EN

COMMISSION OF THE EUROPEAN COMMUNITIES

Brussels, 30.3.2009
COM(2009) 149 final

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, 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"

{SEC(2009) 399}
{SEC(2009) 400}

(presented by the Commission)

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, 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"

1. INTRODUCTION

Information and Communication Technologies (ICTs) are increasingly intertwined in our daily activities. Some of these ICT systems, services, networks and infrastructures (in short, ICT infrastructures) form a vital part of European economy and society, either providing essential goods and services or constituting the underpinning platform of other critical infrastructures. They are typically regarded as critical information infrastructures (CIIs)[1] as their disruption or destruction would have a serious impact on vital societal functions. Recent examples include the large-scale cyber-attacks targeting Estonia in 2007 and the breaks of transcontinental cables in 2008.

The World Economic Forum estimated in 2008 that there is a 10 to 20% probability of a major CII breakdown in the next 10 years, with a potential global economic cost of approximately 250 billion US$.[2]

This Communication focuses on prevention, preparedness and awareness and defines a plan of immediate actions to strengthen the security and resilience of CIIs. This focus is consistent with the debate launched at the request of the Council and the European Parliament to addresses the challenges and priorities for network and information security (NIS) policy and the most appropriate instruments needed at EU level to tackle them. The proposed actions are also complementary to those to prevent, fight and prosecute criminal and terrorist activities targeting CIIs and synergetic with current and prospective EU research efforts in the field of network and information security, as well as with international initiatives in this area.

2. THE POLICY CONTEXT

This Communication develops the European policy to strengthen the security of and the trust in the information society. Already in 2005, the Commission[3] highlighted the urgent need to coordinate efforts to build trust and confidence of stakeholders in electronic communications and services. To this end a strategy for a secure information society[4] was adopted in 2006. Its main elements, including the security and resilience of ICT infrastructures, were endorsed in Council Resolution 2007/068/01. However, ownership and implementation by stakeholders appear insufficient. This strategy also strengthens the role, on tactical and operational levels,

[1] A definition of CIIs was proposed in COM(2005) 576 final

[2] Global Risks 2008

[3] COM(2005) 229

[4] COM(2006) 251

of the European Network and Information Security Agency (ENISA), established in 2004 to contribute to the goals of ensuring a high and effective level of NIS within the Community and developing a culture of NIS for the benefit of EU citizens, consumers, enterprises and administrations.

In 2008 ENISA's mandate was extended *'à l'identique'* until March 2012.[5] At the same time, the Council and the European Parliament called for *"further discussion on the future of ENISA and on the general direction of the European efforts towards an increased network and information security."* To support this debate, the Commission launched last November an on-line public consultation,[6] the analysis of which will be made available shortly.

The activities planned in this Communication are conducted under and in parallel to the European Programme for Critical Infrastructure Protection (EPCIP)[7]. A key element of EPCIP is the Directive[8] on the identification and designation of European Critical Infrastructures,[9] which identifies the ICT sector as a future priority sector. Another important element of EPCIP is the Critical Infrastructure Warning Information Network (CIWIN).[10]

On the regulatory side, the Commission proposal to reform the Regulatory Framework for electronic communications networks and services[11] contains new provisions on security and integrity, in particular to strengthen operators' obligations to ensure that appropriate measures are taken to meet identified risks, guarantee the continuity of supply of services and notify security breaches.[12] This approach is conducive to the general objective of enhancing the security and resilience of CIIs. The European Parliament and the Council broadly support these provisions.

The actions proposed in this Communication complement existing and prospective measures in the area of police and judicial cooperation to prevent, fight and prosecute criminal and terrorist activities targeting ICT infrastructures, as envisaged *inter alia* by the Council Framework Decision on attacks against information systems[13] and its planned update.[14]

This initiative takes into account NATO activities on common policy on cyber defence, i.e. the Cyber Defence Management Authority and the Cooperative Cyber Defence Centre of Excellence.

Lastly, due account is given to international policy developments, in particular to the G8 principles on CIIP[15]; the UN General Assembly Resolution 58/199 *Creation of a global culture of cybersecurity and the protection of critical information infrastructures* and the recent OECD Recommendation on the Protection of Critical Information Infrastructures.

