2010 - House of Lords enquiry into EU Internal Security Strategy

This is JANET(UK)?s submission to the inquiry into the EU Internal Security Strategy [1] by the Home Affairs Sub-Committee of the House of Lords Select Committee on the European Union. JANET(UK) [2] is the operator of JANET, the UK?s National Research and Education Network, which connects universities, colleges, research organisations and regional schools networks to each other, to peer research networks in other countries and to the public Internet. Our evidence therefore relates only to Objective 3 of the Strategy ? Raise Levels of Security for Citizens and Businesses in Cyberspace ? and in particular to pages 9 and 10 of the Commission Communication ?ISS in Action [3]? (COM(2010) 673). JANET(UK) has operated a Computer Security Incident Response Team (CSIRT [4]) for its network and customers since 1993 and has participated in CSIRT cooperation activities in the UK, Europe and worldwide, including operating the EuroCERT pilot from 1997 to 1999.

In the area of **operational cooperation** we welcome the recognition in Action 3 of the important role of cooperating CSIRTs in dealing effectively with security incidents and promoting good preventive practice. Since many security incidents involve more than one country we strongly support the recommendation to increase the proportion of the European Internet that is covered by a CSIRT by encouraging the creation of at least a national CSIRT in each Member State and a CSIRT for the European Institutions. It is important that such CSIRTs are brought into existing trusted collaboration networks such as the European Government CERTs group [5], TERENA?s CSIRT Task Force [6] and the global Forum of Incident Response and Security Teams [7] (FIRST).

Since ENISA has provided, and continues to provide, an important facilitating role by gathering and promoting best practice in the field of Network and Information Security we welcome the proposal in Action 1 to provide a complementary body, working with ENISA, to gather and promote good practice in dealing with cybercrime. However we doubt that a direct operational role for such a body would be helpful since it would at best add an additional layer of organisational complexity and at worst disrupt existing bi- and multi-lateral working relationships between national cybercrime centres. The new body?s role, like that of ENISA and the EISAS discussed below, should be to ensure ? by developing, documenting and disseminating best practice ? that relationships between those centres exist and work effectively, not to replace them.

On **prevention and anticipation**, we welcome the focus in Action 2 on dealing with criminally illegal material at source rather than, as has been suggested elsewhere, attempting to create blocks that are likely to be ineffective at the technical level and do little either to address the crime or to help its victims. However processes for requiring material to be removed from Internet hosts must have a clear definition of what material is covered and effective and trusted safeguards (as provided, for example, by sections 3 & 4 of the *Terrorism Act 2006* [8] and the Internet Watch Foundation?s [9] handling of indecent images of children) otherwise there is a risk, as identified by the Law Commission [10] in 2002 for defamation law, of creating mechanisms that can be used to censor legitimate comment and criticism.

On Action 3?s proposal to create a European Information Sharing and Alert System (EISAS) we note and support the conclusion of ENISA?s 2007 report [11] that the most effective role for the EU is as a facilitator for national Information Sharing and Alert Systems (ISAS) ? such as the UK?s GetSafeOnline [12] ? rather than itself attempting to run an ISAS. This role would provide a clearing house to analyse and promote good practice in running national ISAS and a facilitator of discussions between those national Systems. Provided it is this facilitating role that is intended, we consider that the plan to work with ENISA to establish an operational service by 2013 should be achievable.

Links
[1] http://www.parliament.uk/business/committees/committees-a-z/lords-select/eu-home-affairs-sub-committee-f-/news/lords-committee-to-investigate-the-eu-internal-security-strategy/
[2] http://www.ja.net/
[3] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM%3A2010%3A0673%3AFIN%3AEN%3APDF
[4] http://www.ja.net/services/csirt/
[5] http://www.egc-group.org/
[6] http://www.terena.org/activities/tf-csirt/
[7] http://www.first.org/
[8] http://www.legislation.gov.uk/ukpga/2006/11/section/3
[9] http://www.iwf.org.uk/
[10] http://www.lawcom.gov.uk/docs/defamation2.pdf
[11] http://www.enisa.europa.eu/act/cert/other-work/files/EISAS_finalreport.pdf
[12] http://www.getsafeonline.org/