Resposta do ICP-ANACOM à Consulta Pública

"Towards a Strengthened Network and Information Security Policy in Europe"

A. *On the CHALLENGES to network and information security*

- *Electronic networks and services constitute the nervous system of our society and the economy, and recent large scale cross-border cyber attacks, for example in Estonia, have highlighted our dependence on them. In this context, what are the major challenges for network and information security to be considered at the national, EU and international level, in particular with regard to resilience of electronic communication networks and information infrastructures? (optional)*

ICP-ANACOM is a Portuguese Public Body charged, among other things, with the regulation of the electronic communications sector, in that regard the major challenges are necessarily interrelated with the fulfilment of the regulatory objectives for this economic sector taking into account the situation of the market.

The electronic communications market is deeply involved in a quite complex transition process for which a certain number of trends should be highlighted, namely:

- The development of Next Generation Networks, based on the Internet Protocol, and of rising levels of mobile and fixed broadband continuously available to the user;
- The rising dependence of almost all public and private economic activity, including electronic government, and even essential public

services on the continuous good operation of the services that this economic sector provides;

- The need of operators and service providers to have access to large financial resources in order to cope with the required investments, now further complicated by the present global financial crisis;
- The rising dependence on convergent, complex products and equipments, mostly functionally based on software applications, resulting of ever more complex production, integration and distribution channels, reaching the market with undetected implementation flaws and thus creating unknown vulnerabilities;
- The increasing relevance of this sector in what regards the economic development of our societies and the quality of life of their citizens.

It is, therefore, critical that the decisions and actions made at national, European and international levels regarding network and information security are taken at an appropriate level and by public and private stakeholders and that they:

- give origin to the implementation of a sustainable and economic sound network and information security strategy, that allows all stakeholders, including users, to maximize their advantages and their understanding;
- promote innovation and development of the market;
- foster effective and timely cooperation between all stakeholders at all levels, national, European and international;
- do not create barriers to competition;
- promote overall visibility and transparency of the network and information security incidents, and, finally,
- strengthen the defence of the legitimate rights of the citizen and the combat against cybercrime.

The question raises the issue of large scale attacks, in fact, there are many other causes of disruption to electronic communications networks and services that should be taken into account as challenges regarding the strengthen of its resilience, namely: the disruption of cables and other physical media, natural catastrophes, the availability of electric power supply, attacks to the physical infrastructure and also logical attacks, the use of products and appliances with unknown flaws, and traffic overloads.

Taking into account what has been previously presented ICP-ANACOM is of the opinion that the major challenges are related to how economic policy can be developed in order to address the following issues:

- The social and economic public NIS requirements vs The commercial interests of the operators and service providers
  - How to align them?
  - Which common infra-structures should be installed and made operational?
  - What type of funding is necessary?
  - Which cooperation processes between both public and private stakeholders should become operational?
  - What should be done by each stakeholder?
  - How to improve visibility and transparency of NIS incidents?
- The information processing and broadband power at the user hands vs The user lack of NIS knowledge
  - How to improve user awareness about his own responsibility?
  - How to help the user develop network and information security requirements according to his needs?
  - What can be done so that each user negotiates the NIS related aspects of service level agreements according to his needs?
  - How to increase user participation in NIS policy issues?
- The present policy and economic cooperation processing time vs The time constraints of effective incident reaction
  - How should the cooperation effort between stakeholders be developed in order to cope with the time constraints?
  - What can be done to improve early detection?

  - What type of measurements should be done and which information should be shared at each phase of the incident lifecycle?
  - What type of exercises and training should be developed?
  - How can cooperation be improved by using modelling and simulation?
  - What can be done to reduce recovery times?
  - What can be done by each stakeholder to reduce the potential negative impact of incidents?
  - What are the interdependences between electronic communication networks and services? How should they be taken into account during the incident lifecycle?
- The implementation of an effective NIS policy vs The development of the electronic communications market
  - What are the common costs between stakeholders and how should they be shared?
  - How to reduce the information gap between stakeholders?
  - How to improve accountability?
  - How to implement an effective NIS policy with minimum impact on market dynamics?
  - How to foster innovation and competition?
  - How to adapt the policy to technological and market developments?
  - Which technical standards should be adopted?
  - How to improve the protection of user rights?
  - How to improve the NIS understanding of each stakeholder?
  - How to harmonize the different NIS related policy and legal instruments?

B. ***On the PRIORITIES of a possibly modernised network and information security policy***

- *Given the importance of electronic networks and services for society and the economy, <u>what should be the three key priorities for policy to address the evolving challenges to network and information security at the EU and the international level</u>? (optional)*

The three key priorities for Network and Information Security EU and International policy should be:

- Improve understanding and visibility of network information security issues to all stakeholders
- Develop a proactive cooperative resilience approach to the security of electronic communications networks and services
- Improve accountability and responsibility of all stakeholders

- *Member States have a key role and overall responsibility in guaranteeing the security and continuity of critical services for citizens and businesses. In this context, <u>what should be the focus of future EU policy</u> in order to: •enhance cooperation at the EU level between national competent bodies; and •achieve a holistic, all-encompassing approach to network and information security; •reinforce the synergy between measures focusing on prevention and resilience ("first pillar") and measures supporting judicial and law enforcement cooperation ("third pillar")? (optional)*

The guarantee of the security and continuity of critical services for citizens and businesses should in fact be always the result of the adoption at EU level of coherent policies along the first and third pillars, and even more when the market is regulated, as is the case for the electronic communications market.

