Ministerial Conference of the G-8 Countries
on Combating Transnational Organized Crime
(Moscow, October 19-20, 1999)

COMMUNIQUE

1. The G-8 are committed to the fight against the dark side of globalization - transnational organized crime which threatens to damage our societies and our economies. Several years ago, the Eight agreed on the need to bring our law enforcement practices into the 21st century to counter this global menace and, during the French G-8 Presidency, created the Lyon Group of Senior Experts on Transnational Organized Crime to undertake this task.

2. We want to begin by expressing our sincere condolences to the people of the Russian Federation who have suffered the tragic loss of so many innocent lives as a result of the recent bombings. We, representing the Governments of the Eight, reiterate our determination to work together against terrorism in all its forms and to combat the international network which supports terrorism. We have adopted a statement on terrorism. We do so with a firm commitment to the UN Charter and norms of international law, including respect for human rights.

3. Two years ago we met in Washington and agreed on an action plan on high-tech and computer related crime, which was later approved at the Birmingham Summit. Last December, we met at the unprecedented ministerial video conference and reviewed our follow up of that action plan.

4. Consistent with commitments made at these meetings, we have agreed on measures to facilitate mutual legal assistance among our countries. We have agreed on principles and recommendations for seizing assets of international criminals and on a model asset sharing agreement. We continue to affirm the importance of and to seek opportunities to make use of video-testimony in international criminal cases. We are working to implement our commitment either to extradite our nationals for trial in the country where they have committed crimes or to conduct effective domestic prosecutions in lieu thereof. We are promoting acceptance among other members of the international community of recommendations developed by our experts for combating transnational organized crime (Lyon Group Forty Recommendations). We have implemented our commitment to establish a 24-hour, seven-day network of experts to assist in high-tech crime investigations. Since its establishment this network has been used successfully to investigate high-tech cases involving serious crimes, including threats to life. This network has now been extended to include a number of other countries.

5. In Moscow, under the chairmanship of Russia, we are meeting again at the Ministerial level to demonstrate our commitment to joint efforts against transnational organized crime, to extending effective anti-money laundering standards throughout the world, and to undermining the financial basis of criminal organizations, including the ability to corrupt public officials.

6. We have agreed that transnational organized crime can only be successfully combated by combining preventive and enforcement measures.

7. We have agreed to bring our anti-money laundering regimes into closer alignment and to consider putting certain responsibilities, as appropriate, on those professionals, such as lawyers, accountants, company formation agents, auditors, and other financial intermediaries who can either block or facilitate the entry of organized crime money into the financial system. We have agreed that all G-8 Members who have not yet done so should consider the possibility of accession to the Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime. We also agreed on the importance of an outreach to the media and non-governmental organizations because they have important roles to play in the fight against crime and corruption.

8. Today, we have endorsed the Guiding Principles and Plan of Action to Combat the Smuggling of and Trafficking in Human Beings, which was prepared by the G-8's Lyon Group under guidance provided at the G-8 Summit in Birmingham in 1998 [Annex 2].

9. We are meeting to give a guiding impulse to our joint actions against transnational organized crime by focusing on high-tech crime and the financial aspects of organized crime. Organized crime is taking advantage of the Internet and other new technologies to conduct transnational crime, including money laundering and serious fraud. We must deny criminals the ability to use these new technologies against our citizens.

10. We have agreed to cooperate against an immediate threat — the possible use of Y2K as a cover for high-tech transnational organized crime frauds. We have agreed to support the continuing work of our Lyon Group subgroup on high-tech crime. We must explore new options for locating and identifying criminals who use networked communications for illegal purposes.

11. We have reaffirmed our support for the intensive work made in the UN to adopt the Convention against Transnational Organized Crime, as well as the Protocols on firearms, smuggling of migrants and trafficking in persons by the end of the year 2000. We will reinforce our effort for this purpose.

12. We ask our experts to report on the progress in fighting transnational organized crime to our heads of States and Governments at the Kyushu-Okinawa Summit next year.

13. Specifically, with regard to high-tech crime and financial crime, including money laundering, we have all endorsed the following statements.

High-tech crime

14. As the use of the Internet and other new technologies increase, more criminals are provided with opportunities to commit crimes remotely, via telephone lines and data networks. Presently, malicious programming code and harmful communications (such as child pornography) may pass through several carriers located in different countries. And infrastructures such as banking and finance increasingly are becoming networked and thereby vulnerable to cyber-attack from distant locations. We convene today to provide additional personal attention to and direction for our joint action against this transnational criminality.

