Alþingi
Erindi nr. 140/754
komudagur 9.12.2011

EUROPEAN COMMISSION

Brussels, 31.3.2011
COM(2011) 163 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

'Achievements and next steps: towards global cyber-security'

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

'Achievements and next steps: towards global cyber-security'

1. INTRODUCTION

On 30 March 2009, the Commission adopted a Communication on Critical Information Infrastructure Protection – 'Protecting Europe from large scale cyber-attacks and cyber-disruptions: enhancing preparedness, security and resilience'[1] setting out a plan (the 'CIIP action plan') to strengthen the security and resilience of vital Information and Communication Technology (ICT) infrastructures. The aim was to stimulate and support the development of a high level of preparedness, security and resilience capabilities both at national and European level. This approach was broadly endorsed by the Council in 2009.[2]

The CIIP action plan is built on five pillars: preparedness and prevention, detection and response, mitigation and recovery, international cooperation and criteria for European Critical Infrastructures in the field of ICT. It sets out the work to be done under each pillar by the Commission, the Member States and/or industry, with the support of the European Network and Information Security Agency (ENISA).

The Digital Agenda for Europe[3] (DAE), adopted in May 2010, and the related Council Conclusions[4] highlighted the shared understanding that trust and security are fundamental pre-conditions for the wide uptake of ICT and therefore for achieving the objectives of the 'smart growth' dimension of the Europe 2020 Strategy.[5] The DAE emphasises the need for all stakeholders to join their forces in a holistic effort to ensure the security and resilience of ICT infrastructures, by focusing on prevention, preparedness and awareness, as well as to develop effective and coordinated mechanisms to respond to new and increasingly sophisticated forms of cyber-attacks and cyber-crime. This approach ensures that both the preventive and the reactive dimensions of the challenge are duly taken into account.

The following measures, announced in the Digital Agenda, have been taken in the last months: the Commission adopted on September 2010 a proposal for a Directive on attacks against information systems.[6] It aims to strengthen the fight against cyber-crime by approximating Member States' criminal law systems and improving cooperation between judicial and other competent authorities. It also introduces provisions to deal with new forms of cyber-attacks, in particular botnets. Complementing this, the Commission at the same time

---

1 COM(2009) 149

2 Council Resolution of 18 December 2009 on a collaborative European approach to Network and Information Security (2009/C 321/01)

3 COM(2010) 245

4 Council Conclusions of 31 May 2010 on Digital Agenda for Europe (10130/10)

5 COM(2010) 2020 and Conclusions of the European Council of 25/26 March 2010 (EUCO 7/10)

6 COM(2010) 517 final

tabled a proposal[7] for a new mandate to strengthen and modernise the European Network and Information Security Agency (ENISA) in order to boost trust and network security. Strengthening and modernising ENISA will help the EU, Member States and private stakeholders develop their capabilities and preparedness to prevent, detect and respond to cyber-security challenges.

Last but not least, the DAE, the Stockholm Programme/Action Plan[8] and the EU Internal Security Strategy in action[9] (ISS) underline the Commission's commitment to building a digital environment where every European can fully express his or her economic and social potential.

This Communication takes stock of the results achieved since the adoption of the CIIP action plan in 2009. It describes the next steps planned for each action at both European and international level. It also focuses on the global dimension of the challenges and the importance of boosting cooperation among Member States and the private sector at national, European and international level, in order to address global interdependencies.

2. AN EVOLVING SCENARIO

The impact assessment accompanying the CIIP action plan[10] and a broad array of analyses and reports by private and public stakeholders highlight not only Europe's social, political and economic dependencies on ICT, but also the steady growth in the number, scope, sophistication and potential impact of threats – be they natural or man-made.

New and technologically more sophisticated threats have emerged. Their global geo-political dimension is becoming progressively clearer. We are witnessing a trend towards using ICT for political, economic and military predominance, including through offensive capabilities. 'Cyber-warfare' or 'cyber-terrorism' are sometimes mentioned in this context.

In addition, as illustrated in the recent South Mediterranean events, some regimes are also ready and able to arbitrarily deprive or disrupt their own citizen's access to IT means of communication - notably Internet and mobile communications - for political purposes. Such unilateral domestic interventions may in turn have severe effects on other parts of the world[11].

In order to gain a more comprehensive understanding of these various threats, it can be useful to regroup them along the following categories:

- **exploitation** purposes, such as "advanced persistent threats"[12] for economic and political espionage purposes (e.g. GhostNet[13]), identity theft, the recent attacks against the Emissions Trading System[14] or against government IT systems[15];

---

7 COM(2010) 521
8 COM(2010) 171
9 COM(2010) 673
10 SEC(2009) 399
11 Joint communication on a partnership for democracy and shared prosperity with the Southern Meditarranean ; COM(2011)200 of 08.03.2011.
12 I.e. continuous and coordinated attacks against government agencies and the public sector. It is now becoming an issue for the private sector (see the "RSA 2011 cybercrime trends report").
13 See the reports by the Information Warfare Monitor project: "Tracking GhostNet: investigating a Cyber Espionage Network" (2009) and "Shadows in the Cloud: Investigating Cyber Espionage 2.0" (2010).

