March 2007

ETNO Common Position on the draft "Directive on the identification and designation of European Critical Infrastructure" and the report on "Availability and Robustness of Electronic Communications Infrastructures"

Executive Summary
ETNO Members have a longstanding experience of operating business continuity plans and cooperating with national authorities on critical infrastructure protection. Although the latter is most and foremost a national responsibility, ETNO welcomes the Commission's initiatives that will lead to a common approach at EU level and better protection of ECI. The current position paper highlights the importance of coherent action across all sectors and countries, the need to respect proportionality and complementarities and to create a level playing field among all operators. Special attention is drawn to the protection of customer owned and co-located infrastructure. ETNO supports all ten recommendations proposed in the ARECI study, except number seven on standardisation that should remain an industry-lead activity.

This ETNO Common Position represents the Association's second public views on the issue. This reply expresses our more general opinion on the concept and organisation of Critical Infrastructure Protection in Europe taking into account the recent Alcatel-Lucent study on "Availability and Robustness of Electronic Communications Infrastructures (ARECI)" and the proposed "Directive on the identification and designation of European Critical Infrastructure and the need to improve their protection" COM(2006)0787 final.

Evidently, the destruction or disruption of a critical infrastructure providing key services could entail the loss of lives, the loss of property, a collapse of public confidence and morale in the EU. Any such disruptions or manipulations of critical infrastructure should, to the extent possible, be brief, infrequent, manageable, geographically isolated and minimally detrimental to the welfare of the Member States, their citizens and the European Union.

However, to ensure that resources allocated to robustness and availability of ECI are used in the most efficient way, it first of all is necessary to ensure that the most vulnerable infrastructure sectors are identified particularly those that haven't got the extent of redundancy typically present in the telecommunications sector.

Secondly, the definition of the correct and precise criteria of what may constitute a European CI within a given sector needs to be laid down in the draft Directive. The procedure to have general and sectoral criteria defined by a Committee as defined in Articles 3 and 11(3) may lead to an over-inclusive approach.

Telecommunications infrastructure for publicly offered network services is based on systems and elements optimized to service the general public. It allows scalable network extensions that are based on statistical usage patterns. This is the basis for the creation of network services produced at affordable cost, which may have its limitations under extreme circumstances. For network services in special situations - like a local or regional crisis, high load situations and high stress situations - special measures will be needed to increase availability especially for priority services like emergency, emergency support and emergency relief operations. This is normally part of the national readiness procedures.

In the ARECI draft Final report it is suggested that future network operators may not be recognized as part of the critical infrastructure by Member States or by other industry participants. This makes very little sense as regulation in this field needs to be operator neutral as well as technology neutral. To exclude 'new entrants' or certain technologies will in times of a crisis most definitely weaken the robustness of the new entrants' networks, both for their subscribers and for services they may provide to other network providers. Also, without new entrants realizing their own critical role, they may not appropriately plan, invest and maintain vital emergency preparedness and disaster recovery capabilities and this could impact those operating the critical infrastructure except if new entrants would be deliberately isolated during the emergency period.

In the ARECI draft Final report a need for Best Practices is identified and initial Key Findings are suggested. Most of these Best Practices have already been implemented everywhere or everywhere considered critical by most ETNO Members. This is a clear indication that the Best Practices have a recognised value. It can also be inferred that while there are costs associated with implementing these Best Practices and Measures, a significant part of those costs have already been incurred and were considered functional in an economically justified business model.

However, it is a fact that a growing number of Member States are preparing their own approaches to critical infrastructure protection while waiting for the Commission to put forward a general European CIP programme, so that they can take into account the common EU approach. Delaying the adoption of a common framework would increase the chance that various incompatible approaches to CIP would be developed by the Member States. Weak links have to be eliminated especially where pan-

European effects come into play. The risk of one Member State suffering because another has failed to adequately protect infrastructure on their territory needs to be minimised. We need a competitive, sound playing field with essential security measures. Additional costs for companies operating in more than one Member State resulting from differing security measures need to be minimised. Common rules for essential security measures in the CIP field will be of benefit to businesses assuming the ECI are defined in accordance with the principles of proportionality and complementarities. The EPCIP should not put forward any concrete protection measures. A plan with too ambitious protection measures for current network services could disturb Europe's position and ICT usage growth. The objective should be to establish procedures leading to the identification of protection gaps and in some degree harmonisation. Only if such gaps and differences are identified, measures should be taken to address them.

Consequently, ETNO Members recognize that:

- It is clear that the protection of critical infrastructure is first and foremost a national responsibility. From a coordination point of view, a coherent key issue in preparedness and robustness at EU level is the presence of well established coordination between the national authorities.
- That there is a need to identify and designate critical infrastructures in a coherent fashion (using the same sector-based criteria in the entire EU) and assess whether they require additional protection measures.

Recent and future networks entail more customer-owned and customer-powered access equipment (e.g., wireless handsets, routers, and modems) located outside the controlled central office environment. Consequently some subscribers that are not operationally nor contractually associated to an operator, will have an increased responsibility regarding access equipment and its dependencies. Their liability should be identified since equipment that is owned, maintained and powered by the customer allows less control over its security and availability. This can have an impact on the common infrastructure. Furthermore, there may be additional security aspects that the network operator should consider with highly capable end user devices. Without advanced capabilities of networks to discover end user device profiles, subscriber services may be unavailable. This needs to be understood as a justified need and not as an attempt to impact customer's privacy.

