HOUSE OF LORDS

SELECT COMMITTEE ON THE EUROPEAN UNION
Sub-Committee F (Home Affairs)

INQUIRY INTO
EU POLICY ON PROTECTING EUROPE FROM LARGE SCALE CYBER-ATTACKS

Call for Evidence

Sub-Committee F (Home Affairs) of the House of Lords Select Committee on the European Union is conducting an inquiry into **EU policy on protecting Europe from large scale cyber-attacks**.

Following on from the EU Directive 2008/114/EC "*on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection",* in March 2009 the EU Commission published a Communication on Critical National Infrastructure Protection entitled *"Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience"* (COM(2009)149 final, Council document 8375/09). This document was accompanied by 400+ pages of *"Impact Assessment"* (COM(2009)399 and 400, Council document 8375/09 ADD 1-4) setting out the background to the Commission's approach to this issue.

The Commission is concerned that an increasing number of vital services depend on digital systems, and in particular on a working Internet. Major economic or social damage could be caused if these digital systems are disrupted, either by "hacking" or "spamming" attacks, or as a result of technical failures, or as a side-effects of a natural disaster.

The Commission is especially concerned that intentional "cyber-attacks" are growing in sophistication and frequency, and that the risks that services now run are poorly understood and insufficiently analysed.

The proposal has four specific goals:

- to bridge gaps in national policies for security and resilience of critical systems;
- to enhance European governance of this area;
- to improve Europe's incidence response capability;
- to improve the resilience and stability of the Internet.

This inquiry will focus on what are the proper roles for the EU and its Member States in this important area, where many of the critical systems involved are operated by private industry and not – as was once the case for communications providers – by public bodies. The Sub-Committee welcomes evidence on all aspects of the inquiry, but in particular on the following issues:

Threat analysis

- How vulnerable is the Internet to wide-spread technical failures? To what extent is it likely to be affected by natural disasters?
- Is the Internet industry doing enough to ensure the resilience and stability of the Internet, or is regulatory intervention unavoidable? What are the cost implications if the industry volunteers, or is forced, to do more?
- The Commission is particularly concerned about cyber-attacks, and draws attention to events in Estonia in Spring 2007 and Georgia in August 2008. Is this concern justified?

- The events in Estonia led to a more public involvement by NATO in cyber-protection issues. Should the military be more involved in protecting the Internet?
- How concerned should be we be about criminally operated "botnets"? What evidence do we have that shows the scale of this problem, and the extent to which it can be tackled at the European level?

International responses

- The Commission believes that a pan-European approach is needed to identify and designate European Critical Infrastructures, and that national responses will be fragmented and inefficient. Is this analysis correct? Would multi-national companies be especially in favour of multi-national policies?
- The Commission draws attention to the emergence of "public-private partnerships" as the reference model for governance issues relating to critical infrastructure protection. However, they see no such partnerships at the European level and wish to encourage them. Are the Commission correct in this aim?
- Are there indeed market failures occurring so that there is inadequate preparation for high impact, low probability events? And if so, how should they be addressed?
- The Commission supports the European Information Sharing and Alert System (EISAS). Is it appropriate to develop this type of pan-European early warning and incident response capability?
- Are Government operated Computer Emergency Response Teams (CERTs) an appropriate mechanism for dealing with Internet incidents?
- Will the UK's existing approaches to this policy area be adversely affected by fitting in with a European-wide system – or will this lead to improvements?
- Is it sensible to develop European-centric approaches at all, or should there be much more emphasis on a worldwide approach? In particular, are US policies consistent with the proposed European approach to the problem?

European Network and Information Security Agency (ENISA)

- The Commission sees a major role for ENISA in developing national CERTs, and in assessing the development and deployment of EISAS. Is ENISA an appropriate body for this work?
- Is ENISA being effective in its role, or does it need reform?

Timescales

- Most of the Commission's plans are to be put into practice by the end of 2010. Is this timescale realistic?

GUIDANCE FOR THOSE SUBMITTING WRITTEN EVIDENCE

The deadline for submitting written evidence is Friday 13 November 2009.

Submissions should be sent to:

Michael Collon
Clerk to Sub-Committee F (Home Affairs)
Select Committee on the European Union,
House of Lords, London SW1A 0PW.

Telephone 020 7219 8650; Fax 020 7219 6715.

and also, or instead, as an email attachment in 'Word' to collonm@parliament.uk (Versions in Word are needed for evidence which is to be published.)

Please ensure that you include relevant contact details. Evidence should be attributed and dated, with a note of your name and position, and should state whether it is submitted on an individual or corporate basis.

Witnesses are encouraged to focus on those issues of which they have particular knowledge or experience; submissions are not required to cover all the questions.

Paragraphs should be numbered. If drawings or charts are included, we ask that they should be black-and-white and of camera-ready quality. Lengthy submissions should include a summary.

Evidence sent in hard copy should be clearly printed or typed on single sides of A4 paper, unstapled.

Evidence becomes the property of the Committee, and may be placed on the Committee's website, printed or circulated by the Committee at any stage. You may publicise or publish your evidence yourself, but in doing so you should indicate that it was prepared for the Committee. If your evidence is not printed, it will in due course be made available to the public in the Parliamentary Record Office.

Personal contact details supplied to the Committee will be removed from evidence before publication, but will be retained by the Committee Office for specific purposes relating to the Committee's work.

The Committee will invite some of those who submit written evidence to give oral evidence, usually in public at Westminster. Public sessions begin in November 2009 and will be broadcast live on the Internet. Transcripts of these sessions will also be published on the Parliamentary website www.parliament.uk/hleuf where progress of the inquiry can also be followed, and further details of the Sub-Committee's work can be found. The Weekly Bulletin of House of Lords Select Committees is available free from the Committee Office, House of Lords, London SW1A OPW (tel. 020 7219 4911).

This is a public call for evidence aimed at reaching a wide cross-section of informed opinion. Please bring it to the attention of other groups and individuals who may not have received a copy direct.

House of Lords
October 2009