- **disruption** purposes, such as Distributed Denial of Service attacks or spamming generated via botnets (e.g. the Conficker network of 7 million machines and the Spanish-based Mariposa network of 12.7 million machines[16]), Stuxnet[17] and cut-off of communication means;

- **destruction** purposes. This is a scenario that has not yet materialised but, given the increasing pervasiveness of ICT in Critical Infrastructures (e.g. smart grids and water systems), it cannot be ruled out for the years to come.[18]

3. THE EUROPEAN UNION AND THE GLOBAL CONTEXT

The challenges ahead are neither specific to the European Union (EU), nor can they be overcome by the EU on its own. The pervasiveness of ICT and of the Internet allows more efficient, effective and economic communication, coordination and cooperation among stakeholders and results in a vibrant ecosystem of innovation in all fields of life. However, threats can now originate from anywhere in the world and, due to global interconnectedness, impact any part of the world.

A purely European approach is not sufficient to address the challenges ahead. Although the objective of building a coherent and cooperative approach within the EU remains as important as ever, it needs to be embedded into a global coordination strategy reaching out to key partners, be they individual nations or relevant international organisations.

We need to work towards a global understanding of the risks involved in the widespread, massive use of ICT by all segments of society. Even more, we need to devise strategies to appropriately and effectively manage – prevent, counter, mitigate and react to – these risks. The DAE calls for the "*cooperation of relevant actors [...] to be organised at global level to be effectively able to fight and mitigate security threats*" and sets out the goal to '*work with global stakeholders notably to strengthen **global risk management** in the digital and in the physical sphere and conduct internationally coordinated targeted actions against computer-based crime and security attacks*'.

4. THE IMPLEMENTATION OF THE CIIP ACTION PLAN: SOME HIGHLIGHTS

The full report of the achievements and next steps of the CIIP action plan is available in annex. The following are a few highlights of the state of play.

4.1. Preparedness and prevention

- The **European Forum of Member States** (EFMS) has made significant progress in fostering discussion and exchanges between relevant authorities on good policy practices

---

14 See the Q&A at http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/11/34&format=HTML&aged=0&language=EN&guiLanguage=fr.

15 E.g. the recent attacks against the French Government

16 See OECD/IFP project on "Future Global Shocks", "Reducing systemic cyber-security risks", 14 January 2011, at http://www.oecd.org/dataoecd/3/42/46894657.pdf.

17 See http://www.enisa.europa.eu/media/press-releases/stuxnet-analysis

18 See World Economic Forum, Global Risks 2011.

related to security and resilience of ICT infrastructures. EFMS is acknowledged by Member States to be an important platform for discussions and exchange of good policy practices.[19] Its future activities will continue to benefit from the support of ENISA and will focus on cooperation among National/Governmental Computer Emergency Response Teams (CERTs), identifying economic and regulatory incentives for security and resilience (whilst respecting the applicable competition and State aid rules), evaluating the state of "cyber-security health" in Europe, driving pan-European exercises, as well as discussing priorities for international outreach on security and resilience.

- The **European Public-Private Partnership for Resilience** (EP3R) was launched as a Europe-wide governance framework for the resilience of ICT infrastructures. It aims at fostering the cooperation between the public and the private sectors on strategic EU security and resilience policy issues. ENISA played a facilitating role for the activities of EP3R and, pursuant to the Commission proposal of 2010 to modernise ENISA, would provide a long-term and sustainable framework for EP3R. EP3R will also serve as a platform for international outreach on public policy, economic and market matters relevant to security and resilience, in particular to strengthen the global risk management of ICT infrastructures.

- The **minimum set of baseline capabilities and services**[20] and related **policy recommendations**[21] for National/Governmental CERTs to function effectively and act as the key component of national capability for preparedness, information sharing, coordination and response have been developed. These results will be a building block to establish, with the support of ENISA, a network of well-functioning National/Governmental CERTs in all Member States by 2012. Such a network will be the backbone of the European Information Sharing and Alert System (EISAS) for citizens and SMEs, to be built with national resources and capabilities by 2013.

4.2. Detection and response

- ENISA devised a high-level roadmap for the development of a European Information Sharing and Alert System (**EISAS**) by 2013,[22] building upon the implementation of *basic services* at the level of National/Governmental CERTs and of *interoperability services* for national information and sharing alert systems to be integrated in EISAS. Appropriate protection of personal data will be one of the key elements of this activity.

4.3. Mitigation and recovery

- So far only 12 Member States that have organised exercises for large-scale network security incident response and disaster recovery[23]. ENISA has developed **a good practice**

---

19 The UK Government's reply to the fifth report from the House of Lords European Union Committee on the CIIP Action Plan states that the EFMS "*has been a success and has tapped into a real needed for policy makers to have an opportunity to exchange experience*".

