An Overview of R&D Activities in Europe on Critical Information Infrastructure Protection (CIIP)

Sandro Bologna[1], Giovanni Di Costanzo[1], Eric Luiijf[2], and Roberto Setola[3]

[1] ENEA
bologna@casaccia.enea.it
[2] TNO Defence, Security and Safety
eric.luiijf@tno.nl
[3] Università CAMPUS Bio-Medico, Complex Systems & Security Lab
r.setola@unicampus.it

Abstract. In recent years there has been an increasing R&D interest in critical infrastructures and their protection. However, this represents a still very immature field of research with very fuzzy and confused boundaries. This paper reports an initial overview of R&D activities in Europe on this topic to illustrate the state of art and to emphasize the major areas of research but also to identify the most relevant lacks.

1 Introduction

Contemporary societies are increasingly dependent on availability, reliability, correctness, safety and security (dependability) of many technological infrastructures, commonly referred to as Critical Infrastructures (CIs) [2]. For many economical, social, political and technological reasons, we observed a rapid change in their organizational, operational and technical structures in the last years. Until one decade ago, these infrastructures could be considered as autonomous vertically integrated systems. They are now tightly coupled with others and show a large numbers of dependencies and interdependencies [3].

Apart from many positive effects to society, the complexity of our infrastructures has increased introducing new and very dangerous vulnerabilities [4]. Due to the presence of links between the different infrastructures, an accidental failure or malicious event in one of them may easily spread across, amplifying its negative consequences. Such phenomena may affect remote users, both from the geographical and/or the logical point of views [5].

Moreover, the actual world socio-political situation emphasizes new classes of threats for these infrastructure, for instance those related to market liberalisation and international activism and terrorism.

These considerations have focused the attention of governments and international organizations on the need to improve dependability, robustness, resilience and plasticity of these infrastructures [2,6]. These strategies are usually referred

J. Lopez (Ed.): CRITIS 2006, LNCS 4347, pp. 91–102, 2006.

to as Critical Infrastructure Protection (CIP) and as Critical Information Infrastructure Protection (CIIP) when the focus is on the ICT component of a critical infrastructure or the critical ICT-sector itself.

The related strategic approaches identify R&D cornerstone elements to face the problem. The US has recently released a specific CIP R&D programme [8] and also the EU Commission has explicitly included this topic in the Preparatory Action on Security Research (PASR) and in the forthcoming 7th Framework Programme (FP).

The EU Commission co-funded also some activities in the 6th FP. One of the project is CI^{2}RCO (Critical Information Infrastructure Research Co-ordination) [9]. CI^{2}RCO is a coordinated action devoted to: 1) snapshot the national and regional R&D initiatives about CIIP existing in the EU-25 countries plus the Associate Candidate Countries (ACC), 2) to identify possible research gaps or areas no adequately investigated and 3) to promote the creation of an European Research Area (ERA) on CIIP.

This paper reports some intermediate high-level results obtained by the CI^{2}RCO project. Details can be found in [10].

2 R&D Analysis

The first problem that has been considered in the analysis of CIIP related R&D initiatives, was the identification of valuable sources. Indeed, due to the broad scope of CIIP many and heterogeneous organizations are involved.

To this end, in a first step, 1155 possible *Point of Contacts* (POCs) were identified in the different EU-25 countries and ACC. Each of them have been contacted personally. On the base of their availability and competence, 89 POCs were selected as national and sector contacts for the CI^{2}RCO project. These belong to ministries (20%), research (52%), technology providers (3%), associations (3%), agencies (10%) and CI stakeholders (12%). These POCs, as shown in Figure 1, ensure a good coverage of the interested countries, although five nations are not covered. Moreover, while the large part of the POCs provided high quality and detailed information about R&D initiatives in their countries other POCs supplied less complete information (i.e., that related to their own activities).

Each POC was asked to fill in questionnaire(s) in order to collect information about national Critical Information Infrastructure Protection (CIIP) strategies and specifically about national and sector-specific CIIP-related R&D initiatives [11].

The CI^{2}RCO consortium initially collected 87 questionnaires which report information on about 135 projects: 77 national initiatives and 58 projects co-funded by EU-commission (for more information [11]). This set of projects was extended to a total number of 156 projects (88 national projects and 68 co-funded projects) with additional information collected from open documents and Internet researches.