

COUNCIL RECOMMENDATION**of 25 June 2001****on contact points maintaining a 24-hour service for combating high-tech crime**

(2001/C 187/02)

THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the position adopted by the Council on 19 March 1998 inviting the Member States to join the G8 24-hour information network for combating high-tech crime, and its endorsement of the network's principles,

Considering the communication of 26 January 2001 from the Commission 'Creating a safer information society by improving the security of information infrastructures and combating computer-related crime: Europe 2002',

Whereas:

- (1) The G8 network's principles concerning national points of contact for the purpose of combating high-tech crime were adopted at the G8 meeting for Ministers of Justice and Home Affairs in Washington DC on 9 and 10 December 1997. To these principles were added an action plan for the establishment of the network and an account of the commitments that the individual States take on if they join the network. In the action plan, the G8 welcomes countries also coming from outside the G8 circle to join the network.
- (2) There is a great advantage in a global network like the G8 network, and there are reasons to believe that its importance will increase. If law enforcement networks combating IT-related crime consist of only a few countries, they cannot obtain a sufficient overview of, or achieve sufficient efficiency in, combating such crime in cyberspace.
- (3) The basic idea behind the network is that the handling of various types of high-tech crime should be swift and highly professional. The emphasis is put on conserving evidence in environments where information can be quickly lost or destroyed. If the first measures taken by the law enforcement authorities are incorrect or slow, they may obstruct or even ruin opportunities to investigate cases of this form of crime. Another purpose of the network is that the countries linked to the network should be able to obtain an overview of computer network crime since it often occurs simultaneously at different locations in different countries.
- (4) The network was established gradually over the years 1998 to 2000, and efforts to extend the number of countries are
- (5) At present, the network is made up of the following countries: Australia, Brazil, Canada, Denmark, Finland, France, Germany, Italy, Japan, The Netherlands, Russia, Spain, Sweden, United Kingdom and USA. Thus, nine EU Member States have joined the network.
- (6) Those EU Member States that have not joined the G8 network form part of Interpol's national central reference point system (NCRP). At present, more than 60 countries are connected to Interpol's network. An NCRP is usually a specialist unit. The NCRPs of Interpol, however, do not always provide 24-hour readiness besides the readiness provided by the communications centres of the National Central Bureaux. The cooperation within Interpol's NCRP network is based on the same principles that are otherwise applied to the Interpol cooperation. This means that measures involving any means of coercion in order, for instance, to conserve evidence are normally not handled through this channel. The G8 network has in its principles emphasised quick measures when it comes to freezing or conserving evidence in computer systems or networks. There is no competitive relation between the two law enforcement networks. On the contrary, they rather complement each other. It should therefore be possible for those EU Member States that are not represented in the G8 network to link a 24-hour function to their specialist units that form part of the Interpol cooperation.
- (7) Experience from, for instance, the world wide 'love letter' virus in May 2000 shows that the G8 network needs to be both extended and improved. Effective maintenance of 24-hour readiness in the form of specialist units in the countries that have joined the network represents an important improvement. Today, it happens that a communications centre receives a message and forwards it only after the opening of the specialist unit. In connection with holidays, such a procedure may result in fatal loss of time.
- (8) A desirable common standard would be that the unit designated as a national contact point really is a specialist

unit that applies recommended international practice to investigations of high-tech crime, and that the unit is prepared to take any possible action, with due regard, of course, to national legislation.

HEREBY RECOMMENDS:

— those Member States that have not yet joined the G8

network of contact points with 24-hour service intended for the combat against high-tech crime to do so,

- Member States to ensure that the unit designated as a contact point maintains 24-hour service, and that the contact point really is a special unit that applies established good practice when investigating IT-related crime. The contact point should also be able to take operational measures.
-