20 See http://www.enisa.europa.eu/act/cert/support/files/baseline-capabilities-for-national-governmental-certs.

21 See http://www.enisa.europa.eu/act/cert/support/files/baseline-capabilities-of-national-governmental-certs-policy-recommendations.

22 http://www.enisa.europa.eu/act/cert/other-work/eisas_folder/eisas_roadmap.

23 Source: ENISA.

guide on national exercises[24] as well as **policy recommendations** on the development of national strategies[25] to support Member States' activities, which should be intensified.

- The first **pan-European exercise on large-scale network security incidents** (Cyber Europe 2010) took place on 4 November 2010 with the involvement of all Member States, of which 19 actively took part in the exercise, plus Switzerland, Norway and Iceland. Future pan-European cyber exercises would undoubtedly benefit from a common framework that builds upon and interlinks national contingency plans, thus providing baseline mechanisms and procedures for communications and cooperation between Member States.

4.4. International cooperation

- **European principles and guidelines for the resilience and stability of the Internet**[26] were discussed and developed in the context of EFMS. The Commission will discuss and promote these principles with relevant stakeholders, in particular the private sector (via EP3R), bilaterally with key international partners, in particular the US, as well as multilaterally. It will do so, within its competences, in fora such as G8, OECD, NATO (notably on the basis of its new Strategic concept adopted in November 2010 and the activities of the Cooperative Cyber-defense Center of Excellence), the ITU (in the context of capacity-building in the area of cyber-security), OSCE (via its Forum for Security Co-operation); ASEAN, Meridian[27], etc. The objective is to make these principles and guidelines a shared framework for international collective engagement on the long-term resilience and stability of the Internet.

4.5. Criteria for European Critical Infrastructures in the ICT sector

- The technical discussion in EFMS led to **a first draft of the ICT sector-specific criteria** for identifying European Critical Infrastructures, with a focus on **fixed and mobile communications and the Internet**. The technical discussion will continue and benefit from the consultations on the draft criteria, at national and European (via EP3R) level, with the private sector. The Commission will also discuss with Member States the ICT sector-specific elements to be considered for the review of the Directive on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection[28] in 2012.

5. THE WAY FORWARD

The implementation of the CIIP action plan is marked by positive achievements, in particular with regard to the recognition that a cooperative approach to network and information security, involving all stakeholders, is needed. It is also broadly in line with the milestones

---

24 See http://www.enisa.europa.eu/act/res/policies/good-practices-1/exercises/national-exercise-good-practice-guide/at_download/fullReport.

25 See http://www.enisa.europa.eu/act/cert/support/files/baseline-capabilities-of-national-governmental-certs-policy-recommendations.

26 See http://ec.europa.eu/information_society/policy/nis/index_en.htm

27 The Meridian process aims to provide Governments worldwide with a means by which they can discuss how to work together at the policy level on critical information infrastructure protection (CIIP). See http://meridianprocess.org/

28 Council Directive 2008/114/EC

and the timeline set out in 2009. However, we should not be complacent as there is still a lot to be done both at National and at European level to make those efforts successful.

It is also particularly important to embed them in a global coordination strategy and therefore to extend such efforts to the international stage, with all relevant stakeholders, to outreach to other regions, countries or organisations which are addressing similar issues and develop partnerships in order to share approaches and related activities, and avoid duplication of efforts.

We need to promote a global culture of risk management. The focus should be on promoting coordinated actions to prevent, detect, mitigate and react to all kinds of disruptions, whether man-made or natural, as well as to prosecute related cyber-crimes. This includes conducting targeted actions against security threats and computer-based crime.

To this end, **the Commission will**:

- **promote principles for the resilience and stability of the Internet** - International principles for the resilience and stability of the Internet should be developed with other countries, with international organisations and, where appropriate, with global private-sector organisations – by using existing *fora* and processes, such as those related to Internet Governance. These principles should serve as a tool for all stakeholders to frame their activities, relating to the stability and resilience of the Internet. To this end, European principles and guidelines could serve as a basis.

- **build strategic international partnerships** - Strategic partnerships should be built on ongoing efforts in critical areas, like cyber-incident management, including exercises and cooperation among CERTs. The engagement of the private sector, which operates on a global scale, is of paramount importance. The EU-U.S. Working Group on Cyber-security and Cyber-crime, established during the EU-U.S. Summit of November 2010, is an important step in this direction. The Working Group will focus on cyber incident management, public-private partnerships, awareness raising and cyber-crime. It may also consider options for outreach to other regions or countries, notably addressing similar issues to share approaches and related activities and avoid duplication of effort, as appropriate. Further outreach and coordination should be pursued in international fora, notably in the G8. On the European side, key factors for success would be good coordination between all EU institutions, relevant agencies (in particular ENISA and Europol) and Member States.

- **develop trust in the cloud** - It is essential to strengthen discussions on the best governance strategies for emerging technologies with a global impact, such as cloud computing. These discussions should certainly include, but not be limited to, the appropriate governance framework for the protection of personal data. Trust is essential in order to reap its full benefits.[29]

---

[29] See for example ENISA's reports "Cloud Computing Information Assurance Framework" (2009), at http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-information-assurance-framework/at_download/fullReport) and "Security and resilience in governmental clouds" (2011), at http://www.enisa.europa.eu/act/rm/emerging-and-future-risk/deliverables/security-and-resilience-in-governmental-clouds/).

