

**Meeting of Justice and Interior Ministers of The Eight
December 9-10, 1997**

COMMUNIQUÉ

**WASHINGTON, D.C.
DECEMBER 10**

At the Summit of The Eight in Denver, our Heads of State and Government directed us to intensify our efforts to implement the forty recommendations of the Summit of Lyon, in order to combat transnational organized criminal activity posing an ever-greater threat to the individual and collective security of our citizens. With increased international movement by organized criminal groups and their use of new global communications technologies, the protection of our citizens' safety, traditionally a domestic concern, requires unprecedented levels of international cooperation. Our responsibility is not only to react to the activities of organized criminal groups, but also to anticipate and prevent their growth.

We meet today at the Ministerial level to agree upon a program of specific actions designed to accomplish two critical tasks: enhancing our abilities to investigate and prosecute high-tech crimes and strengthening international legal regimes for extradition and mutual legal assistance to ensure that no criminal receives safe haven anywhere in the world.

With regard to high-tech crime, we must start by recognizing that new computer and telecommunications technologies offer unprecedented opportunities for global communication. As nations become increasingly reliant upon these technologies, including wireless communications, their exploitation by high-tech criminals poses an ever-greater threat to public safety. This threat takes at least two forms. First, sophisticated criminals are targeting computer

and telecommunications systems to obtain or alter valuable information without authority and may attempt to disrupt critical commercial and public systems. Second, criminals, including members of organized crime groups and terrorists, are using these new technologies to facilitate traditional offenses. Clearly, the misuse of information systems in these ways poses a serious threat to public safety.

National laws apply to the Internet and other global networks. But while the enactment and enforcement of criminal laws have been, and remain, a national responsibility, the nature of modern communications networks makes it impossible for any country acting alone to address this emerging high-tech crime problem. A common approach addressing the unique, borderless nature of global networks is needed and must have several distinct components.

Each country must have in place domestic laws that ensure that the improper use of computer networks is appropriately criminalized and that evidence of high-tech crimes can be preserved and collected in a timely fashion. Countries must also ensure that a sufficient number of technically-literate, appropriately-equipped personnel are available to address high-tech crimes.

Such domestic efforts must be complemented by a new level of international cooperation, especially since global networks facilitate the commission of transborder offenses. Therefore, consistent with principles of sovereignty and the protection of human rights, democratic freedoms and privacy, nations must be able to collect and exchange information internationally, especially within the short time frame so often required when investigating international high-tech crimes.

The development of effective solutions will also require unprecedented cooperation between government and industry. It is the industrial sector that is designing, deploying and maintaining these global networks and is primarily responsible for the development of technical standards. Thus, it is incumbent on the industrial sector to play its part in developing and distributing secure systems that, when accompanied by adherence to good computer and personnel security practices, serve to prevent computer abuse. Such systems should also be designed to help detect computer abuse, preserve electronic evidence, and assist in ascertaining the location and identity of criminals.

To meet the challenges of the information age, we have agreed to ten Principles and a ten-point Action Plan, annexed to this Communiqué. We direct our experts to promote these Principles throughout the international community and take forward the Action Plan without delay.

Another core area of concern is mutual legal assistance and extradition. We reiterate the fundamental importance of either returning our nationals for trial in the country in which the crime was committed or, where that is not possible, conducting effective domestic prosecutions in lieu thereof. Those of us that conduct domestic prosecution of our nationals in lieu of extradition agree to pursue such prosecutions with the same commitment of time, personnel and financial resources as are devoted to the prosecution of serious crimes committed within our own territory.

We recognize that the need for enhanced cooperation in extradition and mutual assistance is particularly acute with respect to high-tech crime and other areas of emerging significance. We commit to remove impediments in existing cooperation regimes by such means as

approaching issues of dual criminality with flexibility, and we will ensure that serious computer abuses have criminal penalties sufficient to make them extraditable. We also commit to enhance coordination among States in multi-jurisdictional cases, so as to minimize conflicts and duplications in investigations and prosecutions, consult as to where best to prosecute, and allocate responsibility for gathering and sharing evidence.

We are also convinced that we must further enhance our abilities to obtain testimony from witnesses located abroad for use in criminal proceedings in our States. We agree to intensify our efforts to use video-link technology as a means of securing testimony or statements from a witness located abroad. Where possible, we will locate or establish facilities with technical video-link capability, allow the use of video-link as a form of mutual assistance to other States and provide for the punishment of perjury committed during video-link transmissions.

