Judicial cooperation in criminal matters: combating attacks against information systems

2010/0273(COD) - 13/09/2017 - Follow-up document

The Commission presented a report assessing the extent to which the Member States have taken the necessary measures in order to comply with Directive 2013/40/EU on attacks against information systems.

The objectives of the Directive are to approximate the criminal law of the Member States in the area of attacks against information systems and to improve cooperation between competent authorities. This is done by establishing minimum rules concerning the definition of criminal offences and sanctions in the area of attacks against information systems and by requiring operational 24/7 points of contact.

By the transposition date, **22 Member States had notified the Commission that they had fully completed the Directive's transposition**. As of 31 May 2017, infringement procedures for non-communication of national transposition measures against BE, BG and IE were still pending. However, the Commission acknowledges the efforts made by the Member States to transpose the Directive.

The analysis in this report is based on the information that Member States provided by 31 May 2017.

Progress made: the report concluded that the Directive has made **real progress in criminalising cyberattacks** on a comparable level across the Member States, facilitating cross-border cooperation between law enforcement authorities investigating cyberattacks.

Member States have amended criminal codes and other relevant legislation. They have **streamlined their procedures** and set up or improved cooperation schemes.

Scope for improvement: the Commission confirmed, however, that there is **considerable scope for improvement** if Member States were to fully implement all of its provisions. The main improvements to be implemented by the Member States relate in particular to:

- **the use of the definitions** of the terms 'information system', 'computer data', 'legal person' and 'without right' provided by the Directive: only two countries have introduced legislation covering all aspects of these definitions;
- the **inclusion of all the possibilities that define specific criminal related offences** (illegal access to information systems, illegal data interference, illegal interception of computer data: tools, such as computer programmes or passwords, used to commit offences);
- the **establishment of common standards of penalties for cyberattacks** (minimum levels of maximum penalties, penalties where a significant number of information systems have been affected, offences committed by a criminal organisations, causing serious damage, involvement critical infrastructure information systems in offences, identity theft, liability of legal persons).

Other issues appear to relate to the implementation of administrative provisions on **appropriate reporting channels** and the monitoring and statistics for the offences included in the Directive.

Outlook: the Commission states that it will continue to support Member States in their implementation of the Directive and will provide additional opportunities for Member States to identify and exchange best practices in the second half of 2017.

The Commission currently **sees no need to propose amendments to the Directive**. It is considering measures to **improve cross-border access to electronic evidence** for criminal investigations, including proposing legislative measures by the beginning of 2018. It is also considering the role of encryption in criminal investigations and will report on its findings by October 2017.

Lastly, the Commission is committed to ensuring that the transposition is finalised across the EU and that the provisions are correctly implemented.