15. Our goals are to ensure that our people are protected from those who use new technologies for criminal purposes, such as child exploitation, financial crime, and attacks on critical infrastructures, and to ensure that no criminal receives safe haven anywhere in the world. We are determined that our law enforcement authorities have the technical ability and legal processes to find criminals who abuse technologies and bring them to justice. The safety of our people and their economic prosperity depend upon our leadership and determination and our ability to take coordinated action. We direct our experts to continue their work, particularly, on problems which arise for our law enforcement authorities from new developments in information technology and their use by criminals.

16. Strength of G-8 Legal Systems. Our experts have completed a comprehensive review of G-8 legal systems to assess whether those systems appropriately criminalize abuses of telecommunications and computer systems and promote the investigation of high-tech crimes. While, over the past decade, our governments have acted to see that their legal systems account for new technologies, there remains room for improvement. Where laws or legal processes require enhancements, we are committed to use best efforts to fill these gaps and, consistent with fundamental national legal principles, to promote new legal mechanisms for law enforcement to facilitate investigations and prosecutions.

17. Principles on Transborder Access to Stored Computer Data. Criminals take advantage of the jurisdictional inability of law enforcement authorities to operate across national borders as easily as criminals can. High-tech crimes may rapidly affect people in many countries, and evidence of these crimes, which may be quickly altered or destroyed, may be located anywhere in the world. Recognizing these facts, and taking into account principles relating to sovereignty and to the protection of human rights, democratic freedoms and privacy, our law enforcement authorities conducting criminal investigations should in some circumstances be able to pursue investigations across territorial borders. We have today adopted certain principles for access to data stored in a foreign state, which are contained in the Annex 1 to this Communique. We are committed to work

towards implementation of these principles through international cooperation, including legal instruments, and through national laws and policies, and invite all nations to join in this effort. We note, however, that continued work is required in this area, including on the appropriate collection, preservation and disclosure of traffic data, and we direct our experts to make further progress in consultation with industry.

18. Locating and Identifying High-tech Criminals. To ensure that we can all locate and identify criminals who use networked communications for illegal purposes, we must enhance our ability to trace communications while they are occurring and afterwards, even when those communications pass through multiple countries. Existing processes are often too slow and are designed more to address bilateral cooperation than crimes requiring the immediate assistance of many countries. Faster or novel solutions must be found. We, as Ministers, direct our experts to develop, in consultation with industry, a concrete set of options for tracing networked communications across national borders in criminal investigations and provide those options as soon as possible within one year.

19. International Network of 24-hour Contacts. Our 24-hour points of contact network, which allows us to respond to fast-breaking investigations, has now been expanded from the eight G-8 countries to a number of additional countries around the world. The speed of electronic communications and perishability of electronic evidence requires real-time assistance, and this growing global network has dramatically increased our investigative abilities. We direct our experts to facilitate further growth of this network. G-8 nations and their partners should also use this network proactively to notify other countries when they learn of significant potential threats to our shared networks.

20. Criminality Associated with the 'Millenium Bug'. Our countries have been at the forefront of efforts to successfully tackle the 'Millennium Bug' or 'Y2K Problem', which presents a major threat to the increasingly networked global economy. We are concerned that the Millennium Bug may either provide new opportunities for fraud and financial crimes, or mask ongoing criminality, if systems for accounting and reporting are disrupted. Therefore, as part of our new proactive use of our 24-hour network, we will provide early warning of Y2K-related abuses.

21. Internet Fraud. We recognize that Internet fraud, in all of its forms, poses a significant threat to the growth and development of electronic commerce and to the confidence that consumers place in electronic commercial transactions. To counter this threat, we are undertaking a comprehensive response, including crime prevention, investigation, and prosecution. For example, we are sharing information on international Internet fraud schemes — including information relating to the criminals, their methods and techniques, the victims involved in these schemes, and reports of enforcement actions - so that criminals defrauding people in multiple countries are investigated and prosecuted for the full range of

their criminal activities.

22. Industry Partnership. At the Washington Ministerial, we noted that the development of effective solutions to high-tech crime requires unprecedented cooperation between government and industry. Since then, we have been consulting regularly with industry, seeking to promote the growth of, and confidence in, the Internet by effectively combating high-tech and computer-related crime. To further this important dialogue and support ongoing efforts to develop cooperative solutions, we now direct our representatives to convene a conference where the G-8 and industry can share ideas on Internet crime, with particular emphasis on issues relating to locating and identifying Internet criminals.

