EUROPEAN UNION
THE COUNCIL

Brussels, 19 December 1997

13539/97

LIMITE

CRIMORG 38

NOTE

from : Incoming United Kingdom Presidency

to : Multidisciplinary Group on Organized Crime (MDG)

Subject: Communique by the Justice and Interior Ministers of the Eight

At the invitation of US Attorney General Janet Reno, the Justice and Interior Ministers of the Eight met for the first time in Washington on 9-10 December to discuss the fight against transnational organised crime. Attached to this note is the Communique which they issued setting out their conclusions and a programme of work.

2. The Presidency intends to invite the Multi-Disciplinary Group to discuss, at its January meeting, links between the work programme of the Eight and the European Union's Action Plan to combat organised crime.

High tech crime

3. The Ministers of the Eight have adopted a set of ten principles on combatting high tech crime, combined with a ten point action plan. This is attached to the Communique. United Kingdom Home Secretary Jack Straw intends to report on this work to his European Union colleagues at the informal meeting of the Justice and Home Affairs Council in January, and in particular to commend to them the principles and action plan.

4. The European Union itself is already committed to work on high tech crime (Recommendations 5 and 26f of the EU Action Plan) and the Luxembourg Presidency arranged a very useful seminar in the margins of the November meeting of the Multi-Disciplinary Group, with United States, Council of Europe and other participants.

5. The Presidency will invite the views of MDG delegates on the document prepared by the Eight, and on how Recommendation 5 of the EU Action Plan might be taken forward.

Other forms of co-operation

6. The Communique also covers other actions against transnational organised crime, including

- extradition of own nationals or prosecution in lieu of extradition
- investigation and prosecution of multi-jurisdiction cases to be co-ordinated
- continued examination of the use of video-link technology for securing evidence from witnesses located abroad
- confiscation and sharing of criminal assets
- joint operational projects to target major criminal organisations and activities
- work on firearms trafficking and other cross-border crime and smuggling.

7. The MDG will be invited to note the Communique and discuss its implications for the Group's own work.

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.

UNION EUROPEENNE

Bruxelles, le 19 décembre 1997 (12.01)

LE CONSEIL

(OR.en)

13539/97

LIMITE

CRIMORG 38

N O T E

de : la future présidence du Royaume-Uni

au : Groupe multidisciplinaire sur la criminalité organisée

Objet : Communiqué des ministres de la justice et de l'intérieur des Huit

1. A l'invitation du ministre de la justice des Etats-Unis, Mme Janet Reno, les ministres de la justice et de l'intérieur des Huit se sont réunis pour la première fois à Washington les 9 et 10 décembre pour discuter de la lutte contre la criminalité organisée transnationale. On trouvera en annexe à la présente note leur communiqué, qui présente leurs conclusions ainsi qu'un plan d'action.

2. La présidence se propose d'inviter le Groupe multidisciplinaire à examiner, lors de sa réunion de janvier, les liens entre le plan d'action des Huit et le programme d'action de l'Union européenne relatif à la criminalité organisée.

La criminalité liée à la haute technologie

3. Les ministres des Huit ont adopté un ensemble de principes sur lesquels doit reposer la lutte contre la criminalité liée à la haute technologie ; ces principes sont assortis d'un plan d'action en dix points, qui est joint au communiqué. Le ministre de l'intérieur du Royaume-Uni, M. Jack Straw, a l'intention de présenter ces travaux à ses collègues de l'Union européenne lors de la réunion informelle des ministres de la justice et de l'intérieur qui se tiendra en janvier, et en particulier de les inviter vivement à adopter ces principes et ce plan d'action.

4. L'Union européenne s'est elle-même déjà engagée à agir contre la criminalité liée à la haute technologie (recommandations 5 et 26 f du plan d'action de l'UE) et la présidence luxembourgeoise a organisé un séminaire très utile en marge de la réunion de novembre du Groupe multidisciplinaire, auquel ont participé, entre autres, les Etats-Unis et le Conseil de l'Europe.

5. La présidence invitera les délégués du Groupe multidisciplinaire à faire part de leurs remarques sur le document des Huit et sur la manière dont la recommandation nº 5 du programme d'action de l'UE pourrait être appliquée.

Autres formes de coopération

6. Le communiqué mentionne aussi d'autres mesures pour lutter contre la criminalité organisée transnationale, à savoir :

   - l'extradition par le pays dont les intéressés sont ressortissants ou le recours à des poursuites judiciaires à la place de l'extradition ;

   - la coordination des enquêtes et des procédures judiciaires dans le cas des affaires relevant de plusieurs juridictions ;

   - poursuite de l'examen de la possibilité d'avoir recours aux techniques de vidéo-conférence pour obtenir la déposition de témoins se trouvant à l'étranger ;

   - confiscation et partage des biens d'origine criminelle ;

   - projets opérationnels conjoints visant les grandes organisations et activités criminelles ;

   - lutte contre le trafic d'armes ainsi que les autres activités criminelles transfrontières et la contrebande.

