

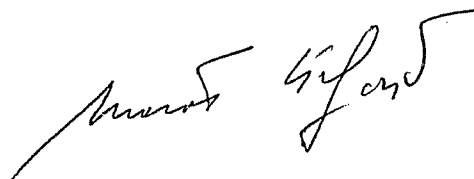
Brussels, 13/07/2010  
C/2010/4879

*Dear Lord Roper,*

*The European Commission would like to thank the European Union Select Committee of the House of Lords for the transmission of its report "Protecting Europe against large scale cyber-attacks" sent on 25 March 2010.*

*In line with the Commission's decision to encourage national Parliaments to react to its proposals in order to improve the process of policy formulation, we welcome this opportunity to respond to your comments. I enclose the Commission's reply and hope you will find this a valuable contribution to your own deliberations.*

*Yours sincerely,*



*Lord Roper  
Chairman of the European Union Select Committee  
House of Lords  
Palace of Westminster  
UK-London SW1A 0PW*



Brussels, June 2010

## **COMMENTS OF THE EUROPEAN COMMISSION ON A REPORT FROM THE HOUSE OF LORDS**

### **COM (2009) 149 ON CRITICAL INFORMATION INFRASTRUCTURE PROTECTION "PROTECTING EUROPE FROM LARGE SCALE CYBER-ATTACKS AND DISRUPTIONS: ENHANCING PREPAREDNESS, SECURITY AND RESILIENCE"**

#### **1. Scope of the Commission's Communication and the related action plan**

The Action Plan on Critical Information Infrastructure Protection (CIIP) proposed by the European Commission in March 2009 addresses the need for Europe to be better protected and prepared to cope with cyber disruptions caused by man-made attacks, natural disasters or technical failures. The proposed approach is an all-hazards one. Hence, COM(2009)149, hereafter referred to as the "CIIP Communication", is not concerned only with the three types of attacks mentioned in the House of Lords' report (point 18). As an example, attacks which aim to steal credit card numbers or to spy on human right activists come within the scope of the CIIP Communication. Indeed, all attacks targeting individuals might undermine the confidence and trust of citizens in information systems. This will have in turn a negative impact on the economy and on the development of the information society.

Additionally, the perspective proposed in the CIIP Communication is the need to address the security and resilience of Critical Information Infrastructures (CIIs) in a systemic perspective as the frontline of defence against failures and attacks. The actions proposed in the CIIP Action Plan are distinct and complementary to those to prevent, fight and prosecute criminal and terrorist activities using or against ICT infrastructures.

Finally, while Internet, and in particular its stability and resilience, is undeniably a key focus of the Communication, the CIIP Action Plan aims at enhancing the protection of all CIIs and not only the Internet.

#### **2. EU role**

The Impact Assessment of the CIIP Communication fully acknowledges the primary role of Member States in the sovereign protection of their critical infrastructure (in line with point 36 and 44 of the House of Lords' report). At the same time, it recognises that a purely national approach to tackle CIIP challenges may not be sufficient. Differences in national approaches and the lack of systematic cross-border co-operation can substantially reduce the effectiveness of domestic countermeasures. Hence, the intention of the CIIP Action Plan is to put forward an integrated EU-wide approach to usefully complement and bring European added value to the national CIIP programmes.

In particular, the CIIP Communication highlights that a European effort is needed to foster the development of awareness and common understanding of the challenges; stimulate the adoption of shared policy objectives and priorities; reinforce cooperation between Member States and integrate national policies in a more European and global dimension.

### **3. Global dimension**

The European Commission welcomes the finding that witnesses "(...) saw value in regional action, provided that it was proposed within a wider framework and led on to global initiatives" (point 30). The intention of the CIIP Action Plan is to foster pan-European cooperation and coordination as a basis for enhanced global cooperation. Indeed, "no country is an island" in this context. The global nature of CIIs, and in particular the Internet, requires a common global approach to security and resilience. It is via a strong EU coordination that a direct impact can be made at the international level.

Addressing CIIP at EU level is not seen by the European Commission as the "*second best option*" (point 41) in the absence of an international response. It is rather a necessary step, which builds itself on capabilities established at national level, conducive to an enhanced global response.

The House of Lords' report deems that the CIIP Communication says little about the role of the EU in a global context (point 54). However, concerning the global dimension of the challenge, the CIIP Communication has identified that the specificities of the Internet, i.e. the fact that it is intrinsically global and highly distributed, calls for a specific, targeted approach. In that context two converging measures have been identified. Firstly, to achieve a common understanding across the EU on what are the European priorities – both in terms of public policy and of operational deployment – to ensure the security and resilience of the Internet; secondly, to engage the global community in agreeing on a set of principles for Internet security and resilience, building upon strategic cooperation with third countries such as the USA, Japan and Canada and making sure that European values are preserved and promoted throughout the process.

Another important instrument to enhance the global response is the proposal made in the CIIP Action Plan to reflect on a practical way to extend at the global level the proposed national and pan-European exercises on large scale networks security incident. Pan-European exercises could be the operational platform for European participation in international network security incidents exercises like the US Cyber Storm.

### **4. Computer Emergency Response Teams (CERTs)**

The House of Lords' report urges the Commission, when responding to the report, to clarify its intentions with regards to the invitation to establish national CERTs in all Member States (point 71). In the CIIP Impact Assessment, the European Commission acknowledged that CERTs are not homogeneous entities, since existing facilities display different characteristics regarding ownership, services provided, constituency served and technical capabilities. National CERTs, for example, represent the point of contact for a whole nation. Sometimes this task is fulfilled by governmental CERTs which serve all governmental agencies and organisations and possibly all public-sector bodies. Hence, those countries which have already in place a sophisticated CERT network have also certainly established the functionality that should be ensured by a national CERT.

