GAINS Summary

Kavé Salamatian, LISTIC, Université de Savoie

The term Critical Internet infrastructure refers to all hardware and software systems that constitute essential components in the operation of the Internet. If any of these systems and services were to be interrupted for a significant period of time, the Internet would collapse, with a significant impact on critical services that rely on it, such as governmental, financial and business services.

The aim of the project is to enhance the prevention of and the preparedness to cyber-attacks against the European Critical Internet infrastructure, promoting and supporting the definition of cyber-strategies to reduce risks and to upgrade security.

Recently, the international community witnessed to a proliferation of disputes in order to control and regulate the Internet. The interest of governments to increase network control and surveillance, and the commercial incentive to collect big data, has furthermore raised serious concerns about the protection of privacy, freedom of speech and other security related risks. Nevertheless, until nowadays relationships between the geopolitical context and the Internet infrastructure have not been taken into account when defining the (cyber and non-cyber) strategies of a Member State.
This project builds upon the results achieved within the Extrabire project (JLS/2009/CIPS/AG/C2-065), that identified real and concrete threats against the protocols used by the main players of the Internet, namely the AUTONOMOUS SYSTEMS (ASs). These systems manage the core of the whole Internet, and their commercial policies drive the routing of the information that transit through the network. The interdomain routing protocols that they use (e.g BGP-Border Gateway Protocol) have been proved to be extremely vulnerable to cyber-attacks conducted by governments and other organizations. Thus, there is a deep need to assess the risks of such threats, studying the connections of the increased dependency on the geopolitics of the Internet network.

The project will develop the concept of the "Geo-Politics Aware Internet Cartography" to support the implementation of EU initiative on Critical Infrastructure protection. In particular, the project objective will be pursued by:
- Developing a visualization mechanism able to highlight the routes that the information follows between ASs of different Countries, and merge this information with geopolitical data (rivalry between Countries, strategic alliances, important events such as insurrections, protests, riots etc.). By using such a mechanism it will be possible to provide updated and evolving information about the Internet cartography, together with the geopolitical interconnections and dependences between States. The objective is to provide a geopolitical map of the Critical Internet infrastructure, that may be used to prevent cyber-attacks against the European Internet infrastructure, and plan future expansions and interconnections in order to upgrade security.
- Performing a comprehensive risk analysis of the existing routing mechanisms between ASs, with a particular emphasis on the vulnerabilities of the BGP protocol.
- Developing techniques that will support the definition of cyber-strategies of a Country, predicting as example the most critical problems, the most cunning cyber-threats, and the best actions to protect the Critical Internet infrastructure. The definition of such cyber-strategies may include to enhance the resiliency of the Internet, to assure both the freedom of speech and the privacy of the citizen, and to protect against terrorism and other security related risks.

The study will be conducted at various scales of analysis (local, regional, global), which will involve looking into not only the Member States but also their (physical and cyber) neighbours, rivals and allies. Both the Member States and the acceding and candidate countries will take advantage of the results of this project.