## Wrap-Up and Outlook

At present, open, pressing, but unanswered questions abound in the field of CIIP. As a result, there is not just one research gap – there is a research canyon to be filled with knowledge; and the research community is just beginning to single out the correct and the most important questions that need to be asked. Academia and practitioners will have to work hand in hand to resolve these issues, especially with the constant danger of being outpaced by the rapid developments. In such a dynamic field, the need to pinpoint the underlying urgent questions that are not subject to erratic change is a big challenge.

One such question concerns the role that states can and should play in CIIP, when the developments of the past decade have led many observers to assume that the forces driving global change are acutely undermining the state and its political agency. What is clear already is that any conception of security capable of dealing with the current world order needs to be linked to a much wider notion of governance than that which characterized the Cold War. In the realm of CIIP, governments are challenged to operate in unfamiliar ways, sharing influence with experts in the IT community, with businesses, and with nonprofit organizations, because the ownership, operation, and supply of the critical systems are in the hands of a largely private industry.

Furthermore, sharing of power with non-state actors is not the only difficult issue: Like other problems involving security, this one has global origins and implications, and its solution will ultimately require transnational institutions. But most states still focus on CIIP as a primarily *national* security issue, even though the (emerging) information infrastructure transcends many boundaries, and it is even possible that essential information services reside outside the nation-state. Effective (national) protection policies must therefore be backed by efforts in the international arena, such as an international regulatory regime for the protection of cyberspace.

As stated more than once in this Handbook, continuing efforts of CIIP policy evaluation and more research into CIIP matters are necessary. In order to stay abreast of the dynamics in the field, additional updates of the CIIP Handbook are planned. These updated versions will try to keep pace with developments in the various countries and on the international stage. It will be most fascinating to observe how the various policies evolve and "ripen" over the coming years.

Center for Security Studies, ETH Zurich
Volume 2, Zürich 2004.

# The International CIIP Handbook 2004: An Inventory and Analysis of Protection Policies in Fourteen Countries

Myriam Dunn and Isabelle Wigert

edited by
Andreas Wenger and Jan Metzger