

9025/97

LIMITE

ENFOPOL 143

NOTE

from : the Presidency

to : K.4 Committee

No. prev. doc. : 8068/1/97 ENFOPOL 115 REV 1; 7171/1/97 ENFOPOL 83 REV 1;
7069/97 ENFOPOL 80; 5754/97 ENFOPOL 27

Subject : **Internet communication interception**

I Introduction

In Enfopol 83 Rev 1 concerning harmonization of Internet-related activities within the EU, which was approved by the K.4 Committee at the meeting of 12/13 May 1997, it was recommended that the Working Group Police Cooperation would "examine to what extent providers of Internet services can be obliged to cooperate in criminal investigations in particular situations".

In the last meeting of the WGPC on 3 June 1997 the delegations agreed on two main items in order to implement recommendation E.

SEMDOC
Statewatch European Documentation &
Monitoring Centre on justice and home
affairs in the European Union

PO Box 1516, London N16 0EW, UK
tel: 0181 802 1882 (00 44 181 802 1882)
fax: 0181 880 1727 (00 44 181 880 1727)

II Co-ordination between the WGPC and the Council of Europe PC-CY

Though the Council of Europe PC-CY is the most consistent and broad-based forum discussing Internet matters, it is not yet ready to discuss the subject of interception. In the meantime, therefore, the WGPC agreed to continue working out policy on the technical interceptability of Internet (see III). At the same time, however, a constant watch must be kept on developments within the Council of Europe PC-CY. This can be done through active mutual consultation between national representatives on both bodies. In view of the fact that the Netherlands is chairing the PC-CY, the Netherlands delegation will assume this coordinating task.

III Outcome of the meeting of the ILETS Standing Technical Committee (STC)

The ILETS STC (chaired by the UK) has studied the technical aspects of the interception of Internet communication. The UK delegation briefed the WGPC on the results of this meeting and will prepare for the WGPC meeting of 24 June 1997 a document with the following themes:

- a) under-reporting is leading to inaccurate assessments of the extent of this threat. Training and awareness for officers is vital;
- b) the involvement of the Internet Service Provider (ISP), whether to trace a target or mount an interception, is central to effective interception. Increased use of mobile access to the Internet will make identifying targets more difficult;
- c) technology is outpacing legislation. The technology thrust is towards converge of telecommunications/IT/broadcasting; one digital packet technology providing a wide range of services;
- d) international co-operation is necessary given that targets could register with ISPs in another country and ISPs can site servers in a range of countries. Computer networks do not recognise international boundaries;
- e) dedicated specialists teams need to be created to gain a full understanding of the medium and its development.

IV Conclusion

If the K.4 Committee can agree with the procedure set out in II and III, the WGPC will continue its work along these lines.