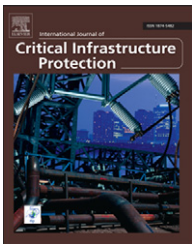
Available online at www.sciencedirect.com

SciVerse ScienceDirect

www.elsevier.com/locate/ijcip



European Reference Network for Critical Infrastructure Protection

Adam M. Lewis, David Ward, Lukasz Cyra, Naouma Kourti*

Security Technology Assessment Unit, Institute for the Protection and the Security of the Citizen, Post Point TP 720, European Commission Joint Research Centre, Via E. Fermi, 2749, I-21027 Ispra (VA), Italy

ARTICLE INFO

Article history:
Received 20 July 2011
Received in revised form
20 February 2013
Accepted 25 February 2013
Available online 28 February 2013

Keywords:
European Union
ERNCIP
Network of laboratories
Experimental security

ABSTRACT

The European Commission has taken the initiative to organize a network consisting of research and technology organizations within the European Union (EU) with capabilities in critical infrastructure protection. Preparatory studies and roadmapping were carried out in 2009–2010 by the European Commission's Joint Research Centre on behalf of the Directorate-General for Home Affairs. The characteristics were planned on the basis of the priorities of the EU member state governments and critical infrastructure stakeholders, and in coherence with EU critical infrastructure protection policy in general. The network of laboratories is called the European Reference Network for Critical Infrastructure Protection (ERNCIP). It is intended to be a long-term, sustainable grouping with a light management structure based on existing European laboratories and facilities. Its main objectives are to agree on common test methodologies and standards, recommend security certification schemes, develop methods for laboratory accreditation, promote the exchange of good and best practices for critical infrastructure protection, and help the development of a single market in the EU for critical infrastructure protection related products and services. A searchable inventory of laboratories and facilities has been compiled and has been publicly released, with an invitation to organizations to upload their descriptions. Thematic groups have been established to focus on priority areas; eight thematic groups are currently operational and two others are in the process of being established.

1. Introduction

The European Union (EU) faces many critical infrastructure protection challenges, some that can only be adequately addressed by the member states acting collectively and some that are significantly different from those faced in other regions of the world. Many of the key questions that must be answered to meet the challenges are of a scientific or engineering character. World-class critical infrastructure protection capabilities are scattered amongst EU member states. What is needed is to coordinate and focus these capabilities on current and future problems.

The European Commission, the EU's executive body, proposed a comprehensive solution: the European Reference Network for Critical Infrastructure Protection (ERNCIP). Its members would be research and technology organizations within the EU with the expertise, experience, facilities and equipment to work on the technical aspects of critical infrastructure protection. ERNCIP would be devoted to experimental security, including testing and evaluation, threat and risk assessment, and the analysis of critical infrastructure dependencies. ERNCIP would be designed to meet the priorities of the European Commission, the governments of the member states and the various critical infrastructure

*Corresponding author. Tel.: +39 0332 785786.
E-mail address: Adam.Lewis@jrc.ec.europa.eu (A.M. Lewis).

1874-5482/$ - see front matter © 2013 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.ijcip.2013.02.004

stakeholders. Also, it would be designed to be coherent with EU critical infrastructure protection policy in general. ERNCIP would help member states to supplement their national technical capabilities by drawing on the capabilities of other EU countries.

Note that the word "network" in ERNCIP is used in the general sense of a group of entities that constitute a widely distributed organization with a common purpose. ERNCIP is not a computer network.

Following extensive consultations with the various stakeholders, the priorities were shifted slightly and the following eleven objectives were identified:

1. Build ERNCIP on existing facilities and capabilities.
2. Develop an environment of trust and sharing.
3. Understand the state-of-the art of experimental critical infrastructure protection.
4. Agree on European good and best practices for critical infrastructure protection.
5. Advance certification efforts.
6. Ensure that the EU is self-sufficient with regard to issues of priority.
7. Improve the body of knowledge in the domain of critical infrastructure protection.
8. Consider the evolution and change of critical infrastructures.
9. Use the EU's inherent diversity to enhance resilience and competition.
10. Promote international standards.
11. Collaborate with countries outside the EU.

