

## **The rise of Cyber threats**

Over the last two decades, the world's landscape changed considerably and became reliant on the availability and exchange of information in all sectors to fuel economic growth and improved competitiveness.

The common enablers of this revolution are the underlying networks allowing information exchange and the vast storage capacity available where terabytes of digital data are now standard even for home computers.

While initially such networks were often limited to a single enterprise, the entire world has since grown to rely on the pervasive use of large information networks, including the Internet and, more recently, the virtualisation of resources through the adoption of concepts such as cloud computing<sup>1</sup>.

The dependency of the economy on such ICT systems is both a main driver for innovation and a major weakness of operations:

- A main driver because the increased outreach has led to exponential growth and the exchange of sensitive data and information is today vital to the protection of political, societal or economic interests of all countries.
- A major weakness because the pervasiveness and connectivity of infrastructures have made it virtually impossible to unambiguously identify the main operators. Therefore, when failures occur, the chain of responsibility is unclear and structured emergency and recovery plans are difficult to define, while in parallel economic or even life-threatening impacts can reach dimensions that are often huge with respect to the initial cause of failure.

In addition to failures, the dependency of the economy on information networks has also given rise to the emergence of criminal activities that intentionally target them. We increasingly see attacks targeting public and private critical infrastructures as well as identity thefts affecting the privacy of citizens and the operations of businesses. Security has moved from a contained environment to one whose limits have moved beyond single corporations and indeed into the entire space, leading to the introduction of the "cyber security" terminology.

The US government has made important investments on intelligence and cyber security. In Europe, the approach and funding is more fragmented (often also national level).

However, not only do ICT security capabilities of national public and private users/operators need to be increased, but also the competitiveness and competence of the European ICT security providers has to be strongly supported.

### **Solutions to tackle cyberthreats**

1- Need for regulations of critical infrastructures to trigger implementation of security policies and investment at the level of the threat

An increased dialogue and cooperation between MS and EU Institutions as well as the private sector (operators and suppliers) could identify common issues across EU countries for cyber security and the protection of ICT networks (not only telecom), defining ways and means for the development of common tools and solutions (including: technical standards / procedures, sharing of best practices etc) to allow a secure exchange of data or reinforced ICT network protection, whenever requested.

This dialogue should also allow the EC to elaborate a common framework to secure Europe's information systems, demanding that security of ICT systems is considered from the initial design of

the system, and possible to be updated throughout all the phases of its life. Such a framework should also foresee a liability model for the deployed solutions and services.

The development of these EU approaches, linking different sectors and stakeholders, on common cyber security issues (ID theft, Denial of Service and System interference, cyber espionage, cyber defence etc.) will bring a stronger support to the fight against terrorism and crime.

The coordination of means and of approaches could be enhanced with the creation of a comprehensive EU Cyber Security Programme to promote specific policies and the management of technical and operational controls necessary for security compliance.

2- Need for industrialised monitoring and reaction tools : There is a need for a sort of "Security Cockpit" (i.e. like an aircraft cockpit) that is providing the support to the operators of a "Security Operation Center" by bringing the right level of information and suggested reactions to the operators.

- Today organizations are lacking IT operators with the right level of experience to face the threats that are emerging. As there is always an operator behind decisions, operators need to be trained : training requires simulators. So simulators could be an efficient enabler towards an increased efficiency of operators.
- Deployment and management of credible identity management systems to ensure that only authorized personnel have the relevant access to IT systems of these infrastructures. We need to "ban anonymity from the networks"

We, EADS and the industry at large, are working on it and we would be more than happy to elaborate on this should we have more time.