July 2014

Europe's ICT sector

- The need for coordinated and responsive EU policies -

Background

ICT is the backbone of every modern society, and here the EU needs to become the single market of choice for governments and industry, where trusted core NIS technologies and services for industry and citizens are concerned (i.e. Trust in EU products and services). However, over the past 15 years Europe has lost its leading position in ICT technology. All the new global players are situated outside the EU. In addition, "Old" companies still dominate the market. This leaves only a few big players from the EU. This problem needs to be urgently addressed.

Problem

Development and production of (almost) all infrastructure components currently lies outside the borders of the EU. In many cases, these infrastructure components are implemented despite unresolved security issues. The EU does not have a track record in state involvement in strategic and technologically complex economic programs other than the "Airbus-project". There is a need for an innovative business model for EU companies producing cybersecurity products and services. While Member States are guided in respect of industry policy strategies, notably for Automotive and Green Energy initiatives, for the Cyber Security Strategy (JOIN(2013)1) or the NIS directive (COM(2013)48), there is no properly coordinated EU industry policy specifically in place for the IT security sector. Here discussion is needed on trusted IT products versus manipulated products & technologies (backdoors, compromised cryptographic algorithms), where European ICT industry is lagging behind compared to the United States and China. Similarly, the EU should ensure that the cost of implementing NIS legislation and policy does not penalise EU companies in a global market.

In addition, the EU has currently little or no influence on the Internet-governance structure. There is a major competitive disadvantage for EU companies due to tax arbitrage of non EU companies in the EU internal market. EU companies of all sectors are victims of industrial espionage and, finally, EU ICT companies have a low "capital stock", esp. SMEs and so are easy candidates for unfriendly take overs, mergers and acquisitions.

Solutions

An alternative business model for EU cybersecurity industry, equivalent to the Airbus investment model would greatly facilitate EU competitiveness in the field.

In order to ensure that the EU achieves a position of market leader in security, a certain number of technical guidelines and standards should be obligatory and should also be supported by an associated certification-scheme. This approach is already adopted in other sectors: no aircraft, no train, no car can be put on the rail or the road without approval of the national/international regulatory body. Technical Guidelines, Standards, Certification, Audits, also incorporated into business models, should mean that these standards have a global impact and so favour competition in global markets.

EU funded research projects in the area of NIS should be more closely linked to policy goals and the interaction between research communities and industry should be improved. In particular, the EU should introduce mechanisms to help ensure that NIS research projects lead to concrete products and services and that research teams remain available to support the development of these products and services until industry can sensibly take over.

Industrial policy should make maximum use of the advantages that the EU's public procurement market has to offer to stimulate the necessary changes in EU policy and, by getting private sector organisations to create collective requirements for entire sectors, to leverage procurement to move the market in the right direction. In addition, cooperation between EU SMEs that are active in the NIS area should be fostered to allow more effective competition in global tenders. Whilst this is difficult to achieve for the global SME community, the goal is achievable for the more focused community of SMEs in the NIS field.

Greater reliance should be placed on the EU's justified reputation for trustworthiness outside its boundaries, to confer a competitive advantage in cybersecurity matters. At the same time, the EU should seek to achieve a reasonable balance between measures that are derived from strong ethical principles and measures appropriately reflecting current business practices and so which could more effectively stimulate economic growth throughout the EU.