International CIIP Handbook

An Inventory of Protection Policies in Eight Countries

Critical Information Infrastructure Protection

Edited by
Andreas Wenger, Jan Metzger, Myriam Dunn

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

The CIIP Handbook is also available on the Internet in full text:
www.isn.ethz.ch/crn
All comments on the CIIP Handbook are most welcome.

Eds.: Andreas Wenger, Jan Metzger, Myriam Dunn
Center for Security Studies and Conflict Research at the Swiss Federal Institute of Technology (ETH) Zurich, Switzerland
In cooperation with Ernst Basler + Partners Ltd.

Contact:
Center for Security Studies and Conflict Research
Seilergraben 45–49
ETH Zentrum SEI
CH-8092 Zurich
Switzerland

Phone: +41 (0) 1 632 08 37 / 40 25
Fax: +41 (0) 1 632 19 41
E-mail: crn@sipo.gess.ethz.ch

Layout and Design: Marco Zanoli
Graphics: Robert Ladner

ISBN 3-905641-85-2

International

CIIP Handbook

An Inventory of Protection Policies in Eight Countries

Critical

Information

Infrastructure

Protection

Edited by
Andreas Wenger, Jan Metzger, Myriam Dunn

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Contents

Preface

The nature of risks and vulnerabilities in modern societies is becoming more and more transnational today. An open, non-hierarchical dialog on newly recognized vulnerabilities at the physical, cyber, and psychological levels is needed to create new knowledge and a better understanding of new risks and of their causes, interactions, probabilities, and costs.

It is on the basis of these premises that the "Comprehensive Risk Analysis and Management Network" (CRN, www.isn.ethz.ch/crn) was launched two years ago as a joint Swiss-Swedish initiative. The CRN is an internet and workshop initiative for international dialog on national-level security risks and vulnerabilities. As a complementary service to the International Relations and Security Network (ISN, www.isn.ethz.ch), the CRN is coordinated and developed by the Center for Security Studies and Conflict Research at the Swiss Federal Institute of Technology (ETH) Zurich, Switzerland in cooperation with the current CRN partner institutions:

- The Swedish Emergency Management Agency (SEMA), Sweden,
- The General Directorate for Security Policy, Federal Ministry of Defense, Austria,
- The Directorate for Civil Defense and Emergency Planning (DCDEP), Norway,
- The Federal Office for National Economic Supply (NES), Federal Department of Economic Affairs, Switzerland,
- The Swiss Federal Department of Defense, Civil Protection, and Sports (DDPS), Switzerland.

The International Critical Information Infrastructure Protection (CIIP) Handbook is the product of a joint effort within the CRN partner network. The CIIP Handbook provides an inventory of national protection policies in eight countries: Australia, Canada, Germany, the Netherlands, Norway, Sweden, Switzerland, and the United States. It is an important step towards a comprehensive overview of existing efforts in critical information infrastructure protection. Work on this first CRN publication started in 2001. Portions of the study were reviewed and validated by international experts before, during, and after the 2nd CRN workshop "Critical Infrastructure Protection in Europe – Lessons Learned and Steps Ahead", which took place in Zurich from 8–10 November 2001. A major part of the coordination as well as the editorial and administrative work was shared

with Ernst Basler + Partners Ltd. (www.ebp.ch), a leading government consulting company in Switzerland.

Because of the dynamics in the field and in order to include additional country surveys and models, a regular update of the CIIP Handbook is planned. We therefore ask the reader to inform us of any inaccuracies or to submit any comments regarding the content. Those countries not yet included are especially encouraged to submit information to us. Please see the front inside cover for contact information. The entire publication plus additional features will also be available on the Internet (http://www.isn.ethz.ch/crn).

The editors would like to thank all the partners involved, in particular the national experts who generously shared their experience and knowledge with us.* We are looking forward to continuing the development and coordination of the CRN partnership.

Zurich, September 2002

Prof. Dr. Andreas Wenger
Deputy Director,
Center for Security Studies
and Conflict Research

Dr. Jan Metzger
CRN Coordinator,
Senior Researcher

Myriam Dunn, lic. phil. I
Researcher CIIP
Center for Security Studies
and Conflict Research

* We also thank the following for their help in the completion of this project: Daniel Bircher, Stefano Bruno, and Robert Ladner (all from Ernst Basler + Partners Ltd.), Christopher Findlay, Barbara Gleich, Liv Minder, Leo Niedermann, Michelle Norgate, Reto Wollenmann, and Marco Zanoli (all from the Center for Security Studies and Conflict Research at the Swiss Federal Institute of Technology, ETH Zurich).