Since security is a shared responsibility of everyone, all Member States have to ensure that their national measures and efforts will collectively contribute towards a coordinated European approach to prevent, detect, mitigate and react to all kinds of cyber disruptions and attacks. In this respect, **the Member States should commit to**:

- **enhance EU preparedness by establishing a network of well functioning National/Governmental CERTs by 2012.** Similarly, the EU Institutions will also establish a CERT at their level by 2012. All these efforts should take advantage of the related minimum set of baseline capabilities and services and related policy recommendations drafted by ENISA, which will continue providing its support to these initiatives. This activity will also advance the development of a European Information Sharing and Alert System (EISAS) to the wider public by 2013.

- **a European cyber-incident contingency plan by 2012 and regular pan-European cyber exercises.** Cyber exercises are an important element of a coherent strategy for cyber incident contingency planning and recovery both at the national and European level. Future pan-European cyber exercises should be based on a European cyber incident contingency plan that builds upon and interlinks with national contingency plans. Such a plan should provide the baseline mechanisms and procedure for communications between Member States and, last but not least, support the scoping and organisation of future pan-European exercises. ENISA will work with Member States on the development of such a European cyber incident contingency plan by 2012. In the same timeframe, all Member States should develop regular national contingency plans and response and recovery exercises.

- **European coordinated efforts in international fora and discussions on enhancing security and resilience of Internet.** Member States should cooperate together and with the Commission on promoting the development of a principles- or norms-based approach to the issue of the global stability and resilience of the Internet. The aim should be to promote prevention and preparedness at all levels and by all stakeholders, thus balancing a current tendency of the discussions to focus on the military and/or national security angles.

6. CONCLUSION

Experience shows that purely national or regional approaches to tackle the security and resilience challenges are not enough. European cooperation has developed significantly since 2009 with encouraging achievements, in particular the Cyber Europe 2010 exercise. However, Europe should continue its efforts to build a coherent and cooperative approach across the EU. A modernised ENISA should step up its support to Member States, the EU institutions and the private sector in this long-term endeavour.

European efforts, in order to be successful, have to be embedded in a coordinated approach at global level. To this end, the Commission will promote discussions on cyber-security in all appropriate international fora.

A CIIP Ministerial Conference, organised by the Hungarian Presidency of the EU, will take place on 14-15 April 2011. This will be a key opportunity to reinforce the commitment towards strengthened cooperation and coordination among Member States, at both the European and international level.

ANNEX

The CIIP action plan: Detailed overview of achievements and next steps

The results of the activities conducted in the context of the CIIP action plan are broadly in line with the milestones and the timeline set by the Commission in 2009. In the following, "achievements" and "next steps" for all pillars are described. This snapshot takes into account that some activities were further elaborated in the Digital Agenda for Europe (DAE) and the Internal Security Strategy in action (ISS).

1. Preparedness and prevention

Baseline of capabilities and services for pan-European cooperation

Achievements

- In 2009, ENISA, together with the Computer Emergency Response Team (CERT) community in Europe, developed and agreed on a minimum set of baseline capabilities and services that National/Governmental CERTs need to have in order to function effectively in support of pan-European cooperation. A consensus was achieved on a list of 'must have' requirements in the areas of operation, technical capabilities, mandate and cooperation.[30]

- In 2010, ENISA worked with the CERT community in Europe to turn the above operationally-oriented requirements into a set of policy recommendations[31] for National/Governmental CERTs to act as the key component of national capability for preparedness, information sharing, coordination and response.

- To date, 20 Member States[32] have developed National/Governmental CERTs and almost all others have plans to set one up. As announced in the DAE and further specified in the ISS, the Commission has proposed measures to establish a CERT for the EU Institutions by 2012.

Next steps

- ENISA will continue to support those Member States which have not yet established National/Governmental CERTs that satisfy the agreed baseline requirements mentioned above, in order to ensure that the target of having well-functioning National/Governmental CERTs in all Member States by the end of 2011 is achieved. This milestone will pave the way for the establishment of a well-functioning network of CERTs at national level **by 2012**, as envisaged in the DAE.

- ENISA, with the cooperation of the National/Governmental CERTs, will discuss whether and how to extend the "baseline capabilities" in order to adapt the CERTs' ability to support Member States in ensuring the resilience and stability of vital ICT infrastructures, and to become the backbone of the European Information Sharing and Alert System

30 See http://www.enisa.europa.eu/act/cert/support/files/baseline-capabilities-for-national-governmental-certs.

31 See http://www.enisa.europa.eu/act/cert/support/files/baseline-capabilities-of-national-governmental-certs-policy-recommendations.

32 Source ENISA

(EISAS) for citizens and SMEs, to be built with national resources and capabilities **by 2013,** as announced in the ISS.