Nowadays, there is a generic practice that network operators and providers of applications and services are co-locating for various reasons, and this trend will continue with the deployment of future networks. This applies especially to newcomers. Physical diversity for both network operators and subscribers can be compromised by co-location sites. Also, future networks will consist of many components from many suppliers, both in the core network and at the customer premise. These components will have vastly different capabilities, levels of maturity and sophistication in terms of quality, reliability, and security. Combining multiple components and network elements will place an increased burden on network operators to ensure quality, reliability, and security in future networks too. Both of these factors, co-location and multiple components have direct implication on costs and consequently need to be considered carefully to fulfil a specific service expectation.

ETNO Members are supporting the concept that resiliency and robustness of future ECI designated networks or ICT systems cannot be measured or improved without appropriated reliability and security metrics. This is an important factor since future networks will be multi-services networks that support a variety of new applications. Each application will have very specific characteristics (e.g. always on, location and presence services, real time, store and forward) that will present different stresses to and load situations on the network. Availability and development security metrics need to receive more attention via collaborative efforts

Furthermore, it is necessary to consider that the reliability and security of local governments / administrations networks directly impact the networks to which they connect, and must be treated as critical infrastructure. Consequently, they should be submitted to the same metrics.

In case ECI are identified within the areas of *Information, Communication Technologies, ICT* (Annex I of the draft Directive) ETNO Members believe that to effectively protect the information infrastructure, connected enterprise networks must take a systemic security management approach, which aims to ensure that an enterprise doesn’t just buy security but genuinely produces its part of it. Systematic security management should be built around a set of core principles whose intent is to ensure an optimal balance of protection while maintaining the ability to share vulnerability and response information and develop innovation among strategic partners. Concerning the telecommunications sector, some standards are already available and recent work on the ISO 27000 series is showing a substantial progress, allowing norms to implement a platform to maintain permanent security measures. This can be done using the ISMS – Information Security Management System - as defined in 27001 and using the code of practice defined in 27002.

Also, and only referring to the telecommunications sector, ETSI and ITU are progressing and harmonising standards namely in the area of Baseline Security for Telecommunications Operators.

So, it is ETNO’s point of view that the required minimum basic guidelines to harmonise telecom operators procedures concerning Critical Infrastructure protection already exist and could be used broadly.

ETNO welcomes that Article 6 of the draft ECI Directive requires all CI owners / operators designated as ECI to appoint a Security Liaison Office (SLO). This SLO would function as the contact point for security issues between the ECI and the relevant CIP authorities in the Member States.

Based on aforementioned comments, it is possible to summarize ETNO’s position on the 10 Recommendations proposed by the ARECI study on Availability and Robustness of Electronic Communications Infrastructures.

1 – Recommendation on Emergency Preparedness - improve the speed of response – ETNO has a positive reaction to this proposal.

2 – Recommendation on Priority Communications on Public Networks - vital calls are not blocked. – ETNO has a positive response and would like to recall that some procedures are already adopted in some EU Members States. Most ETNO Members are ready to follow ITU Recommendations on the issue.

3 – Recommendation on Formal Mutual Aid - Agreements enhance network resilience. – ETNO has a positive reaction to this principle, although practical implementation in a competitive market situation looks limited in the current situation.

4 – Recommendation on Critical Infrastructure Information Sharing - informing each other. - ETNO has a positive reaction to this. Moreover, such practice is already common practice among ETNO Members through formalized groups (e.g. ETNO and other fora). In addition ETNO would like to stress the need, for authorities namely Law Enforcement Agencies to participate in such information sharing. Often national security agencies, police and NTA's actually have some information - but only very seldom paint the full picture of actual threats to industry partners.

5 – Recommendation on Inter-Infrastructure Dependency - critical sectors working together. – ETNO has a positive reaction to this. However it is considered that a National approach must be the starting point.

6 – Recommendation on Supply Chain Integrity and Trusted Operation - clean networks. ETNO has a positive view of this proposal.

7 – Recommendation on Unified European Voice in Standards - more clout for unique European needs. - ETNO Members are not in agreement with this proposal. It is felt that such proposal is contrary to European competition rules. Also some common standards are already adopted and standards development should remain an industry-lead activity.

8 – Recommendation on Interoperability Testing - a level playing field.- ETNO has a very positive view on this proposal. Also new standards on interoperability testing are being developed by ITU.

9 – Recommendation on Vigorous Ownership of Partnering Health - it is my responsibility. – ETNO has a positive view on this proposal, especially if there is support of national bodies with an equal division of efforts over all parties involved to maintain a level playing field.

10 – Recommendation on Discretionary European Expert Best Practices - harnessing expertise. – ETNO has a positive view on this issue. Moreover, such is already practice among ETNO Members.

ETNO Members reaffirm their position to support, maintain and improve co-operation and collaboration with EU programmes to develop a possible common approach to the Critical Infrastructure Protection in telecommunication sector. However, based on a long experience in the telecommunication sector most ETNO Members have already adopted the common practice to prepare business continuity plans. They are working in a sector possessing recognised security/safety obligations, which needs to be taken into account when the designation of ECI takes place and when the proportionality of measures is assessed.