COMMISSION OF THE EUROPEAN COMMUNITIES

Brussels, 30.3.2009
SEC(2009)400

COMMISSION STAFF WORKING DOCUMENT

Accompanying document to the

COMMUNICATION FROM THE COMMISSION TO THE COUNCIL, THE EUROPEAN PARLIAMENT, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS

on Critical Information Infrastructure Protection
"Protecting Europe from large scale cyber attacks and disruptions: enhancing preparedness, security and resilience"

SUMMARY OF THE IMPACT ASSESSMENT

{COM(2009) 149}
{SEC(2009) 399}

SUMMARY OF THE IMPACT ASSESSMENT

1. WHAT IS THE PROBLEM?

The ICT sector is vital for the EU economy and society

Information and Communication Technologies (ICTs) have become the backbone of the EU economy and society as a whole. **The ICT sector is vital for all segments of society**. **Businesses rely on the ICT sector** both in terms of direct sales and of efficiency/effectiveness of internal processes. ICTs are also **more and more pervasive for the functioning of governments and public administrations**: the uptake of e-Government services at all levels, while guaranteeing more efficient procedures, makes the public sector heavily dependent on ICTs for many operations. Last, not least, **citizens increasingly rely on Information Society services and use ICTs in their daily activities**: besides the negative effects a cyber-disruption would have on such activities, more and more personal data of citizens are communicated and transmitted electronically. Inadequate security measures could lead to loss of sensitive personal information and pose the risk of identity theft or other fraud.[1] **Enhancing the security and resilience of such infrastructures is, therefore, also absolutely vital for the protection of citizens' personal data and the proper enforcement of the right to privacy.**

ICT systems and services are a vital infrastructure *per se* as well as an underpinning platform for other critical technological and societal infrastructures. This was acknowledged in the European Commission Green Paper on a European Programme for Critical Infrastructure Protection which captured with the concept of **Critical Information Infrastructures (CII)** all "*ICT systems that are critical infrastructures for themselves or that are essential for the operation of critical infrastructures (telecommunications, computers/software, Internet, satellites, etc.)*"[2], similarly to the OECD approach[3].

Despite the existing terminological differences, **what is important is that the notion of CII is conducive to a systemic perspective to policies for the secure and continuous functioning of ICT systems, services, networks and infrastructures** ("ICT infrastructures") of which the **Internet is a very important component**, due to its widespread diffusion and the process of technological convergence.

---

1 http://www.timesonline.co.uk/tol/news/uk/crime/article4211711.ece
2 COM(2005) 576 final
3 http://www.oecd.org/dataoecd/1/13/40825404.pdf.

What is at stake?

The pervasiveness of CII implies that the effects of cyber-disruptions can be **widely felt on the whole society**.

The risks due to man-made attacks, natural disasters or technical failures are often not fully understood and/or analysed. Consequently, awareness across stakeholders is insufficient to devise adequate safeguards and countermeasures.

Cyber-attacks have risen to an unprecedented level of sophistication and are often performed by individuals or criminal groups for profit or political reasons. **The large scale cyber-attacks on Estonia, Lithuania and Georgia are examples of a general trend.** The huge number of viruses, worms and other malware, the expansion of botnets and the rise of spam confirm the severity of the problem[4]. **ICT infrastructures are under constant attack** and if Europe does not prepare itself the impact of attacks would be much more severe.

The high dependence on CII, their cross-border interconnectedness and interdependencies with other infrastructures, raise the need of **addressing their security and resilience in a systemic perspective as the frontline of defence** against failures and attacks, in addition and complementarily to measures to prevent, fight and prosecute criminal and terrorist activities targeting CII.

Nature of the problem

Presently, **the security and resilience of CII is mostly addressed on a national level, with little pan-European coordination. The lack of systematic cross-border co-operation substantially reduces the effectiveness of domestic countermeasures.** Moreover, the **low level of security and resilience of CII in one country has the potential to increase vulnerabilities and risks in others.**

Since CII are global, tightly interconnected and interdependent with other infrastructures, ensuring their security and resilience **can not be achieved via purely national and uncoordinated approaches.** Moreover, **it is a common perception that market forces do not provide sufficient incentives to the private sector for investing to protect CIIs at the level that governments would normally demand**.

