Part I

CIIP Country Surveys

by Dr. Stefano Bruno

Dr. Stefano Bruno is consultant at Ernst Basler + Partners Ltd.

Introduction

Part I of this handbook surveys critical information infrastructure protection (CIIP) efforts in eight countries (Australia, Canada, Germany, the Netherlands, Norway, Sweden, Switzerland, and the United States). For each survey, six subjects of high importance covering conceptual, organizational, and legal aspects of CIIP are considered:

(1) Concept of CIIP and Description of System

The first section discusses the main assumptions and premises underlying the CIIP policy concept. It lists country-specific critical sectors and provides definitions of CII and CIIP.

(2) CIIP Initiatives and Policy

The second section gives an overview of the most important steps taken since the late 1990s at the governmental level to handle CIIP. A first subsection focuses on initiatives, a second highlights the main elements of CIIP policy. This includes descriptions of specific committees, commissions, task forces, and working groups, main findings of key official reports and fundamental studies, and important national programs.

(3) Law and Legislative Action

The third section lists important pieces of legislation enacted for the promotion of CIIP. This includes acts defining the responsibilities of the government authorities in case of emergencies as well as legislation dealing with issues such as technical IT security, data protection, damage to data, fraudulent use of a computer, the handling of electronic signatures, etc. Several countries have begun reviewing their legislation since 11 September 2001. These developments are considered as far as possible.

(4) Organizational Analysis

The fourth section gives an overview of important public actors in the national CIIP organizational framework. It only characterizes the specific responsibilities or public actors at the state (federal) level (such as ministries, national offices, agencies, coordination groups, etc.). Public actors at the lower state level and private actors (companies, industry, etc.) are omitted. Due to the growing importance of public-private partnerships, the most important of these are presented.

(5) Early Warning

The fifth section describes national organizations responsible for CIIP early warning, namely CIIP-related information-sharing organizations such as CERTs, ISACs, etc. Furthermore, reference is made to plans for the development of comprehensive early warning alert and incident report structures.

(6) Research and Development

The sixth section provides an overview of important public and private actors involved in CIIP-related research and development (R&D). This includes national research councils, network centers of excellence, universities, industry research laboratories, etc. In addition, depending on the information available, the main R&D fields are summarized for each country.