EUROPEAN COMMISSION
IMPACT ASSESSMENT BOARD

Brussels,
D(2009) 2204 19

31 AOUT 2009

Opinion

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

(draft version of 11 August 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 revised report has clarified the content of the preferred option and how it will be implemented. It has explained how action at EU level would contribute to the international cooperation, discussed the possibilities for complementary action at global level, and assessed its impact on third countries. The revision of the IA report has led to the modification of the proposed minimum level of the maximum penalty for large-scale cyber attacks from the original level of 2-5 years to 5 years.

(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: While the IA report has been improved, there are still

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

several key issues which require further explanation. First, the report still needs to provide evidence for the link between enhanced penalisation for large-scale attacks and effective law enforcement. Second, it should strengthen the arguments for why the EU and not Member States should set the minimum levels of maximum penalties for large-scale cyber attacks. Finally, the report should strengthen its justification for setting those penalties at 5 years.

(1) Explain further why enhanced penalisation of and approximation of criminal laws against cybercrime is an effective measure to combat cybercrime. The revised report has explained why the applied level of penalties (and the good functioning of contact points) can be important for the effective cross-border law enforcement and judicial cooperation. However, it should substantiate the claim that the current level of penalties in some Member States leads to a situation where they consider the crimes insufficiently serious to warrant rapid enforcement or the use of certain investigative techniques and tools. The report should also discuss to what extent the effectiveness of the enhanced penalisation would depend on the ability or willingness of some Member States to provide additional resources to investigate and enforce cybercrime (e.g. use of advanced techniques and tools). Given the critical role of non-legislative measures from the effective law enforcement perspective, and as recommended in the IAB's first opinion, the report should clarify how the necessary level of commitment among the Member States to implement the voluntary measures would be assured.

(2) Elaborate further the discussion about the appropriate level of action. While the revised report has addressed the question of the necessity of EU action in the field of penalisation of large-scale cyber attacks, it should substantiate the claim that Member States which have not experienced large-scale attacks do not have sufficient incentives to upgrade their legislation on their own. The report should clarify to what extent this attitude results from the lack of awareness of related risks and to what extent from unequal distribution of the actual risks among Member States. Should the former be the case, the report should discuss why an awareness raising instrument (for example, a recommendation) would not be sufficient to induce relevant Member States to raise penalties and to give large-scale cyber attacks higher priority in their law enforcement.

(3) Strengthen the analysis to support the approach for setting the level of penalties for large-scale attacks. While the report has provided arguments which support the choice of the minimum level of the maximum penalty of 5 years, it should substantiate the claim that this level is appropriate for the gravity of the crime as opposed to the current, predominant level of 1-3 years (e.g. by referring to relevant studies, publications, opinions of criminal law experts). The report should also clarify and substantiate the statement that setting this minimum level at 5 years "corresponds to the notion of serious crime".

(D) Procedure and presentation

It appears that all necessary procedural elements have been complied with.

2) IAB scrutiny process

Reference number	2009/JLS/048 (CLWP 2009 Priority)
Author DG	JLS
External expertise used	No
Date of Board Meeting	Written procedure
Date of adoption of Opinion	31 AOUT 2009 The present opinion concerns a resubmitted draft IA report. The first IAB opinion was issued on 2 June 2009.