European Public-Private Partnership for Resilience (EP3R)

Achievements

- In 2009, EP3R was launched as a Europe-wide governance framework for the resilience of ICT infrastructures, fostering the cooperation between the public and the private sector on security and resilience objectives, baseline requirements, good policy practices and measures. As stated in the ISS, EP3R will also "*engage with international partners to strengthen the global risk management of IT networks.*" ENISA has facilitated the activities of EP3R.

- Private and public stakeholders were consulted to devise the objectives, principles and structure of EP3R and identify incentives to encourage relevant stakeholders to become actively involved.[33] Priority areas for EP3R were identified in the proposal to modernise ENISA.[34]

- In parallel to devising the structure of EP3R, three working groups were launched at the end of 2010 on (a) key assets, resources and functions for the continuous and secure provision of electronic communications across countries; (b) baseline requirements for the security and resilience of electronic communications; (c) coordination and cooperation needs and mechanisms to prepare for and respond to large-scale disruptions affecting electronic communications.

- In 2010, the Commission proposal to modernise ENISA provided a long-term and sustainable framework for EP3R: it proposed that ENISA should "*support cooperation between public and private stakeholders on the Union level, inter alia, by promoting information sharing and awareness raising, and facilitating their efforts to develop and take up standards for risk management and for the security of electronic products, networks and services*".

Next steps

- In 2011, EP3R will continue strengthening cooperation between public- and private-sector stakeholders to improve security and resilience via innovative measures and instruments, and to identify stakeholders' responsibilities. Leveraging the facilitating role and support of ENISA, the EP3R Working Groups will deliver their initial results. Future activity will also address cyber security challenges of smart grids, buidling on the preparatory work being carried out by the Commission and ENISA.

- EP3R will serve as a platform for global outreach on public policy, economic and market matters relevant to security and resilience. The Commission intends to leverage EP3R in support of the activities of the EU-U.S. Working Group on Cyber-security and Cyber-crime with a view to providing a coherent environment for cooperation between the public and private sector, whilst respecting the applicable competition and State aid rules.

---

33 See http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/impl_activities/index_en.htm

34 COM(2010) 521

- In the long term and in line with the proposal for a new ENISA Regulation, it is envisaged that EP3R should become a key activity of a modernised ENISA.

European Forum for Member States (EFMS)

Achievements

- In 2009, EFMS was established to foster discussions and exchanges between relevant public authorities regarding good policy practices, with the aim of sharing policy objectives and priorities on security and resilience of ICT infrastructures, directly benefiting from the work and support provided by ENISA. EFMS, which meets on a quarterly basis, has been supported since mid-2010 by a dedicated web portal managed by ENISA.

- EFMS has made significant progress as regards: (a) the definition of criteria to identify European ICT infrastructures in the context of the Directive on the Identification and Designation of European Critical Infrastructures;[35] (b) the identification of European priorities, principles and guidelines for Internet resilience and stability; (c) the exchange of good policy practices, in particular on cyber exercises.

- EFMS is acknowledged by Member States to be an important platform for discussions and exchange of good policy practices.[36]

Next steps

- In 2011, EFMS will finalise the technical discussion on ICT criteria for European Critical Infrastructures as well as provide the long-term orientations and priorities for pan-European large-scale exercises on network and information security.

- EFMS will be further involved in discussions on priorities for international outreach on security and resilience, notably in relation to the activities of the EU-U.S. Working Group on Cyber-security and Cyber-crime.

- Priority areas for future EFMS activities, which will draw and benefit from the direct support of ENISA, include[37]: devising methods for effective cooperation between National/Governmental CERTs; leveraging minimum requirements in public procurement to boost cyber-security; identifying economic and regulatory incentives for security and resilience (whilst respecting the applicable competition and State aid rules); evaluating the state of 'cyber-security health' in Europe.

2. Detection and response

European Information Sharing and Alert System (EISAS)

Achievements

35 Council Directive 2008/114/EC.

36 The UK Government's reply to the fifth report from the House of Lords European Union Committee on the CIIP Action Plan states that the EFMS "*has been a success and has tapped into a real needed for policy makers to have an opportunity to exchange experience*".

37 COM(2010) 251

- Two prototype projects (FISHAS and NEISAS) have been funded by the Commission and are currently producing their final results.

- Drawing from its 2007 feasibility report[38] and the analysis of relevant projects at the national and European levels, ENISA devised a high-level roadmap for the development of EISAS by 2013.[39]

Next steps

- In 2011, ENISA will support the Member States in implementing the EISAS roadmap by developing the 'basic services' needed by Member States for establishing their national Information Sharing and Alert System (ISAS) built on their National/Governmental CERT capability.

- In 2012, ENISA will develop the 'interoperability services' enabling each national ISAS to be functionally integrated into EISAS. ENISA will also support Member States in testing such services via the phased integration of national systems.

- In the course of 2011-2012, ENISA will engage National/Governmental CERTs in integrating ISAS capability in their services.