[5] Regulation (EC) No 1007/2008

[6] http://ec.europa.eu/information_society/newsroom/cf/itemlongdetail.cfm?item_id=4464

[7] COM(2006) 786 final

[8] 2008/114/EC

[9] http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressData/en/gena/104617.pdf

[10] COM(2008) 676 final

[11] COM(2007) 697, COM(2007) 698, COM(2007) 699

[12] Art. 13 Framework Directive

[13] 2005/222/JHA

[14] COM(2008) 712

[15] http://www.usdoj.gov/criminal/cybercrime/g82004/G8_CIIP_Principles.pdf

3. WHAT IS AT STAKE

3.1. Critical information infrastructures are vital for the economy and societal growth of the EU

The economic and societal role of the ICT sector and ICT infrastructures is highlighted in recent reports on innovation and economic growth. This includes the Communication on i2010 mid-term review[16], the Aho Group report[17] and the European Union yearly economic reports.[18] The OECD underlines the importance of ICTs and the Internet "*to boost economic performance and social well-being, and to strengthen societies' capacity to improve the quality of life for citizens worldwide*"[19]. It further recommends policies that strengthen confidence in the Internet infrastructure.

The ICT sector is vital for all segments of society. Businesses rely on the ICT sector both in terms of direct sales and for the efficiency of internal processes. ICTs are a critical component of innovation and are responsible for nearly 40% of productivity growth.[20] ICTs are also pervasive for the work of governments and public administrations: the uptake of eGovernment services at all levels, as well as new applications such as innovative solutions related to health, energy and political participation, make the public sector heavily dependent on ICTs. Last, not least, citizens increasingly rely on and use ICTs in their daily activities: strengthening CII security would increase citizens' trust in ICTs, not least thanks to a better protection of personal data and privacy.

3.2. The risks to critical information infrastructures

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

Cyber-attacks have risen to an unprecedented level of sophistication. Simple experiments are now turning into sophisticated activities performed for profit or political reasons. The recent large scale cyber-attacks on Estonia, Lithuania and Georgia are the most widely covered examples of a general trend. The huge number of viruses, worms and other forms of malware, the expansion of botnets and the continuous rise of spam confirm the severity of the problem.[21]

The high dependence on CIIs, their cross-border interconnectedness and interdependencies with other infrastructures, as well as the vulnerabilities and threats they face raise the need to address their security and resilience in a systemic perspective as the frontline of defence against failures and attacks.

[16] COM(2008) 199 final

[17] http://ec.europa.eu/invest-in-research/action/2006_ahogroup_en.htm

[18] EU Economy 2007 Review http://ec.europa.eu/economy_finance/publications/publication10130_en.pdf

[19] http://www.oecd.org/dataoecd/1/29/40821707.pdf

[20] http://epp.eurostat.ec.europa.eu/ - Science and Technology/Information Society

[21] COM(2006) 688 final

3.3. Security and resilience of critical information infrastructures to boost confidence in the information society

In order to ensure that ICT infrastructures are used to their maximum extent, thus fully realising the economic and social opportunities of the information society, all stakeholders must have a high level of confidence and trust in them. This depends on various elements, the most important of which is ensuring their high level of security and resilience. Diversity, openness, interoperability, usability, transparency, accountability, auditability of the different components and competition are key drivers for security development and stimulate the deployment of security-enhancing products, processes and services. As the Commission already highlighted[22], this is a shared responsibility: no single stakeholder has the means to ensure the security and resilience of all ICT infrastructures and to carry all the related responsibilities.

Taking up such responsibilities calls for a risk management approach and culture, able to respond to known threats and anticipate unknown future ones, without over-reacting and stifling the emergence of innovative services and applications.

3.4. The challenges for Europe

In addition and complementarily to all the activities related to the implementation of the Directive on the identification and designation of the European Critical Infrastructures, in particular the identification of ICT sector-specific criteria, a number of broader challenges need to be addressed in order to strengthen the security and resilience of CIIs.

3.4.1. Uneven and uncoordinated national approaches

Although there are commonalities among the challenges and the issues faced, measures and regimes to ensure the security and resilience of CIIs, as well as the level of expertise and preparedness, differ across Member States.

