January 2009

ETNO Expert Contribution in reply to the Public consultation "Towards a Strengthened Network and Information Security Policy in Europe"

Executive Summary
With this Expert Contribution ETNO wishes to provide the European Commission with input on the future objectives of a strong and coordinated Network and Information Security Policy at the EU level.

Considering the international nature of the Internet, Network and Information security challenges require a strong, coordinated European response without unnecessary regulatory burdens on e-communications service and network providers.

In order to avoid overlaps with ongoing initiatives and benefit from already agreed principles, the EU should foster enhanced cooperation at the international level with other entities.

There is a clear need for more awareness and understanding of Network and Information Security issues, including the need to develop a "culture of security".

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 in the field of 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?*

Security and secure networks and services are of the utmost importance for ETNO companies. In most cases, security is considered as a quality differentiation. Therefore, responsible operators are investing huge amounts of money in providing secure services. ETNO is of the opinion that mandatory security levels should not be imposed on providers of e-communications networks and services.

However, what needs to be considered in a coordinated manner at the national, EU and international level is the harmonisation of current regulation focusing on the new social and economic reality that make up information networks and services.

At the international level, legal coordination and a common approach are needed to fight against those countries that tolerate illegal activities against network and information security. A lot of initiatives from different entities do already exist, therefore better coordination at all levels should be preferred to new structures, which could imply overlaps. As an example, one should mention the 2001 Council of Europe Convention on Cybercrime, the ongoing ITU work on Network and Information Security, the OECD's Guidelines for the security of information systems and networks.
A key objective for all stakeholders is to ensure the availability of information networks and systems for critical infrastructures and services, especially in the event of any catastrophe that may occur.

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, 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?*

    1. *Promoting mechanisms that allow protection of identity on the Internet to be guaranteed*
    2. *EU common policy and security guidelines (baseline security controls)*
    3. *Resources funding (i.e. tax reduction for those companies that reach certain security levels, EU funding)*

- *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, what should be the focus of future EU policy 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")?*

  Improve co-operation:

    - Institutional early warning system at the European level and at the national level that allows the coordinated handling of serious threats such as terrorist attacks, with regard to whether its impact is local as well as global, as well as whether it affects relations with third countries (outside the EU).

  Holistic focus:

- Coordination at the national and European level of all stakeholders (public administrations, providers of e-communications services and networks and citizens) that will:
  - Ensure that MSs have identified the major threats and their evolution with regard to their impact (scope and consequences)
  - Prioritize, finance and issue guidelines
  - Ensure that MSs have identified critical services and infrastructures and promote their strengthening (repetition, continuity) in such a way that secure e-communications are guaranteed within the EU and with third countries
  - Provide training and raise awareness of the proper use of technologies amongst all stakeholders (public and private) and citizens.

Synergy between "first pillar" and "third pillar" measures:

- Standardization of the conditions for processing information geared towards prevention (identification and tracking of risks).
- Better coordination between Law Enforcement Authorities from all Member States, and beyond the EU. Considering the international nature of the Internet, trans-border cooperation of Police Forces is a key element and should be enhanced (in line with the principles of the Council of Europe 2001 Convention).
- The recent ENISA stock taking of national regulatory and policy environments related to the resilience of public e-Communications Networks shows the need for this coordination, as even within the EU Member States are free to deploy a variety of policies, regulations and strategies to facilitate, support and strengthen dependability and resilience of public e-communication networks.

- *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?*

  At the EU level, it could be necessary to introduce and manage security certification programmes for security experts, similar to those existing in the United States. That would certify that those industry experts having followed the programmes can qualify as security experts.

- *Because of the global nature of the Internet, each and every country has a degree of interdependence 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?*

  From an operational point of view, trans-national cooperation within the EU could be supported by identifying the critical communication nodes and components in order to enable the replication and capacity of alternative

routings and by establishing levels that allow effective traffic controls in a coordinated way in the event of wide-scale risks.

From an organisational point of view, the above mentioned certification programmes would provide harmonised training and recognition of security experts within the EU, establishing a European system of security certifications. This could be a role to be fulfilled by ENISA.

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?

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?

At the EU level, it would be convenient to set up an incident response team having the ability to coordinate teams in the various Member States. This team will intervene in case of serious threats such as cross-border terrorist cyber attacks to critical infrastructure.

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"?

- *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 was indeed an important step in the promotion of an EU-wide culture of network and information security. However, due to various reasons, the full potential of the Agency is still to be reached.

Its current role focuses on advisory and knowledge management activities should be maintained. The importance of a coordinated approach within the EU has increased since 2004 and will increase further. An agency can well be the right instrument to address issues in the area of network and information security, under the condition that this agency is empowered appropriately.

The size of staff of the Agency should be derived from activities and projects undertaken.

The agency should develop itself as a knowledge base in the area of network and information security and be the reference at EU level and international level. Main activities of ENISA should be focused to facilitate discussion.

Therefore, ENISA should continue working on awareness and visibility, not only within the information security community but also reaching schools, universities. In order to do so, the appointment of "Mr ENISA" or "Mrs ENISA" (a high profile and well-recognised "ENISA Ambassador") would help in providing the Agency with more visibility and more awareness of the projects undertaken by ENISA.

- *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?*

  Cross-border public-private partnerships are key to promote dialogue amongst all stakeholders involved. An international conference would allow the launch of a comprehensive debate on obligations and responsibilities as well as on supervision mechanisms and monitoring.

* * *