Parliamentary **Assembly**
Assemblée parlementaire

Parliamentary Assembly
Assemblée parlementaire
COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Doc. 11333
27 June 2007

How to prevent cybercrime against state institutions in member and observer states?

Opinion[1]
Committee on Economic Affairs and Development
Rapporteur: Mrs Anna LILLIEHÖÖK, Sweden, Group of the European People's Party (EPP/CD)

A. Committee conclusions

The Committee on Economic Affairs and Development appreciates the opportunity to contribute to a highly topical, timely and important debate on cybercrime. It fully shares the concern of the Committee on Legal Affairs and Human Rights that highlights the vulnerability of modern society to cybercrime as a threat to democracy, human rights and the rule of law.

The Economic Committee is convinced that cybercrime is liable to hurt state institutions just as much as it can damage the socio-economic tissue of society. Public and private institutions face a common need for enhanced network security and protection of critical infrastructure. They should work together more actively towards developing international cross-sector co-operation on the basis of public-private partnerships.

B. Proposed amendment to the draft resolution

After sub-paragraph 14.5., to insert the following new sub-paragraph:

> "associate the private sector more closely, notably by building public-private partnerships for more effective and cross-sector international co-operation against cybercrime;"

C. Explanatory memorandum by Mrs Lilliehöök, Rapporteur

The spread of information technologies over the past decades has gone hand in hand with the increasing openness of states to free movement of capital, goods, persons and ideas but also rendered them more vulnerable to new global problems. Our societies have developed sophisticated computer applications in a race for faster, cheaper and more accessible tools without taking time to ponder the necessary safeguards to protect the stability of digital networks and systems. Cybercrime came into being as a sobering reminder that criminals too are quick to exploit new opportunities in the cyberspace where up until recently virtually everything was allowed and everything was possible.

[1] See the report presented by the Committee on Legal Affairs and Human Rights (Doc. 11325)

F – 67075 Strasbourg Cedex, e-mail: assembly@coe.int
tel : + 33 3 88 41 2000, fax + 33 3 88 41 2776

Today, the Council of Europe Cybercrime Convention is the only binding international instrument on cybercrime which been endorsed not only by member states but also by many non-European states. It is an open, comprehensive and ambitious treaty that deserves our unconditional support and implementation without delay. We hope that Assembly's debate on cybercrime will create momentum for speeding up accession of European and other states to this convention in order to realise its full potential.

We should stress in this context some of the salient findings of cybercrime experts, representing both public and private sectors, who gathered in Strasbourg on 11-12 June 2007 to analyse trends in cybercrime and to propose practical steps required to counteract new threats. Thus, it appears that

- Vicious software is evolving rapidly and is increasingly used to perpetrate economic crimes;
- Cyber-offenders tend to organise for crime aimed at generating illicit profits and criminal enterprises feed further expansion of the shadow economy;
- Irrational cyber attacks are being replaced by more targeted attacks on specific users (individuals, groups, organisations, enterprises, sectors, etc.), especially with a view to pursuing criminal economic purposes;
- The perceived risk of cyber attacks against critical infrastructure is on the rise;
- A new generation of cyber technologies is bringing in new challenges to law enforcement.

Clearly, the private and public sectors share the need for high levels of cyber security. Their means and approaches may differ but are complementary to a large extent. As the threat of cybercrime and attacks against the world wide web must be tackled by a truly global and cross sector response, wide and rapid implementation of the Cybercrime Convention would be a major step in the right direction.

Another step is a quest for closer interaction between public and private institutions in furthering global co-operation to develop innovative regulatory and technical measures for the enhanced protection of cyber networks and underlying vital infrastructure. Having launched the Cybercrime Convention, its monitoring mechanism and the capacity building activity for law enforcement authorities, the Council of Europe is a useful platform for dialogue, information sharing, cross-border legislative action and policy co-ordination, organising training workshops and building public-private partnerships for curbing cybercrime.

Cyber-space is tight and interactive: any wrongdoing may backlash with offenders ending up themselves as victims of the digital networks spinning out of control. We therefore wish to address a warning against leniency and lack of vigilance or action to restrain the risks of ill-intentioned cyber attacks for political, economic or other reasons. Finally, as we urge member states to ratify the Cybercrime Convention, we address in particular those states with "state-of-the-art" technology and expertise where we have seen the greatest risks for new malevolent technology development.

* * *

Reporting committee: Committee on Legal Affairs and Human Rights

Committee seized for opinion: Committee on Economic Affairs and Development

Reference to committee: Request for an urgent debate, Reference No. 3365 of 25 June 2007

Draft opinion approved by the Committee on Economic Affairs and Development on 26 June 2007