A purely national approach runs the risk of producing a fragmentation and inefficiency across Europe. Differences in national approaches and the lack of systematic cross-border co-operation substantially reduce the effectiveness of domestic countermeasures, *inter alia* because, due to the interconnectedness of CIIs, a low level of security and resilience of CIIs in a country has the potential to increase vulnerabilities and risks in other ones.

To overcome this situation a European effort is needed to bring added value to national policies and programmes by fostering the development of awareness and common understanding of the challenges; stimulating the adoption of shared policy objectives and priorities; reinforcing cooperation between Member States and integrating national policies in a more European and global dimension.

3.4.2. Need for a new European governance model for CIIs

Enhancing the security and the resilience of CIIs poses peculiar governance challenges. While Member States remain ultimately responsible for defining CII-related policies, their implementation depends on the involvement of the private sector, which owns or controls a large number of CIIs. On the other hand, markets do not always provide sufficient incentives

[22] COM(2006) 251 final

for the private sector to invest in the protection of CIIs at the level that governments would normally demand.

To address this governance problem public-private partnerships (PPPs) have emerged at the national level as the reference model. However, despite the consensus that PPPs would also be desirable on a European level, European PPPs have not materialised so far. A Europe-wide multi-stakeholder governance framework, which may include an enhanced role of ENISA, could foster the involvement of the private sector in the definition of strategic public policy objectives as well as operational priorities and measures. This framework would bridge the gap between national policy-making and operational reality on the ground.

3.4.3. Limited European early warning and incident response capability

Governance mechanisms will be truly effective only if all participants have reliable information to act upon. This is particularly relevant for governments that have the ultimate responsibility to ensure the security and well-being of citizens.

However, processes and practices for monitoring and reporting network security incidents differ significantly across Member States. Some do not have a reference organisation as a monitoring point. More importantly, cooperation and information sharing between Member States of reliable and actionable data on security incidents appears underdeveloped, being either informal or limited to bilateral or limitedly multilateral exchanges. In addition, simulating incidents and running exercises to test response capabilities are strategic in enhancing the security and resilience of CIIs, in particular by focusing on flexible strategies and processes for dealing with the unpredictability of potential crises. In the EU, cyber-security exercises are still in an embryonic state. Exercises running across national boundaries are very limited. As recent events[23] showed, mutual aid is an essential element of a proper response to large-scale threats and attacks to CIIs.

A strong European early warning and incident response capability has to rely on well-functioning National/Governmental Computer Emergency Response Teams (CERTs), i.e. having a common baseline in terms of capabilities. These bodies need to act as national catalysers of stakeholders' interests and capacity for public policy activities (including those related to information and alert sharing systems reaching out to citizens and SMEs) and to engage in effective cross-border cooperation and information exchange, possibly leveraging existing organisations such as the European Governmental CERTs Group (EGC).[24]

3.4.4. International cooperation

The rise of the Internet as a key CII requires particular attention to its resilience and stability. The Internet, thanks to its distributed, redundant design has proven to be a very robust infrastructure. However, its phenomenal growth produced a rising physical and logical complexity and the emergence of new services and uses: it is fair to question the capability of the Internet to withstand the rising number of disruptions and cyber-attacks.

The divergence of views on the criticality of the elements making up the Internet partly explains the diversity of governmental positions expressed in international fora and the often contradicting perceptions of the importance of this matter. This could hinder a proper

[23] http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/large_scale/

[24] http://www.egc-group.org/

prevention of, preparedness for and ability to recover from threats affecting the Internet. For example, the consequences of the transition from IPv4 to IPv6 should also be assessed in terms of CII security.

The Internet is a global and highly distributed network of networks, with control centres not necessarily following national boundaries. This calls for a specific, targeted approach in order to ensure its resilience and stability, based on two converging measures. First, achieving a common consensus on the European priorities for the resilience and stability of the Internet, in terms of public policy and of operational deployment. Secondly, engaging the global community to develop a set of principles, reflecting European core values, for Internet resilience and stability, in the framework of our strategic dialogue and cooperation with third countries and international organisations. These activities would build upon the recognition by the World Summit on Information Society[25] of the key importance of the stability of the Internet.

4. THE WAY FORWARD: TOWARDS MORE EU COORDINATION AND COOPERATION

Because of the Community and international dimension of the problem an integrated EU approach to enhance the security and resilience of CIIs would complement and add value to national programmes as well as to the existing bilateral and multilateral cooperation schemes between Member States.