23. We commend our experts in the Lyon Group and the Subgroup on High-tech Crime and urge them to maintain their hard work and creativity in addressing the daunting challenges in this growing area of criminal activity. They should also continue to coordinate their work with other international fora.

Financial aspects of transnational organized crime.

24. The financial crime and money laundering activities of transnational organized crime are a threat to the national security of all nations. Money laundering epitomizes the globalization of crime and has created a class of professional money launderers and money laundering organizations. International cooperation and a multidisciplinary approach to block the laundering of illegally acquired proceeds are essential elements of the fight against serious transnational organized crime and will help ensure an environment which promotes official integrity and is intolerant of corruption.

25. We warmly welcome the work of our colleagues, the Finance Ministers, through a variety of fora, and the work of the Financial Action Task Force (FATF), in combating money laundering. Great strides have been made, in particular, in extending anti-money laundering standards throughout the world. We must take all the steps that are necessary to ensure that criminals and their laundered money can find no safe haven.

26. We have considered a range of additional measures which we can take at the G-8 level to complement this work, and, in particular, to further enhance our cooperation with other countries.

27. We agreed, taking into account existing national legislation and international agreements, to enhance our cooperation. We agreed to bring into closer alignment our legislation covering the laundering of the proceeds of serious crimes and to render the fullest mutual assistance in the investigation and prosecution of serious crime, as well as in confiscating proceeds of crime. This assistance may include, where appropriate, making restitution to the victims of crime and, where legal and appropriate, assisting in the collection of fines imposed by foreign courts, and the

sharing or transfer of all or part of such confiscated assets between and among us.

28. We support efforts to ensure that the 40 Recommendations of the Financial Action Task Force become accepted and implemented worldwide, including in offshore centers, and for the FATF to continue its special emphasis on dealing with non-cooperative jurisdictions. We welcome the proposal to include provisions against money laundering in the UN Convention Against Transnational Organized Crime, under which signatories to the Convention would demonstrate their commitment to adopt and adhere to the 40 Recommendations.

29. We agreed to promote the implementation of the relevant existing international and regional instruments on mutual legal assistance and law enforcement cooperation.

30. We will take appropriate steps to ensure that bank secrecy provisions and other laws governing access to financial information (including information collected and held by financial institutions for tax purposes), allow for appropriate mutual assistance in support of criminal investigations, prosecutions and, if permissible under national legislation, related civil proceedings.

31. We support the proposals of the various fora, especially the FATF, which are studying the issue of non-cooperative jurisdictions. Jurisdictions with inadequate financial regulation and supervision, as well as excessive bank and corporate secrecy, play a significant role in laundering the proceeds of serious crime. A number of jurisdictions are also characterized by the absence of compulsory financial supervision over the activity of banks and other providers of financial services, and by the absence of obligations on rendering international legal assistance in the seizure and confiscation of the proceeds of illegal origin. This allows criminal groups to create and make use of off-shore financial institutions, trusts, shell companies, and nominee accounts to hide the indentity of the beneficial owners for the purpose of laundering the proceeds of crime. These practices should not be allowed to continue. We urge the FATF and other groups to take action as quickly as they can.

32. We recognize that many money-laundering schemes involve the corruption of financial intermediaries. We will therefore consider requiring or enhancing suspicious transaction reporting by the «gatekeepers» to the international financial system, including company formation agents, accountants, auditors and lawyers, as well as making the intentional failure to file the reports a punishable offense, as appropriate.

33. We have a serious concern about the threat posed by criminal use of new payment technologies, such as Internet banking, to launder the proceeds of crime. We encourage the FATF to develop its work in this area.

34. We will promote improvements in the quantity and quality of information flowing through the international systems of payments and we encourage

renewed study of the issue by our colleagues and the FATF.

35. We call for support of relevant international and national organizations to assist in the training of judicial and law enforcement personnel and rendering mutual assistance to strengthen relevant institutions. We will study effective methods of preventing and investigating crimes and assist in forensic and technical cooperation.

36. In order to improve the investigation of economic and financial crime, we will consider measures, as deemed appropriate, such as creating or enhancing multidisciplinary structures or task forces within our countries.

