Judicial cooperation in criminal matters: combating attacks against information systems

2010/0273(COD) - 09/06/2011

The Council adopted a **general approach** on a draft directive on attacks against information systems, proposed by the Commission in September 2010. The general approach will constitute the basis for the Council's negotiations with the European Parliament on this proposal under the ordinary legislative procedure.

The proposal aims to update the existing rules dating from 2005 (Framework Decision 2005/222/JHA), while building on the Council of Europe Convention on Cybercrime (Budapest Convention). It establishes minimum rules for the definition of criminal offences and the penalty levels in the area of attacks against IT systems. It also aims to facilitate the prevention of such attacks and to improve the cooperation between member states' authorities in this field. The new rules would retain most of the provisions currently in place - namely the penalisation of illegal access, illegal system interference and illegal data interference as well as instigation, aiding, abetting and attempt to commit those criminal offences - and **include the following new elements**:

- penalisation of the production and making available of tools (e.g. malicious software designed to create "botnets"[1] or unrightfully obtained computer passwords) for committing the offences;
- illegal interception of computer data will become a criminal offence;
- improvement of European cooperation in criminal matters by strengthening the existing structure of 24/7 contact points, including an obligation to provide feedback within eight hours to urgent requests; and
- the obligation to collect basic statistical data on cybercrimes.

Concerning the level **of criminal penalties**, the new rules would **raise the thresholds**:

- in the general case to a maximum term of imprisonment of at least two years;
- if committed against a significant number of IT systems, e. g. in order to create a "botnet", to a maximum term of imprisonment of at least three years;
- if the attack has been committed by an organised criminal group, or has caused serious damage, e.g. through the use of a "botnet", or has affected a critical IT system, to a maximum term of imprisonment of at least five years.

These new forms of aggravating circumstances are intended to address the emerging threats posed by large scale cyber attacks, which are increasingly reported across Europe and have the potential severely to damage public interests.

Lastly, the Council has clarified the rules concerning the establishment of jurisdiction by the member states on cybercrime.

While the UK and Ireland participate in the adoption and application of this directive, Denmark would not be bound by it.