The International CIIP Handbook 2004: Findings and Prospects

Myriam Dunn and Isabelle Wigert, CIIP Research Group
Center for Security Studies, ETH Zurich, Switzerland

Critical information infrastructure protection (CIIP) has developed into a key part of national security policy during the late 90s, when a new, delicate problem became apparent: the dependency of modern industrialized societies on a wide variety of national and international information infrastructures.


Myriam Dunn

The United States was the first nation to broadly address the perceived new vulnerabilities of vital infrastructures. Following that example, countries all over the world have since taken steps of their own to understand the vulnerabilities of and threats to their *critical information infrastructure* (CII), and have proposed measures for the protection of these assets. *The International CIIP Handbook*, first published in 2002 and substantially expanded for the 2004 edition, compiles and analyzes such *governmental efforts* to protect CII.[1]

The differences in the state and quality of the protection practices in the fourteen studied countries are substantial. Nevertheless, a number of mutual key issues and major future challenges can be identified. Next to more or less well-discussed topics such as the need for better public-private-partnerships, information sharing concepts, or improved early warning schemes, two issues have emerged that have received very little scholarly attention so far and warrant focus in the year ahead. The first is the apparent difficulty to distinguish between CIP and CIIP. The second is the implications of diverse viewpoints of what is "critical" for current and future protection practices. Due to these issues as well as a lack of understanding of complex interdependencies, there is an urgent need for interdisciplinary research as a major future challenge.

CIP and CIIP as Differing but Interrelated Concepts

A focus on CIIP creates immediate difficulties for any researcher since a clear distinction between CIP and CIIP is lacking in most countries. In official publications, both terms are used inconsistently, whereby the term CIP is frequently used even if the document is actually referring to CIIP. In protection practice, CIIP is mostly handled as a subset of CIP in the sense that CIP is more than CIIP but CIIP is an essential part of CIP. 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 the critical *information* infrastructure. It is however important that the two should not be discussed as completely separate concepts: An exclusive focus on cyber-threats that ignores important traditional physical threats is just as dangerous as the neglect of the virtual dimension.

What exactly is to be included in the CI and what in the CII is another question of difficulty: While the CI is always defined in terms of sectors and CIP as measures to secure these critical sectors of society, CII and CIIP are hardly ever defined. One could therefore argue that the distinction between CIP/CIIP is overly artificial. However, the CIP community would highly profit from a clear conceptual distinction due to several factors. First, the protection of the CII has become especially important due to an invaluable and growing role in the economic sector, an interlinking position between various infrastructure sectors, and an essential role for the functioning of other infrastructures at all times. CIIP therefore demands special attention.


Isabelle Wigert

Secondly, the system characteristics of the emerging information

(Continued, Page 13)