37. We agreed on the importance of extending predicate offenses of money laundering beyond drug-related offenses to other serious crimes, such as bribery or corruption. We agree to support each other in steps to counter corruption in our countries and the threat it can pose to our societies. We are committed to upholding public integrity and to assuring openness in our personnel systems, as well as ethical and administrative codes of conduct that proscribe conflicts of interest and promote the highest levels of professionalism and integrity. We agree on the need for impartial investigators, prosecutors and judicial personnel who can fairly and effectively enforce laws against corruption. We agree on the importance of transparency and integrity in government and public discussion on all aspects of the issue of upholding integrity and preventing corruption among public officials.

38. In order to improve mutual cooperation in conducting investigations of financial crime, we are determined to improve by all available means the effectiveness and efficiency of exchanges of law enforcement and financial regulatory information and we encourage all nations to join us in these efforts.

39. In order to enhance the effectiveness of law enforcement measures to fight the laundering of illegally acquired proceeds and to ensure reliable and rapid exchange of information, we encourage:

a) the application of the "10 Key Principles" approved at the Cologne Summit for improving the exchange of information between financial supervisory authorities and law enforcement authorities;

b) the creation of Financial Intelligence Units, where they do not already exist

c) the use of all available channels of communications between competent bodies, authorities and services.

40. Using the recommendations of the Lyon group and available intelligence information about suspicious transactions and large criminal cross-border movement of currency and monetary instruments, we will intensify efforts to identify mechanisms by which money launderers smuggle currency across the borders and to share available information.

41. Law enforcement experts will develop and agree to priorities for investigation and prosecution of money launderers and take joint action whenever possible.

42. In accordance with fundamental legal principles of domestic law, we will consider domestic and international mechanisms to alert law enforcement agencies about money launderers and related individuals who seek visas to travel to our countries, and take appropriate steps to address this phenomenon.

Moscow, October 20, 1999

Silke Mann

Annex 1

PRINCIPLES ON TRANSBORDER ACCESS TO STORED COMPUTER DATA

PRINCIPLES ON ACCESSING DATA STORED IN A FOREIGN STATE

The G8 agree that the following principles should apply when law enforcement agents employed by law enforcement agencies are investigating criminal matters and require transborder access to, copying of, or search and seizure of electronic data (including historical traffic data, but not including interceptions), and such principles should be implemented through treaties, and through national laws and policies:

PRESERVATION OF DATA STORED IN A COMPUTER SYSTEM

1. Each State shall ensure its ability to secure rapid preservation of data that is stored in a computer system, in particular data held by third .parties such as service providers, and that is subject to short retention practices or is otherwise particularly vulnerable to loss or modification, for the purpose of seeking its access, search, copying, seizure or disclosure, and ensure that preservation is possible even if necessary only to assist another State.

2. A State may request another State to secure rapid preservation of data stored in a computer system located in that other State.

3. Upon receiving a request from another State, the requested State shall take all appropriate means, in accordance with its national law, to preserve such data expeditiously. Such preservation shall be for a reasonable time to permit the making of a formal request for the access, search, copying, seizure or disclosure of such data.

EXPEDITED MUTUAL LEGAL ASSISTANCE

4. Upon receiving a formal request for access, search, copying, seizure or disclosure of data, including data that has been preserved, the requested State shall, in accordance with its national law, execute the request as expeditiously as possible, by:

a) Responding pursuant to traditional legal assistance procedures, or

b) Ratifying or endorsing any judicial or other legal authorization that was

granted in the requesting State and, pursuant to traditional legal assistance procedures, disclosing any data seized to the requesting State; or

c) Using any other method of assistance permitted by the law of the requested State,

5. Each State shall, in appropriate circumstances, accept and respond to legal assistance requests made under these Principles by expedited but reliable means of communications, including voice, fax or e-mail, with written confirmation to follow where required.

TRANSBORDER ACCESS TO STORED DATA NOT REQUIRING LEGAL ASSISTANCE

6. Notwithstanding anything in these Principles, a State need not obtain authorization from another State when it is acting in accordance with its national law for the purpose of:

a) accessing publicly available (open source) data, regardless of where the data is geographically located;

b) accessing, searching, copying, or seizing data stored in a computer system located in another State, if acting in accordance with the lawful and voluntary consent of a person who has the lawful authority to disclose to it that data.

The searching State should consider notifying the searched State, if such notification is permitted by national law and the data reveals a violation of criminal law or otherwise appears to be of interest to the searched State.