The focus of the EU strategy should be the coherence and harmonisation of the different policies that address the public policy requirements regarding the security and continuity of critical services, to which the major contribution comes from the private sector, while promoting the competitiveness and the cooperation among all stakeholders.

- *The security and resilience of the Internet is a joint responsibility of all stakeholders, including operators, service providers, hardware and software providers, end-users, public bodies and national governments. This responsibility is shared across geographical boundaries, in particular when responding to large-scale cyber attacks. In this context, what role should the EU play to strengthen the preparedness of the key stakeholders? (optional)*

The security and resilience of the Internet and other ICT networks based on the Internet Protocol, such as NGN's, should be the result of a comprehensive security policy that covers not only software applications and services but also physical infrastructures and their overall management.

A good reference to this was given in the results and recommendations presented in the final report of the ARECI study (Availability and Robustness of Electronic Communications Infrastructures).

Another good source of references is the result of the work of ITU-T, namely through the deliverables of its study group 17, two examples of such are the ITU-T Recommendations X.805: "Security architecture for systems providing end-to-end communications", X.1051: "Information security management guidelines for telecommunications organizations based on ISO/IEC 27002" and X.1121: "Framework of security technologies for mobile end-to-end data communications".

As matter of efficiency and of dealing with the complexity of the subject matter the EU could promote the adoption of a common, standards based, auditable technical approach covering the different aspects of the security of the Internet and other ICT networks, based on IP, such as NGN's.

This would facilitate preparation and cooperation among all stakeholders.

Furthermore the EU could promote the development and implementation of an EU level exercise and training program involving the different stakeholders, public authorities and private companies.

- *Because of the global nature of the Internet, each and every country has a degree of inter-dependence with other countries, not least when responding to large-scale cyber attacks. How can we support trans-national cooperation in the EU to cope with evolving network and information security challenges? (optional)*

The challenges created by the changing nature of the threat has to be dealt with the promotion of research and development, with the promotion of innovation and the recurrent training and joint exercise of the different stakeholders elements.

Furthermore a common set of indicators should be adopted so that progress and preparation can be evaluated and goals might be fixed.

The EU could also promote the study of the interdependences between electronic communication networks and services across borders.

C. On the MEANS needed to address the challenges

- *What instruments are needed at EU level to tackle the challenges and support the policy priorities in the field of network and information security? In particular, what instruments or mechanisms are needed to enhance preparedness to handle large scale cyber disruptions and to ensure high levels of security and resilience of electronic networks and infrastructures? (optional)*

On the question of means the needs are legal coverage, adequate visibility and transparency, accountability, financial support and access to human talent.

Furthermore, there is a need to develop common standards and technical regulations to set a common technical framework and address NIS at EU level.

- *A strong and effective European incident response capability could be a key element of ensuring fast responses to cyber attacks and speedy recovery from disruptions. Building upon initiatives at national level, what EU instruments or actions could be considered to reinforce incident response capability? (optional*)

All the instruments that the EU could adopt in order to improve the availability of the means previously referred would foster the development of a European Incident response capability.

On the matter of the actions, ICP-ANACOM would consider that the promotion of a EU level training and exercise program would also give a positive contribution in this regard.

- *In 2004, the creation of the European Agency for Network and Information Security (ENISA) was an important step in promoting an EU-wide cooperation in the field of network and information security. Given the evolving network and information security challenges, is an Agency still the right instrument to "enhance the capability of the Community, the Member States and, as a consequence, the business community to prevent, address and respond to network and information security problems"? (compulsory)*
  - *If yes, what should be the mandate and the size of such an Agency to successfully meet this objective?*
  - *If no, what are the alternatives that should be considered?*

The creation of ENISA has proven to be, in spite of all the hurdles, a positive contribution to the promotion of Network and Information Security subject matters among the different EU stakeholders.

The Agency main role is to contribute to the development of a Culture of Security in the internal market and in that regard its scope should be enlarged in order to improve connections between policies and R&D and technical standards. Its mandate should also be enlarged so that it is reinforced beyond technical issues and also covers the economic and social dimensions of network and information security.

Furthermore taking into account the current development stage of the review of the EU regulatory framework for electronic communications networks and services, and namely the proposals regarding ENISA involvement in article 13a of the Framework Directive, the review of the ENISA regulation should accordingly create a stronger cooperation of ENISA with the National Regulatory Authorities.

Meanwhile the answers given to the questions above also bring about that other types of cooperation at EU level, are needed, namely operational, for which an agency due to its constituency and legal status does not seem to be the best answer..

Therefore while maintaining ENISA and reviewing its mandate as proposed another type of body should be developed, built on the representation of the different stakeholders that gives place to the implementation of an effective and cooperative NIS policy at EU level.

- *Given the shared responsibility of stakeholders for Internet security and resilience, what are the most appropriate instruments to foster international dialogue and cooperation? In particular, what instruments are required to nurture cross-border public-private partnerships to ensure the good functioning of today's electronic networks and infrastructures? (optional)*

In what regards international cooperation there are already a number of fora where international cooperation can and is taking place, namely, the OECD, the UN, the IGF, the ITU, the ISO, the IETF, the Interpol, the CERT community, the Council of Europe and NATO, etc.

The type of cooperation and the relevant stakeholders determines the best forum to where to cooperate.

The examples given have in common that public authorities are present in almost all of them. That does not give a complete answer to cooperation needs but, nevertheless, answers the question by stating that we do not foresee a need for further EU instrument in this regard.

08.01.2009