



EUROPEAN COMMISSION  
IMPACT ASSESSMENT BOARD

Brussels, 02 JUN 2009  
D(2009) 4224

## Opinion

**Title**                      **Impact Assessment on: Proposal to amend Framework Decision 2005/222/JHA on attacks against information systems**

**(draft version of 4 May 2009)**

**Lead DG**                      **JLS**

### **1) Impact Assessment Board Opinion**

#### **(A) Context**

The Council Framework Decision 2005/222/JHA (FD) responds to the objective to improve cooperation between judicial and other competent authorities, including the police and other specialised law enforcement services of the Member States, through approximating rules on criminal law in the Member States in the area of attacks against information systems. The Framework Decision closely follows the Council of Europe Convention on Cybercrime (signed in 2001, entered into force in 2004), which is regarded by experts as constituting the highest international standard to date. However, the large-scale simultaneous attacks against information systems (2007 in Estonia and 2008 in Lithuania) were not the centre of focus when the Framework Decision was adopted. This impact assessment considers options for EU action in response to these developments.

#### **(B) Positive aspects**

The report gives a comprehensive overview of the context of this initiative. Despite the largely technical character of the issues, a good effort has been made to make it accessible to a non-specialist reader.

#### **(C) Main recommendations for improvements**

*The recommendations below are listed in order of descending importance. Some more technical comments will be transmitted directly to the author DG.*

#### **General recommendation:**

**There are several key issues where significant improvements are needed to the IA report. These concern further clarification of how the proposed measures would be**

Commission européenne, B-1049 Bruxelles / Europese Commissie, B-1049 Brussel - Belgium. Telephone: (32-2) 299 11 11. Office: BERL 6/29. Telephone: direct line (32-2) 2981898. Fax: (32-2) 2965960.

E-mail: [impact-assessment-board@ec.europa.eu](mailto:impact-assessment-board@ec.europa.eu)

**effective and sufficient to combat the cybercrime, the elaboration of the analysis of the appropriate level of action (global/EU/Member States), and clarification of the content of the preferred option.**

**Given that the recommendations concern the key elements of the IA report, the IAB requests DG JLS to resubmit a revised version of the IA report, on which the Board will issue a new opinion.**

**(1) Explain why enhanced penalisation of and approximation of criminal laws against cyber crime is an effective measure to combat cybercrime.** Given that key problem drivers behind the increase of attacks against information systems is insufficient cooperation at European and international level as well as lack of awareness of the risks among users/potential victims, it is not clear how the measures focussing mainly on criminalisation of cybercrime and accessibility of contact points would be effective in detecting and preventing such crimes. The report should therefore explain and provide evidence to support the view that (a) the applied level of penalties is a decisive factor determining the priorities in criminal investigation, and that a higher priority for investigating cybercrime will have a dissuasive effect (b) improved accessibility of contact points would effectively enhance the cross-border law-enforcement. Furthermore, the report should be more explicit about the limits of legislative measures and highlight further the importance of non-legislative actions. It should be clear which elements of Option 2 'Non-legislative measures' and Option 3 'Update of the existing FD' constitute the preferred option and the report should present this combined option up-front so that it can be fully assessed and compared to the other options. Given the critical role of non-legislative measures from the effective law enforcement perspective, the report should clarify how the necessary level of commitment among the Member States to implement the voluntary measures would be assured. The source of finance for the planned training activities should be clarified.

**(2) Elaborate the discussion about the appropriate level of action.** Given the global nature of cyber crime, the report should (a) explain how the action at EU level would contribute to the international cooperation (e.g. Interpol, G 8 Roma-Lyon High Tech Crime Group) and (b) discuss the possibilities for complementary action at global level by proposing an option of updating the Council of Europe Convention on Cybercrime. In addition, the report should assess the impacts of more advanced measures in the EU (going beyond the requirements of the Council of Europe Convention) on third countries, especially the potential 'export' of cybercrime.

Given that some Member States have already taken action to criminalise cyber attacks in their national legislation, the report should also demonstrate why the EU level legislative action is proportionate and why it is not sufficient to let the Member States to handle the issue on their own.

**(3) Provide analysis to support the approach for setting the level of penalties for large-scale attacks.** Given the cultural and historical differences in the legal systems of the Member States, the report should discuss the expected impacts of the harmonised level of penalisation in differed jurisdictions, and present the arguments which support the choice of the level of 2-5 years for imprisonment, possibly combined with financial penalties.

**(4) Clarify implementation of the distinction between legitimate and illegitimate use of certain IT tools.** Given that the initiative provides for the criminalisation of the

production, sale, procurement for use, import, and distribution of tools enabling large-scale attacks against information systems while introducing an exception where those tools are used for legitimate purposes, the report should explain how this distinction will be implemented in practice.

**(D) Procedure and presentation**

It appears that all necessary procedural elements have been complied with. The executive summary should contain information on quantified administrative costs.

**2) IAB scrutiny process**

Reference number	2009/JLS/048 (CLWP 2009 Priority)
Author DG	JLS
External expertise used	No
Date of Board Meeting	27 May 2009
Date of adoption of Opinion	<b>02 JUIN 2009</b>