basis, immersing

themselves in computer-related investigations and prosecutions. Efforts along these lines will dramatically expand enforcement capabilities to solve high-tech crimes. I hope that when you return home, each of you will

strongly advocate devoting significant resources to this area, and that we can share our expertise through international training and coordination efforts.

The issues confronting us are very, very difficult, but we can solve them. What will make it all come together in a cohesive way is law enforcement's continued willingness to recognize the new challenges that lay ahead in cyberspace. Whether the challenge is protecting trade secret information, defending intellectual property rights, prosecuting an international hacker, if we do our job right, the people of the world will enjoy the benefits of the information age without becoming its victims.

In closing, I pledge to you my full

support in this very critical area. I consider high-tech crime to be one of the most serious issues demanding my attention, and I am doing everything in my power to ensure that the

United States actively responds to these challenges. I have instructed Mark Richard to keep me apprised of your work, and I would enjoy the opportunity to contact my counterparts in your countries, if and when the need arises. In fact, this past November, I discussed the threat of high-tech crime with the British Home Secretary, Michael Howard, and he enthusiastically pledged his support to P-8 efforts in this area. Likewise, our Deputy Attorney General had a similar meeting with the German State Secretary of the Interior, Professor Doctor Kurt Schelter, in October of last year. It's an old cliche, but united we stand; divided we fall, and we look forward to working with you in every way we can to address this very important and very complex issue.

Thank you.