Introduction

Background

Key sectors of modern society, including those vital to the national security and the essential functioning of industrialized economies, are dependent on a spectrum of highly interdependent national and international software-based control systems for their smooth, reliable, and continuous operation. This information infrastructure underpins many elements of the critical infrastructure (CI), and is hence called critical information infrastructure (CII). The CII is facing a continuous change towards new ways of interaction with societies: Most evident is the growing use of open systems to monitor and control operations of the CI as well as the convergence of the media, information technology, and telecommunications technology towards integrated information and communication technologies (ICT).

The increasing value of information and the availability of electronic means to manage its ever-growing volume have not only made information and information systems an invaluable asset, but a lucrative target, too. Whereas the opportunities of ICT are well-known and exploited, the consequences of the inter-linkages among CI through CII are not yet sufficiently understood. Information systems are exposed to failures, are attractive targets for malicious attacks, and susceptible to cascading effects. These new risks and vulnerabilities have become a crucial security issue throughout the world.

Research Subject

A number of issues indicate an urgent need to effectively protect the CII. These include

- inter-linkages among CI,
- consequences of interdependencies,
- possible cascading effects of failures, and
- newly emerging, insufficiently understood vulnerabilities.

Within the last few years, many countries have taken steps to better understand the vulnerabilities of and threats to their CII and have drafted possible solutions for the protection of these critical assets (critical information infrastructure protection, CIIP). These national protection efforts are the subject of this handbook.

A clear and stringent distinction between the two key terms CIP (critical infrastructure protection) and CIIP is desirable, but very hard to obtain. In official publications, both terms are used inconsistently. It often remains unclear whether policy papers are referring to CIP or CIIP, since both concepts are frequently interchanged in an unsystematic manner. Accordingly, the reader will find both terms used in the handbook. This is not due to a lack of accuracy or random use of the two concepts. Rather, the parallel use of terms reflects the stage of political discussion in the surveyed countries. However, there is at least one characteristic for the distinction of the two concepts. While CIP comprises all critical sectors of a nation's infrastructure, CIIP is only a subset of a comprehensive protection effort, as it focuses on critical information infrastructure.

Purpose and Key Questions

The overall purpose of the International CIIP Handbook is to provide an overview of CII protection practices in eight countries: Australia, Canada, Germany, the Netherlands, Norway, Sweden, Switzerland, and the United States.[1] The book is guided by two key questions:

- What national approaches to critical information infrastructure protection already exist?
- What methods and models are used in the surveyed countries to analyze and evaluate various aspects of the critical information infrastructure?

The handbook's target group consists principally of security policy analysts, researchers, and practitioners. It can be used either as a reference work for a quick overview of the state of the art in CIIP policy formulation and CIIP methods and models, or as a starting point for further, in-depth research. However, the handbook does not claim to offer a comprehensive analysis of the topic: It is only an initial sketch of developments in the field of CIIP and does not provide a comprehensive compilation of existing policies, or methods and models.

1 Although the study concentrates exclusively on national efforts, it is recognized that important initiatives have been undertaken by international organizations such as NATO or the EU.

Structure of the Handbook

The handbook focuses on a security policy perspective and a methodological perspective, which are treated in two separate parts:

- *Part I ("CIIP Country Surveys")* looks at policy efforts for the protection of critical information infrastructure in eight countries. Each survey contains six focal points: (1) Concept of CIIP and Description of System, (2) CIIP Initiatives and Policy, (3) Law and Possible Legislative Action, (4) Organizational Analysis, (5) Early Warning, and (6) Research and Development.
- *Part II ("CII Methods and Models")* introduces methods and models to analyze and evaluate various aspects of CII, looking at both specific national efforts and abstract considerations.

The appendix of the handbook contains a glossary of key terms, a bibliography, a collection of links, a list of national experts, and abbreviations. The contents of the handbook are based on open sources of information. These include websites, government documents, workshops, and conference proceedings.[2] For part I, extensive use has been made of the EU-sponsored Dependability Development Support Initiative DDSI (see http://www.ddsi.org). Additionally, expert interviews were conducted between November 2001 and July 2002. Draft versions of the surveys were reviewed by national experts. Without the invaluable support and help of these experts, the handbook would not have been possible.[3]

Outlook

The deadline for information-gathering and expert input was 31 July 2002. More recent information and developments could not be included in this first edition. However, in order to stay abreast of the dynamics in the field, regular updates of the CIIP Handbook are planned. These updates will include continuous work on the existing country surveys, additional country surveys, and more profound methodological analysis. To support this effort, an online version of this handbook with additional features and the possibility to give feedback is in planning.[4]

2 All links last checked by 31 July 2002.

3 The authors tried to include all the opinions of the persons contacted. In the final version, however, the handbook represents solely the authors' views and interpretations.

4 Available at http://www.isn.ethz.ch/crn.