In November 2010, the representatives of the EU member states accepted the project roadmap that had been produced by the European Commission's Joint Research Centre. The Commission's Directorate-General for Home Affairs then gave the Joint Research Centre the mandate to proceed with the implementation.

2. Critical infrastructure protection challenges in the European Union

The EU is a highly developed modern society. It has three of the world's ten busiest passenger airports [1], the world's largest financial center [2], more mobile phones than people [3], and broadband Internet in most households [4]. But it is also part of the "Old World"—its economic and political systems and its infrastructure are the result of a long history during which profound changes have occurred. Many infrastructures were built before the EU was created or when it had fewer member states. Most infrastructures were conceived on a national basis or to serve empires and trading blocs that no longer exist.

As Europe developed politically and technologically, infrastructure links were established between countries, such that a critical infrastructure failure in one European country can heavily impact other countries, especially where the infrastructure is a cross-border link or feeds one. A survey of cross-border critical infrastructure failures and disruption events in Europe is beyond the scope of this paper, but some examples are provided for purposes of illustration.

A key incident is the Italian electrical blackout of September 28, 2003 [5]. The blackout was initiated when two power lines in Switzerland flashed over in an Alpine storm, causing the Italian grid to increase demand from, and overload, other lines that brought power from France, causing blackouts across the entire Italian grid and additional failures in Switzerland. Tripping of power system elements was also recorded in Austria, Hungary, Germany, the Czech Republic, Slovakia and Spain [6].

Another example of an international electric grid failure is the power outage of November 4, 2006 [7]. The outage occurred when a power line across the River Ems in Germany was switched off to allow a cruise ship to pass, unintentionally triggering blackouts that spread to France, Italy, Spain and Portugal. Power system elements were also tripped in Austria, Hungary, Croatia, Bosnia, Ukraine, Romania and Morocco [8]. In this case, a weather event was not responsible—the cause was a purely technological failure.

Tunnels are also important infrastructure links. In Europe, a number of important road and rail tunnels cross borders or are the primary routes to borders. Tunnels are vulnerable to fire. Examples include the Mont Blanc and Tauern Tunnel fires of 1999 [9], and the Channel Tunnel fires of 1996, 2006 and 2008 [10–12].

Such events may require a European response when several countries are affected and if a technical solution requires action in countries beyond those where the events occurred. Also, there are important lessons to be learned by the countries involved as well as by other countries with similar infrastructures. For example, the expert panel that investigated the Alpine tunnel fires included participants from fifteen countries and international non-governmental organizations in the sector. The panel that investigated the 2003 Italian blackout incorporated experts from nine countries. Experts from no fewer than 22 countries participated in the investigation of the 2006 European blackout.

However, governments are wary of proposals that could compromise their independent control of their national critical infrastructures or that might entail high costs. Under the Treaty on European Union [13], national security remains the sole responsibility of each member state. There are also other reasons why establishing a single critical infrastructure protection policy for Europe is not simple. For one, member states have different critical infrastructure priorities—some place a higher emphasis on crime and terrorism, others on natural hazards. Attitudes towards the balance between civil rights and security differ significantly. Additionally, non-member states may be involved in an incident, as Switzerland was in the 2003 blackout. Moreover, diverse legal and civil service traditions [14] impede the establishment of common practices, such as the legacy of the old communist state systems as a result of the accession of new states to the EU in 2004 and 2007.

As far as threats to critical infrastructure are concerned, terrorism remains a major worry. However, very few terrorist attacks in Europe have targeted the critical infrastructure and the overall number of attacks is declining. Europol [15] recorded 316 attacks in the EU in 2009, 249 in 2010 and 174