7. Le Groupe multidisciplinaire sera invité à prendre note du communiqué et à examiner ce qui en découle pour ses propres travaux.

Collages

ANNEXE DU COMMUNIQUE :
PRINCIPES ET PLAN D'ACTION POUR LA LUTTE CONTRE LA CRIMINALITE LIEE A LA HAUTE TECHNOLOGIE

Enoncé des principes

Nous souscrivons par la présente déclaration aux PRINCIPES énoncés ci-après, que tous les pays devraient adopter :

I. Il ne doit exister aucun refuge sûr pour les individus qui utilisent les technologies de l'information à des fins répréhensibles.

II. Les enquêtes et les poursuites judiciaires auxquelles donne lieu la criminalité internationale liée à la haute technologie doivent être coordonnées entre tous les Etats concernés, quel que soit le lieu où le préjudice est subi.

III. Les agents des services de répression doivent être formés et équipés pour pouvoir faire face à la criminalité liée à la haute technologie.

IV. Les systèmes juridiques doivent garantir la confidentialité, l'intégrité et la disponibilité des données, protéger les systèmes contre toute modification non autorisée et assurer que tout abus grave soit puni.

V. Les systèmes juridiques devraient permettre la conservation des données électroniques, ainsi que l'accès rapide à ces données, deux conditions dont dépend souvent le succès des enquêtes.

VI. Les régimes d'entraide doivent permettre la collecte et l'échange en temps voulu des preuves dans les affaires concernant la criminalité internationale liée à la haute technologie.

VII. L'accès transfrontière par voie électronique des agents des services de répression aux informations publiques (sources ouvertes) doit pouvoir se faire sans l'autorisation de l'Etat où sont situées ces données.

VIII. Des normes légales doivent être définies et observées en ce qui concerne la recherche et l'authentification des données destinées à être utilisées dans les enquêtes et les procédures judiciaires criminelles.

IX. Dans la mesure où cela est réalisable, les systèmes d'information et de télécommunication devraient être conçus de manière à faciliter la prévention et la détection de toute utilisation répréhensible des réseaux, et devraient aussi faciliter la recherche des criminels ainsi que l'obtention des preuves.

X. Les travaux réalisés dans ce domaine devraient être coordonnés avec ceux d'autres instances internationales compétentes afin d'éviter que les mêmes travaux ne soient effectués deux fois.

Plan d'action

En application de ces principes, nous donnons instruction à nos collaborateurs :

1. d'utiliser notre réseau existant d'agents compétents pour faire en sorte que les affaires transnationales de criminalité liée à la haute technologie soient traitées de manière efficace et en temps voulu, et de désigner un point de contact qui soit disponible vingt-quatre heures sur vingt-quatre ;

2. de prendre les mesures nécessaires pour qu'un nombre suffisant d'agents formés et équipés des services de répression soit affecté, d'une part, à la lutte contre la criminalité liée à la haute technologie et, d'autre part, à l'assistance des services de répression des autres Etats ;

3. de vérifier que, dans nos systèmes juridiques, l'utilisation abusive des systèmes de télécommunication et des réseaux informatiques constitue une infraction exposant à des peines appropriées et qu'ils offrent suffisamment de moyens d'instruire les affaires de criminalité liée à la haute technologie ;

4. d'examiner, le cas échéant, les questions soulevées par la criminalité liée à la haute technologie lors de la négociation des accords et arrangements d'entraide ;

5. de continuer à étudier et à mettre au point des solutions pratiques concernant : la préservation des preuves avant qu'elles soient nécessaires pour répondre à une demande d'entraide, les recherches transfrontières, et la recherche électronique de données lorsqu'on ne sait pas où celles-ci sont situées ;

6. de mettre au point des procédures accélérées pour l'obtention de données sur le trafic de tous les opérateurs faisant partie de la chaîne pour une communication donnée et d'étudier les moyens d'accélérer le transfert de ces données au niveau international ;

7. de collaborer avec les industriels pour faire en sorte que les nouvelles technologies nous aident à combattre la criminalité liée à la haute technologie en préservant et en rassemblant les preuves essentielles ;

8. de faire en sorte que, dans les cas d'urgence où cela est justifié, nous puissions accepter les demandes d'entraide concernant la criminalité liée à la haute technologie et y répondre, par des moyens de communication rapides mais fiables, notamment par téléphone, télécopie ou courrier électronique, avec, au besoin, confirmation écrite ultérieure.

9. d'encourager les organismes de normalisation reconnus au niveau international qui opèrent dans les domaines des télécommunications et des technologies de l'information à continuer de définir à l'intention des utilisateurs des secteurs public et privé des normes permettant d'assurer la fiabilité et la sécurité des télécommunications et des technologies de traitement de l'information ;

10. de définir et d'observer des normes légales compatibles pour la recherche et l'authentification des données électroniques destinées à être utilisées dans les enquêtes et les procédures judiciaires pénales.

_____