We emphasize that these agreed-upon cooperation measures can be used by all countries to enhance international cooperation in combating transnational organized crime. Our experts will review annually our implementation at the national level of these international legal cooperation measures. We also urge all States to adopt the recommendations of the Summit of Lyon pertaining to international legal cooperation and the best practices agreed upon by our experts to implement them.

We direct our experts to focus their future work on the following areas: Continued examination of the use of video-link technology and confiscation and sharing of assets obtained through criminal activity; identification of additional measures that would enhance cooperation in areas of emerging significance; ways to further promote acceptance by other members of the

international community of the principles set forth in the above recommendations and practical actions; and coordination among The Eight on the possible elaboration of a U.N. organized crime convention.

In addition to taking action on high-tech crime and mutual legal assistance, we further direct our experts to pursue their work in implementing comprehensive action against transnational organized crime, as mandated by the Denver Summit. Therefore, we welcome the continued efforts of our experts to develop cooperative strategies and policies to combat major transnational criminal organizations and to implement joint operational projects to target such organizations and their criminal activities. We will continue to work together to combat international firearms trafficking and other forms of cross-border crime and smuggling and to address the financial aspects of organized crime.

In conclusion, we recognize the urgent need to make rapid progress in these areas and will take the steps necessary to ensure protection from the physical and financial predation of transnational organized crime. Our task is daunting, but we expect to report substantial progress in this endeavor to the Birmingham Summit in May of 1998.

* * * * *

COMMUNIQUÉ ANNEX: PRINCIPLES AND ACTION PLAN TO COMBAT HIGH-TECH CRIME

Statement of Principles

We hereby endorse the following PRINCIPLES, which should be supported by all countries:

- I. There must be no safe havens for those who abuse information technologies.
- II. Investigation and prosecution of international high-tech crimes must be coordinated among all concerned States, regardless of where harm has occurred.
- III. Law enforcement personnel must be trained and equipped to address high-tech crimes.
- IV. Legal systems must protect the confidentiality, integrity, and availability of data and systems from unauthorized impairment and ensure that serious abuse is penalized.
- V. Legal systems should permit the preservation of and quick access to electronic data, which are often critical to the successful investigation of crime.
- VI. Mutual assistance regimes must ensure the timely gathering and exchange of evidence in cases involving international high-tech crime.
- VII. Transborder electronic access by law enforcement to publicly available (open source) information does not require authorization from the State where the data resides.
- VIII. Forensic standards for retrieving and authenticating electronic data for use in criminal investigations and prosecutions must be developed and employed.
- IX. To the extent practicable, information and telecommunications systems should be designed to help prevent and detect network abuse, and should also facilitate the tracing of criminals and the collection of evidence.
- X. Work in this area should be coordinated with the work of other relevant international fora to ensure against duplication of efforts.

Action Plan

In support of these PRINCIPLES, we are directing our officials to:

1. Use our established network of knowledgeable personnel to ensure a timely, effective response to transnational high-tech cases and designate a point-of-contact who is available on a twenty-four hour basis.
2. Take appropriate steps to ensure that a sufficient number of trained and equipped law enforcement personnel are allocated to the task of combating high-tech crime and assisting law enforcement agencies of other States.
3. Review our legal systems to ensure that they appropriately criminalize abuses of telecommunications and computer systems and promote the investigation of high-tech crimes.
4. Consider issues raised by high-tech crimes, where relevant, when negotiating mutual assistance agreements or arrangements.
5. Continue to examine and develop workable solutions regarding: the preservation of evidence prior to the execution of a request for mutual assistance; transborder searches; and computer searches of data where the location of that data is unknown.
6. Develop expedited procedures for obtaining traffic data from all communications carriers in the chain of a communication and to study ways to expedite the passing of this data internationally.
7. Work jointly with industry to ensure that new technologies facilitate our effort to combat high-tech crime by preserving and collecting critical evidence.
8. Ensure that we can, in urgent and appropriate cases, accept and respond to mutual assistance requests relating to high-tech crime by expedited but reliable means of communications, including voice, fax, or e-mail, with written confirmation to follow where required.
9. Encourage internationally-recognized standards-making bodies in the fields of telecommunications and information technologies to continue providing the public and private sectors with standards for reliable and secure telecommunications and data processing technologies.
10. Develop and employ compatible forensic standards for retrieving and authenticating electronic data for use in criminal investigations and prosecutions.