3. Mitigation and recovery

National contingency planning and exercises

Achievements

- At the end of 2010, 12 Member States had developed a national contingency plan and/or organised exercises for large-scale networks security incident response and disaster recovery.[40]

- Drawing from national and international experiences, ENISA developed a good practice guide on national exercises[41]; organised events with Member States and CERTs worldwide on national exercises; and, more recently, issued policy recommendations concerning the development of national strategies where National/Governmental CERTs/CSIRTs are given a key role in leading national contingency planning exercises and testing, involving private- and public-sector stakeholders.[42]

Next steps

- ENISA will continue to support Member States' efforts to develop national contingency plans and organise regular exercises for large-scale network security incident response and disaster recovery, as a step towards pan-European coordination.

---

38 See http://www.enisa.europa.eu/act/cert/other-work/files/EISAS_finalreport.pdf

39 http://www.enisa.europa.eu/act/cert/other-work/eisas_folder/eisas_roadmap

40 See http://www.enisa.europa.eu/act/res/policies/good-practices-1/exercises/national-exercise-good-practice-guide/at_download/fullReport.

41 See http://www.enisa.europa.eu/act/res/policies/good-practices-1/exercises/national-exercise-good-practice-guide/at_download/fullReport.

42 See http://www.enisa.europa.eu/act/cert/support/files/baseline-capabilities-of-national-governmental-certs-policy-recommendations.

Pan-European exercise on large-scale network security incidents

Achievements

- The first pan-European exercise on large-scale network security incidents *(Cyber Europe 2010)* took place on 4 November 2010 with the involvement of all Member States, of which 19 played the exercise, plus Switzerland, Norway and Iceland. The exercise was organised and evaluated[43] by ENISA with the active involvement in the planning team of eight Member States and the technological support of the Joint Research Centre (JRC).

Next steps

- In 2011, Member States will be engaged in discussing the objective and scope of the next pan-European cyber exercise planned for 2012. The option of a phased approach, with more in-depth exercises, involving a smaller group of Member States with the possible participation of international players, will be considered. ENISA will continue to support this process.

- The Commission is financially supporting the EuroCybex project that will conduct a desk-top exercise in the second half of 2011.

- Cyber exercises are an important component of a coherent strategy for cyber incident contingency planning at both national and European level. Therefore, future pan-European cyber exercises should be based on a European cyber incident contingency plan that builds on and interlinks with national contingency plans. Such a plan should provide the baseline mechanisms and procedure for communications between Member States and, last but not least, support the scoping and organisation of future pan-European exercises. ENISA shall work with Member States on the development of such a European cyber incident contingency plan by 2012. In the same timeframe, all Member States shall develop regular national contingency plans and response and recovery exercises. The coordination necessary to achieve this result will be conducted by the EFMS.

Reinforced cooperation between National/Governmental CERTs

Achievements

- Cooperation between National/Governmental CERTs has intensified. ENISA's work on baseline capabilities for National/Governmental CERTs, CERT exercises and national exercises, and cyber incident management has helped to stimulate and support stronger pan-European cooperation between National/Governmental CERTs.

Next steps

- ENISA will continue supporting the cooperation among National/Governmental CERTs. To this end, in 2011, it will produce an analysis of the requirements and provide guidance on a suitable secure communication channel with CERTs, including a roadmap for implementation and future development. ENISA will also analyse the operational gaps at European level and report on how cross-border collaboration between CERTs and relevant stakeholders can be reinforced, in particular for incident response coordination.

[43] See http://www.enisa.europa.eu/.

- The DAE calls on Member States to establish a well-functioning network of CERTs at national level **by 2012**.

4. International cooperation

Internet resilience and stability

Achievements

- European principles and guidelines for the resilience and stability of the Internet[44] were developed based on work conducted in the EFMS.

Next steps

- In 2011, the Commission will: promote and discuss the principles both in bilateral cooperation with international partners, in particular the US, and in multilateral discussions within the G8, OECD, Meridian and ITU; consult with relevant stakeholders, in particular the private sector, at European level (via EP3R) and internationally (via the Internet Governance Forum and other appropriate fora); and promote discussions with key Internet players/organisations.
- In 2012, international partners will be engaged to make the principles and guidelines a shared framework for international collective engagement on long-term Internet resilience and stability.

Global exercises on recovery and mitigation of large-scale Internet incidents

Achievements

- Seven Member States[45] took part in the US cyber exercise Cyber Storm III as international partners. The Commission and ENISA participated as observers.

Next steps

- In 2011, the Commission will develop with the US, under the umbrella of the EU-U.S. Working Group on Cyber-security and Cyber-crime, a common programme and a roadmap towards joint/synchronised trans-continental cyber exercises in 2012/2013. Options for outreach to other regions or countries addressing similar issues to share approaches and related activities will also be considered.

5. Criteria for European Critical Infrastructures in the ICT sector

Sector specific criteria for identifying European Critical Infrastructures for the ICT sector

Achievements

- The technical discussion on sector specific criteria for ICT in the EFMS led to the development of draft criteria for fixed and mobile communications and the Internet.