Public policy discussions in the aftermath of the events in Estonia suggest that the effects of similar attacks can be limited by preventive measures and by coordinated action during the actual crisis. A more structured exchange of information and good practices across the EU could considerably facilitate fighting cross-border threats.

It is necessary to strengthen the existing instruments for cooperation, including ENISA, and, if necessary, create new tools. A multi-stakeholder, multi-level approach is essential, taking place at the European level while fully respecting and complementing national responsibilities.

A thorough understanding of the environment and constraints is necessary. For example, the distributed nature of the Internet, where edge nodes can be used as vectors of attack, e.g. botnets, is a concern. However, this distributed nature is a key component of stability and resilience and can help a faster recovery than would normally be the case with over-formalised, top-down procedures. This calls for a cautious, case-by-case analysis of public policies and operational procedures to put in place.

The time horizon is also important. There is a clear need to act now and put rapidly in place the necessary elements to build a framework that will enable us to respond to current challenges and that will feed into the future strategy for network and information security.

Five pillars are proposed to tackle these challenges:

(1) Preparedness and prevention: to ensure preparedness at all levels;

(2) Detection and response: to provide adequate early warning mechanisms;

[25] Tunis Agenda for the Information Society, http://www.itu.int/wsis/docs2/tunis/off/6rev1.html

(3) Mitigation and recovery: to reinforce EU defence mechanisms for CII;

(4) International cooperation: to promote EU priorities internationally;

(5) Criteria for the ICT sector: to support the implementation of the Directive on the Identification and Designation of European Critical Infrastructures[26].

5. THE ACTION PLAN

5.1. Preparedness and prevention

Baseline of capabilities and services for pan-European cooperation. The Commission invites Member States and concerned stakeholders to

- define, with the support of ENISA, a minimum level of capabilities and services for National/Governmental CERTs and incident response operations in support to pan-European cooperation.
- make sure National/Governmental CERTs act as the key component of national capability for preparedness, information sharing, coordination and response.

Target: end of 2010 for agreeing on minimum standards; end of 2011 for establishing well functioning National/Governmental CERTs in all Member States.

European Public Private Partnership for Resilience (EP3R). The Commission will

- foster the cooperation between the public and the private sector on security and resilience objectives, baseline requirements, good policy practices and measures. The primary focus of the EP3R would be on the European dimension from strategic (e.g. good policy practices) and tactical/operational (e.g. industrial deployment) perspectives. EP3R should build upon and complement existing national initiatives and the operational activities of ENISA.

Target: end of 2009 for a roadmap and plan for EP3R; mid of 2010 for establishing EP3R; end of 2010 for EP3R to produce its first results.

European Forum for information sharing between Member States. The Commission will

- establish a European Forum for Member States to share information and good policy practices on security and resilience of CIIs. This would benefit from the results of the activities of other organisations, in particular ENISA.

Target: end of 2009 for launching the Forum; end of 2010 for delivering the first results.

5.2. Detection and response

European Information Sharing and Alert System (EISAS). The Commission supports

[26] Council Directive 2008/114/EC

the development and deployment of EISAS, reaching out to citizens and SMEs and being based on national and private sector information and alert sharing systems. The Commission financially supports two complementary prototyping projects.[27] ENISA is called upon to take stock of the results of these projects and other national initiatives and produce a roadmap to further the development and deployment of EISAS.

Target: end of 2010 for completing the prototyping projects; end of 2010 for the roadmap towards a European- system.

5.3. Mitigation and recovery

National contingency planning and exercises. The Commission invites Member States to

- develop national contingency plans and organise regular exercises for large scale networks security incident response and disaster recovery, as a step towards closer pan-European coordination. National/Governmental CERTs/CSIRTs may be tasked to lead national contingency planning exercises and testing, involving private and public sector stakeholders. The involvement of ENISA is called upon to support the exchange of good practices between Member States.

Target: end of 2010 for running at least one national exercise in every Member State.

Pan-European exercises on large-scale network security incidents. The Commission will

- financially support the development of pan-European exercises on Internet security incidents,[28] which may also constitute the operational platform for pan-European participation in international network security incidents exercises, like the US Cyber Storm.

