Introduction

Part II of the Handbook describes methods, models, and approaches used to analyze and evaluate aspects of critical information infrastructures (CII) in the surveyed countries. This is of particular relevance for CIP/CIIP, because it is important to understand the crucial aspects of CI/CII under consideration, such as their behavior under normal circumstances and under stress, as well as their role and criticality for government and society. Such an understanding is necessary in order to cost-effectively prioritize means of preparing for, mitigating, and responding to possible threats.

However, infrastructure owners, regulators, decision-makers, and researchers currently face difficulties in understanding the complex behaviors of interdependent critical infrastructures, because infrastructure networks present numerous theoretical and practical challenges. In general, networks are inherently difficult to understand and to manage. There are several reasons: the structural and dynamical complexity of the networks, their large-scale and time-dependent behavior, their dynamic evolution, the diversity of possible connections between nodes, and node diversity.[1]

Additionally, many of the challenges and problems posed by the infrastructures are just emerging. The inherent system characteristics of new information infrastructures, especially, differ radically from those of traditional infrastructures in terms of scale, connectivity, and dependencies. Moreover, there are several "drivers" that will likely aggravate the problem of critical information infrastructures in the future. Among these drivers are the interlinked aspects of market forces, technological evolutions, and newly emerging risks. This situation forces analysts to constantly look ahead and to develop new analytical techniques, methodologies, and mindsets to keep up with the rapid developments in the technological sphere.

Whenever possible, Part II focuses on approaches for critical information infrastructures (CII). However, the majority of the discussed methods and models are designed for the assessment of critical infrastructures (CI). This is due to the fact that the CII is usually just perceived as one special part of the overall CI. The following seven major aspects of CI/CII assessment are discussed in individual subchapters of Part II:

1 Strogatz, Steven H. "Exploring Complex Networks". *Nature*, 410 (8 March 2001): pp. 268–276. http://tam.cornell.edu/SS_exploring_complex_networks.pdf.

1) *Sector analysis*: This subchapter introduces approaches aimed at defining critical sectors and approaches used to specify various characteristics of critical sectors, such as the economic environment, core processes, or interdependencies betweens sectors;
2) *Interdependency analysis*: This subchapter addresses the question of how to categorize interdependencies and gives examples of qualitative interdependency analyses;
3) *Risk analysis*: This subchapter broadly introduces the technique of risk analysis, specifies nine steps that can be included in an IT risk analysis, and provides examples of risk analysis processes designed specifically for CI /CII;
4) *Threat assessment*: This subchapter addresses aspects of threat assessment, namely a management methodology, a general description of the current threat environment, and an IT risk analysis approach;
5) *Vulnerability assessment*: This subchapter introduces various vulnerability assessment approaches with different focal points;
6) *Impact assessment*: This subchapter shows examples of how to evaluate the impact and consequences of an adverse event;
7) *System analysis*: This subchapter presents approaches that employ mathematical models and simulation tools to assess aspects of CI/ CII.

In each chapter, a diverse range of country-specific approaches serve as examples. Some more comprehensive approaches that offer illustrations for more than one chapter (such as the Australian PreDict approach, or the Dutch KWINT Report) appear more than once under different subheadings. To facilitate reading, these approaches are marked by a sign (♦) and a cross-reference (see also Table 1 for overview of examples in the seven chapters). Further, important terms are included in the key terms section (Appendix A1); an entry is marked by an arrow (→).

Country Specific Approaches	1) Sector Analysis	2) Interdependency Analysis	3) Risk Analysis	4) Threat Assessment	5) Vulnerability Assessment	6) Impact Assessment	7) System Analysis
PreDict (Aus)	233–234	246–247			279–280		
NSW (Aus)			257–258	271–272			
NCPG (Can)	229–230						
CIPTF (Can)	235	247–249	259				
OCIPEP (Can)				273–274		289	
M&S* (EU)							295–296
CORAS(EU)			260–261				
EBIOS (Fr)			261–263				
ACIS (Ger)	236–237						
CYTEX (Ger)					280–281		
Quick Scan (NL)	230–231						
Bitbreuk (NL)	237–238						
KWINT (NL)	238–239				281–282		
BAS(No)			263–265				
Roundtables (Swi)	240–241		260				
NISCC (UK)			267–268			289–292	
DoE (US)	242				282–283		
OCTAVE (US)			268–269				
NIST (US)				274–276			
CIAO (US)					284–286		
NISAC (US)							296–297

Table 1: Examples in Chapters 1 to 7 and corresponding pages.

* This category includes four modeling and simulation projects of the European Union: ACIP, COSIN, DepAuDE, and Safeguard.