---

44 See http://ec.europa.eu/information_society/policy/nis/index_en.htm

45 FR, DE, HU, IT, NL, SE and UK.

Next steps

- EFMS will continue the technical discussion on the sector specific criteria for ICT with a view to completing them by the end of 2011. In parallel, consultations with the private sector on the draft criteria for the ICT sector are planned by some Member States and at European level via EP3R.

- The Commission will discuss with Member States the ICT sector-specific elements to be considered for the review of Directive 2008/114/EC on the identification and designation of European critical infrastructures in 2012.

Countries for which you (Veronica Bocarova) are author: DK, SE
Due Date: 15/11/2011
Instruction:

Table 1 - Financial penalties: minimum and maximum amount – November 2011

Last update: November 2011

Contact: martin.schraa@cullen-international.com

Article 10 of the Authorisation Directive as amended by the EU 2009 regulatory framework strengthens NRAs' enforcement powers so as to improve the effective implementation of the framework.

In particular it states that the NRAs should have the power to require the cessation of the breach of the conditions of the general authorisation or the imposed regulatory obligations, either immediately or within a reasonable time limit and shall take appropriate and proportionate measures aimed at ensuring compliance.

In this regard, the NRA shall have the power *"to impose **dissuasive** financial penalties where appropriate, which may include periodic penalties having retroactive effect"*.

The table below shows whether:

- national legislation on electronic communications establishes the minimum and maximum amount of financial penalties that NRA may impose on electronic communications undertakings; and
- if yes, how applicable minimum and maximum amounts are defined: e.g. nominal amounts, percentage of turnover, etc.

The table distinguishes between lump sum penalties and running penalty fines, which continue until an infringement is stopped.

Country	Provisions on financial penalties in national legislation on electronic communications	Minimum and maximum amount – lump sum penalty	Minimum and maximum amount – Running penalty payment	Nov. 2011 OK?
AT	Administrative offences: § 109 TKG 2003 (to be imposed by the regional Telecommunication Offices, which are four public authorities under control of the Ministry) Skimming off of unlawful benefits: § 111 TKG 2003 (the NRA decides that it was an unlawful act and the Cartel Court afterwards decides on the amount)	Administrative offences: €0 to €4,000, €0 to €8,000, €0 to €37,000 or €0 to €58,000, depending on the severity of the offence. Skimming off of unlawful benefits: depending on the amount of the unlawful benefit, maximum 10% of the undertaking's turnover of the preceding year		
BE	BIPT has the power to imposed administrative fines in case of breach of the regulatory framework (Law of Jan. 17, 2003 setting the status of BIPT).	Minimum 0.5 – maximum 5% of the yearly turnover for the market concerned, with max. €12,5m		
DK	Under chapter 33, §79 and chapter 35, §81 of the Law No.169 of March 3, 2011 on electronic communications networks and services, running financial penalties and one-off fines can be imposed for non-compliance with the Law and specific obligations imposed under the Law. The NRA may issue orders but cannot impose fines directly.	No specific amount is defined in the Law on electronic communications. General provisions on financial penalties are set out in the Penal Code. From the preparatory notes to the Law on electronic communications (p. 109-110), it follows that similar principles should	No specific amount is defined in the Law on electronic communications. General provisions on financial penalties are set out in the Penal Code.	OK

	On the NRA request, the financial penalty can be imposed by the ordinary courts conditional upon the Director of Public Prosecutions raising charges.	apply as for sanctions foreseen under the Competition Law, as follows: The fine is calculated on the basis of three factors: • the seriousness, • the length of the infringement • the turnover of the undertaking. There are three stages of seriousness: minor infringements, serious infringements and very serious infringements. There are also three stages of length, i.e. infringements lasting less than one year, between one and five years and more than five years. The fine may be increased or modified on the basis of the two factors depending on the turnover of the undertaking. For minor infringements the amount of fine would be in the range of DKK 10,000-400,000 (€1,300-€54,000). Very serious infringements should normally result in a fine of more than DKK 15m (approx €2m).		
FI	Communications Market Act 393/2003 • §121 – A conditional fine under law 1113/1990 in order to bring an ongoing breach into an end with a threat of fine • §122 – A penalty payment for a breach of an individual SMP or non-SMP obligation (§18 – 20 of the Act)	Conditional fine • Min and max not defined.	Penalty payment • Min. €1,000 • Max. €1m. However, if the breach has especially significant effects on the market, this may be exceeded. In any case the penalty may not exceed 5% of the operator's turnover from electronic communications networks and services in the previous year.	
FR	The Code of Postal services and Electronic Communications (Law part and Decree part) provides for a number of different fines in relation with various breaches of the law.	Yes ARCEP may impose a fine of up to 5% of the turnover of the operator Legal basis Article L5-3		
DE	§ 149 TKG 2004 : The NRA can impose administrative penalties	€0 to €500,000, €0 to €300,000, €0 to €100,000, €0 to €50,000 or €0 to €10,000, depending on the severity of the offence. The penalty shall be higher than the unlawful benefit gained from the offence. If the above mentioned ranges are not sufficient, the NRA may impose higher penalties.		
GR				
IE	Section 46A(6) of Communications Regulation Act 2002, as amended by Communications Regulation (Amendment) Act	Maximum of €5m or 10% of turnover, whichever is the higher amount	n/a	OK