Target: end of 2010 for the design and run of the first pan-European exercise; end of 2010 for pan-European participation in international exercises.

Reinforced cooperation between National/Governmental CERTs. The Commission invites Member States to

- strengthen the cooperation between National/Governmental CERTs, also by leveraging and expanding existing cooperation mechanisms like the EGC.[29] The active role of ENISA is called upon to stimulate and support pan-European cooperation between National/Governmental CERTs that should lead to enhanced preparedness; reinforced European capacity to react and respond to incidents; pan-European (and/or regional) exercises.

Target: end of 2010 for doubling the number of national bodies participating in ECG; end of 2010 for ENISA to develop reference materials to support pan-European cooperation.

[27] Under the EC Programme "*Prevention, Preparedness and Consequence Management of terrorism and other Security Related Risks*" http://ec.europa.eu/justice_home/funding/cips/funding_cips_en.htm

[28] *Supra* 27

[29] *Supra* 24

5.4. International cooperation

Internet resilience and stability. Three complementary activities are envisaged

- European priorities on long term Internet resilience and stability. The Commission will drive a Europe-wide debate, involving all relevant public and private stakeholders, to define EU priorities for the long term resilience and stability of the Internet.

Target: end of 2010 for EU priorities on critical Internet components and issues.

- Principles and guidelines for Internet resilience and stability (European level). The Commission will work with Member States to define guidelines for the resilience and stability of the Internet, focusing *inter alia* on regional remedial actions, mutual assistance agreements, coordinated recovery and continuity strategies, geographical distribution of critical Internet resources, technological safeguards in the architecture and protocols of the Internet, replication and diversity of services and data. The Commission is already funding a task force for DNS resiliency that, together with other relevant projects, will help build the consensus.[30]

Target: end of 2009 for a European roadmap towards principles and guidelines for Internet resilience and stability; end of 2010 for agreeing on the first draft of such principles and guidelines.

- Principles and guidelines for Internet resilience and stability (global level). The Commission will work with Member States on a roadmap to promote principles and guidelines at the global level. Strategic cooperation with third countries will be developed, notably in Information Society dialogues, as a vehicle to build global consensus.[31]

Target: beginning of 2010 for a roadmap for international cooperation on principles and guidelines for security and resilience; end of 2010 for the first draft of internationally recognised principles and guidelines to be discussed with third countries and in relevant fora, including the Internet Governance Forum.

Global exercises on recovery and mitigation of large scale Internet incidents. The Commission invites European stakeholders to

- reflect on a practical way to extend at the global level the exercises being conducted under the mitigation and recovery pillar, building upon regional contingency plans and capabilities.

Target: end of 2010 for the Commission to propose a framework and a roadmap to support the European involvement and participation in global exercises on recovery and mitigation of large-scale Internet incidents.

[30] *Supra* 27

[31] COM(2008)588 final

5.5. Criteria for European Critical Infrastructures in the ICT sector

ICT sector specific criteria. By building on the initial activity carried out in 2008, the Commission will

- continue to develop, in cooperation with Member States and all relevant stakeholders, the criteria for identifying European critical infrastructures for the ICT sector. To this end, relevant information will be drawn from a specific study being launched.[32]

Target: first half of 2010 for the Commission to define the criteria for the European critical infrastructures for the ICT sector.

6. CONCLUSIONS

Security and resilience of CIIs are the frontline of defence against failures and attacks. Their enhancement across the EU is essential to reap the full benefits of the information society. To achieve this ambitious objective an action plan is proposed to reinforce the tactical and operational cooperation at the European level. The success of these actions depends on their effectiveness to build upon and benefit public and private sector's activities, on the commitment and full participation of Member States, European Institutions and stakeholders.

To this end, a Ministerial Conference will take place on 27-28 April 2009 to discuss the proposed initiatives with Member States and to mark their commitment to the debate on a modernised and reinforced NIS policy in Europe.

Lastly, enhancing the security and resilience of CIIs is a long term objective, whose strategy and measures need regular assessments. Therefore, since this goal is consistent with the general debate on the future of network and information security policy in the EU after 2012, the Commission will initiate a stock-taking exercise toward the end of 2010, in order to evaluate the first phase of actions and to identify and propose further measures, as appropriate.

[32] *Supra* 27