Consultations prior to the CIIP Communication highlighted differences in national systems of early warning and incident response. Some Member States do not routinely

receive network security incident reports and/or have not established an organisation as a focal reporting point. This hinders the pan-European and global cooperation with regards to early warning on incidents and problems resolution. The necessary and effective cooperation and information sharing between public entities implies that Member States need to agree on a common baseline in terms of early warning and response capabilities, for which National/Governmental CERTs are key elements. It is not the intention of the European Commission to impose a “one size fits all” model (point 64) with regard the organisation of such capability, which is left to the discretion and experience of Member States.

## **5. Private sector involvement in public private partnerships**

The European Commission shares the view of the House of Lords that "(..) *it is for the public sector to take the initiative and to offer to experienced Internet entrepreneurs a real say in how public private partnerships are best developed*" (point 79). This is why, in shaping the European Public-Private Partnership for Resilience (EP3R) as proposed in the CIIP communication, the European Commission has followed a step-by-step and bottom-up approach. All relevant stakeholders were invited to take part in the discussions on the necessary building blocks that would best match their requirements<sup>1</sup>.

## **6. EU and NATO**

The CIIP Action Plan takes into account the work conducted by NATO in the context of cyber-security, such as the common policy on cyber defence, the activities of the Cyber Defence Management Authority (CDMA), as well as the outputs of the NATO Cooperative Cyber Defence Centre of Excellence (CCD-COE).

It is very important to stress the different nature of NATO initiatives, which focus mainly on military defence, *vis-à-vis* the European Commission's CIIP initiative, which aims at enhancing a structured coordination and cooperation of civilian resources and capability across Member States. The European Commission is in contact with NATO to ensure coordination between these respective activities.

## **7. Timescales**

As highlighted in the House of Lords' report, the CIIP Communication defines a plan for immediate actions in the short to medium term (until 2011) that can be considered as ambitious. This timeline reflects the concern that we cannot afford to wait to achieve the preparedness and resilience that Europe needs in order to face the increasing level of cyber-threats and cyber-disruptions. We must act now and move rapidly.

At the same time, there is also the need to take account of the fact that enhancing the security and resilience of CIIs is a long term objective. This is why it is important to promote and pursue at the same time operational and tactical cooperation in the short-mid term (until 2011 – via the CIIP Communication) as well as strategic policy discussions for long-term scenarios of the Network and Information Security (NIS) policy in Europe (2012 and beyond). This is the focus of the debate launched in 2008, at the request of the Council and the European Parliament, to address the challenges and priorities for NIS policy, as well as the most appropriate instruments needed at EU level to tackle them, beyond 2012. The work conducted and the lessons learned under the CIIP

---

<sup>1</sup> See the elements of the consultation process on EP3R at the following address:  
[http://ec.europa.eu/information\\_society/policy/nis/strategy/activities/ciip/impl\\_activities/index\\_en.htm](http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/impl_activities/index_en.htm)

action plan will constitute an important input to the more general debate towards an increased and modernised European policy for network and information security.

## **8. The European Network and Information Security Agency (ENISA)**

The European Commission is currently finalising the Impact Assessment of options for the future of ENISA. The analysis takes into consideration the results of the public debate launched in 2008 on the direction of the European efforts towards an increased NIS. This debate was launched at the occasion of extending ENISA's mandate until March 2012<sup>2</sup>. As a first step, the Commission organised a workshop with national NIS experts and launched a public consultation on priorities and means for NIS policy that ended in January 2009<sup>3</sup>. The public consultation<sup>4</sup> carried out from 7 November 2008 to 9 January 2009 gathered a total of 596 contributions.

These discussions culminated in the adoption of the Council Resolution of 18 December 2009 on a collaborative European approach to Network and Information Security<sup>5</sup>. The debate showed a broad support for an Agency with a more flexible and permanent mandate and reinforcement of its resources. The European Commission is also considering the changes brought by the Lisbon Treaty.

ENISA, through its Executive Director, its Management Board and its Permanent Stakeholders Group, took part in this consultation process and will certainly have a say in the future steps (point 110).

Finally, concerning the possible extension of the scope of the work of ENISA before the expiry of the current mandate (point 111), it should be clarified that any extension of the mandate could be done only by amending the establishing Regulation. It is the Commission's intention to come forward soon with a proposal in this regard.

## **9. Conclusion**

The European Commission welcomes the support of the House of Lords and expects that via the proposed CIIP Action Plan, together with existing activities and instruments (such as ENISA) and with a common effort of the European Commission, Member States, the private sector and citizens, Europe can indeed tackle the most immediate challenges it faces and create a more conducive environment for a secure and resilient information society in Europe. This is one of the aims of the Digital Agenda for Europe that has been adopted last May the 19th.

---

<sup>2</sup> Regulation (EC) No 1007/2008 of 24.09.2008.

<sup>3</sup> See: [http://ec.europa.eu/information\\_society/policy/nis/nis\\_public\\_consultation/index\\_en.htm](http://ec.europa.eu/information_society/policy/nis/nis_public_consultation/index_en.htm).

<sup>4</sup> See: [http://ec.europa.eu/information\\_society/policy/nis/enisa/publicconsult/index\\_en.htm](http://ec.europa.eu/information_society/policy/nis/enisa/publicconsult/index_en.htm)

<sup>5</sup> See Council Resolution 2009/C 321/01 of 18 December 2009 at <http://eur-lex.europa.eu/LexUriServ/-LexUriServ.do?uri=OJ:C:2009:321:0001:0004:EN:PDF>.