	2007.			
IT	Art. 98 of the Communications Code	• Breach of SMP obligation: min 2% and max. 5% of annual turnover from the market where the breach took place • Other breaches Many categories to which different fines apply (typically not above €250,000	•	•
LU				
NL	[redacted], art. 15§2	Maximum €450.000 or, if it's more, maximum 10% of the relevant turnover.		
NO	The Electronic Communications Act (in English) • §10-7 Running penalty payment in order to bring an ongoing breach into an end • §12-4 Penalty for a breach of the Act	Penalty • Min and max not defined ("fine or imprisonment up to six months")	Running penalty payment • Min and max. not defined	ok
PT	Law 51/2011, of Sep. 13, 2011 (in PT) amending the Electronic Communications Law. • art. 113 §6 (lump sums) • 116§3/4/5 (running penalties)	Light infringements: between €100 and €100K Serious infringements: between € 250 and €1mn Very serious infringements: between €750 and €5mn. The level of penalties within each category (light, serious and very serious) is based on the nature y of the infringer: an individual, a micro-enterprise, a smail enterprise, a medium enterprise or a big enterprise.	Running penalties must be proportionate and reasonable by taking into account the annual turnover of the infringer in the year which precedes the negative impact on the market caused by the unlawful conduct. • Min: €2000 • Max: €100K The above payments can increase daily but must not exceed a totai of €3mn over a max period of 30 days.	OK
ES	General Telecommunications Law differentiates between 'very serious', 'serious' and 'light' infringements. The penalties vary according to this distinction (Article 56 of Law 32/2003 of Nov. 2003).	Very serious infringements The amount of the penalty should not be below, the gross profit obtained with the infringement nor above the quintuple thereof. If this criteria cannot be applied, or if appiying this criteria would lead to an amount which is lower than the highest amount indicated below, the higher amount should be the maximum limit of the penaity: *For infringements related to non-compliance with CMT decisions* NB 1% of the gross annuai revenues in the last financial year (or in its absence, current year) in the "*affected activity*"; NB 5% of total funds used to commit the infringement; NB 20 million euro. *For other very serious infringements not related to non-compliance with CMT decisions:* NB 2 million euro.	In addition to lump sum penalties, daily penalty payments can be imposed to ensure compliance with CMT decisions or with decisions of the ministry of industry within their respective competences Min. amount: €100/day Max. amount:€10,000/day	OK

		Serious infringements Penalty not below the gross benefit obtained from the infringement and not higher than the double of the gross benefit or, if this criteria cannot be applied, 500,000 €. Light infringements The maximum penalty is of 30,000 €.		
SE	Under Chapter 7, 4§ of the Law on electronic communications (2003:389), if PTS finds a reason to suspect that any undertaking operating under the Law on electronic communications "*does not comply with the Law or the decisions on obligations or conditions or the regulations that have been issued under the Law, or is not operating a radio transmitter in accordance to the attached conditions*", it shall notify the undertaking concerned and give the undertaking an opportunity to state its views within a reasonable time limit. PTS has powers to request *immediate* compliance with the Law and combine its request with a financial penalty. PTS enforcement powers were strengthened in line with the new provisions of Article 10 of the Authorisation Directive, following adoption of the amendments to the Law on electronic communications (2003:389) transposing the EU 2009 framework in May 2011 (see also Chapter 11, Supervision of the government bill (Prop. 2010/11:115), with preparatory notes – p.139) In particular PTS was given powers to require *immediate* cessation of the breach of the law and to propose penalties to ensure compliance. Previously PTS could only propose penalties after providing a reasonable time to ensure compliance (not less than one month). PTS cannot impose the financial penalty directly but has to submit the argumented request on imposing the penalty to the administrative court.	No specific amount is defined in the Law on electronic communications. Financial penalties that are imposed by administrative authorities are regulated by Law on financial penalties (1985:206). Under Article 3 of the Act on financial penalties the amount of the fine is set taking into account the economic situation of the undertaking and conditions that presumably should make it follow the authority's order in connection with the penalty. The amount of the penalty cannot be so low that it would be more beneficial economically for the undertaking not to follow the request to comply. Setting the amount of the penalty such factors as turnover, profit or the number of affected customers could be taken into consideration (see PTS principles for supervision, section 4.3.6)	No specific amount is defined in the Law on electronic communications. Financial penalties that are imposed by administrative authorities are regulated by Law on financial penalties (1985:206). Running penalty payment can be combined with one-off penalty.	OK
CH	Art. 60 of the Law on telecommunications.	Maximum 10 % of the average turnover for the last 3 years.		
UK	Section 97 of Communications Act 2003	Maximum amount of 10% of turnover of the relevant business for the relevant period	n/a	OK