The underlying causes for the general problem outlined above are:

- **uneven approach among Member States to public policies on security and resilience of CII**. There are differences in Member States' policies on the security and resilience of CII. In addition, the level of expertise and preparedness does not seem to be evenly distributed, as highlighted by the analysis of national approaches carried out by the Commission and confirmed by a report of the **European Network and Information Security Agency (ENISA)**[5];
- **difficult uptake of new, Europe-wide governance models**. Enhancing the security and the reliability of CII poses peculiar **governance challenges**. **Governments** are **responsible** for defining CII-related policies, but **involving the private sector is essential** for their **implementation**. **Public-private partnerships** (PPPs) have emerged nationally as the reference model to manage this combination of responsibilities. However, despite the general consensus that PPPs would also be desirable on a European level, they have not materialised so far;

---

4 COM(2006)688 final

5 http://www.enisa.europa.eu/doc/pdf/resilience/stock_taking_final_report_2008.pdf

- **limited European early warning and incident response capability**. Consultations highlighted differences in national systems of early warning and incident response. Some Member States do not routinely receive network security incident reports (although this may be done informally among some operators) and/or have not established an organisation as a focal reporting point. Co-operation and information sharing between **government-level entities** appears **under-developed** and hampered by the lack of trusted sharing and co-ordination mechanisms, which in turn **necessitate all National/Governmental Computer Emergency Response Teams** (CERTs) **to be well-functioning, i.e. have a common baseline in terms of capabilities**. In addition, **EU-level exercises and practical simulations**, a key element to enhance security and resilience of CII, are still in **embryonic state**;
- **low awareness on the risks for Internet security and resilience**. The Internet, thanks to its distributed, redundant design has proven so far to be a **fairly robust and resilient infrastructure**. However, it is fair to **question** its capability to continue withstanding the **rising number** of disruptions and cyber-attacks, considering its **phenomenal growth**, its **growing complexity** and the **emergence of new services**.

No country is an island. The global nature of CII, and in particular of 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.**

2. WHAT IS THE RATIONALE FOR EU ACTION?

A **purely national approach to tackle the problems outlined above may not be sufficient**. Due to significant cross-border effects, many threats to network and information security (NIS) have the potential to cause negative cross-border externalities which cannot be effectively dealt with nationally and can cause disruptions in other countries.

An integrated EU-wide approach to enhancing the security and resilience of CII would usefully complement and bring European value added to the national programmes for critical information infrastructure protection and to the existing cooperation schemes between Member States. As many challenges and issues are common a common approach would benefit all.

Discussions after the Estonian attack suggest that the effects of similar events can be limited by **preventive measures** – such as a more structured information exchange on a European level – and by **coordinated action** during the actual crisis. The Commission, fully respecting the **subsidiarity principle**, is ideally placed to coordinate such efforts, in close cooperation with Member States and other international organisations.

Moreover, national security concerns, while playing an important role in defining NIS policies and obligations, can lead to regulatory fragmentation and affect the competitiveness of the European Union as a whole and the wealth creation capabilities of the European single market.

In 2006, the Commission announced[6] its intention to develop, under the European Programme for Critical Infrastructure Protection[7] (EPCIP), a sector-specific policy for the ICT sector

[6] COM(2006) 251
[7] COM(2006) 786

"with a view to enhancing the security and the resilience of networks and information systems". This announcement was welcomed by the European Council in 2007.[8]

This initiative would take into due account the international dimension, building upon recognised principles like the G8 principles on CIIP, UN General Assembly Resolution 58/199 'Creation of a global culture of cyber-security and the protection of critical information infrastructures' and the recent OECD Recommendation on the Protection of CII.

Last, but not least, the proposed policy initiative takes into account and does not duplicate the NATO cyber-security activities, whose focus is on military fence – i.e. the common policy on cyber defence and 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).

3. WHAT ARE THE OBJECTIVES?

The aim of this initiative would be **to enhance the level of preparedness and response across Europe** against the described risks and threats, avoiding a fragmented approach by Member States. The focus would be on defining shared processes to flexibly cope with known and unknown threats. Relevant public and private stakeholders would be engaged in ensuring that **adequate and consistent levels of preventive, detection, emergency and recovery measures** are put in operation to achieve **the proper level of security and resilience of CII and guarantee the continuity of services**. The improved security and resilience would also have **a positive impact on the protection of personal data and privacy of EU citizens**.

The general objective of this proposal, i.e. to **ensure security and resilience of CII as the frontline of defence**, can be achieved via four specific objectives:

(1) Bridging gaps in national policies for the security and resilience of CII;

(2) Enhancing European governance for the security and resilience of CII;

(3) Strengthening Europe's operational incident response capability;

(4) Enhancing Internet security and resilience.

4. WHAT ARE THE POLICY OPTIONS?

Policy option 1: Business as usual

Not proposing any further action would not be a viable option. Without horizontal actions at EU level, Member States would continue acting individually or in the frame of bilateral or limited multilateral basis. There would be a **risk linked to the evolution of different national approaches,** which might be incompatible. In addition, cooperation across boundaries would be *ad hoc* and may be ineffective due to the sophistication and scale of cyber-attacks.

Since Member States would continue to address these issues at different paces, stakeholders **might refrain from investing in security and resilience**, as the multitude of standards and obligations would decrease their competitiveness. The cross-border nature of the problem would accentuate the differences in security, resilience and preparedness across Europe.The vulnerability of CII in Europe would remain high and possibly rise, despite individual efforts.

Policy option 2: non-binding framework

[8] Council Resolution 2007/C 68/01

The Commission would **provide the framework for coordination and cooperation**, taking the form of a Communication and an Action Plan to engage Members States, the private sector and civil society. The Communication could be endorsed by the Council of the EU and the European Parliament may also decide to contribute to the discussion.

The initiative would focus on the objectives highlighted above, and specifically propose to:

(1) **Promote coherence between national policies for the security and resilience of CII** by:

- identifying transferable examples of public policy practices and commonalities;
- establishing a European Forum for Member States to share information and good policy practices on security and resilience for CII.

(2) **Enhance European governance for the security and resilience of CII** by:

- launching a **European Public Private Partnership for Resilience (E3PR)** to foster cooperation between public and private sectors on security and resilience objectives, baseline requirements, good policy practices and measures.

(3) **Strengthen Europe's operational incident response capability** by:

- establishing well functioning national/governmental CERTs[9] as the key component for national capability for preparedness, information sharing, coordination and response;
- agreeing on a minimum level of capabilities and services for national/governmental CERTs;
- fostering the European cooperation of national/governmental CERTs; easing the contact and cooperation between national response capabilities; organising pan-European and/or regional exercises on simulated large-scale incidents;
- promoting contingency planning for network incident response and disaster recovery;
- funding the development of European exercises on simulated large-scale network security incidents;
- supporting the development and deployment of a European Information Sharing and Alert System (EISAS) to reach out in an equal and effective manner to citizens and SMEs.

(4) **Enhance Internet security and resilience** by:

- defining EU priorities for Internet long term stability and resilience;
- agreeing on a set of European and then International principles for Internet security and resilience.

Policy option 3: binding framework

Most of the issues mentioned above would be addressed through a number of binding measures, which may take the form of a Directive, a Regulation or a Decision, as appropriate.

The Commission may propose binding measures to:

[9] Computer Emergency Response Teams

(1) **define a baseline that would harmonise national policies**. Such measures may focus on additional security and resilience of CII outside the framework of the market legislation already proposed;

(2) **define the role and responsibility of public and private stakeholders** in security and resilience of CII;

(3) **improve operational preparedness**, e.g. via :

(a) a minimal set of standards for harmonised level functions and services for National/Governmental CERTs;

(b) a framework for national contingency planning with a view to develop EU-wide contingency plans.

5. HOW DO THE POLICY OPTIONS COMPARE?

The "business as usual" policy option **does not present any clear strength** in terms of improving the security and resilience of CII in Europe. The decision is, therefore, between a non-binding and a binding framework. At this point in time, the "binding framework" option does not seem feasible, due to *inter alia*:

- the **political reality** of sovereign states, which any NIS policy at the Community level must duly take into account;
- the need to consider the widely distributed operational responsibility in the private sector;
- the lack of accumulated experience in information sharing and cooperation on CII policies between public and private sectors.

In addition, the **low quality of data** currently available on security incidents – due to information asymmetries and national security concerns – hampers the possibility to define regulatory measures in a consistent economic and public policy perspective and poses a **problem to respect the principle of proportionality**, as it is impossible to propose proportionate actions when the precise extent of the problem is not well understood.

Lastly, the timeframe of a binding framework approach, due to the lengthy adoption process, would be incompatible with the need for all stakeholders to act rapidly.

In conclusion, this impact assessment suggests that in the short- and medium-term, policy option 2 is preferable, immediately launching the proposed actions and, in due course, reviewing results, including those of the public debate towards a reinforced and modernised NIS policy in EU. These would then be the basis for assessing needs and options concerning possible future binding measures.

It might then be possible to recommend the implementation of actions similar to those of policy option 3.