CENTER FOR SECURITY STUDIES

Swiss Federal Institute of Technology (ETH Zurich)

Challenges Governments Face in the Field of CIIP: Stakeholders and Perspectives

"Partnerships for Global Cybersecurity"
ITU Headquarters,
Geneva, 15-16 May 2006

Isabelle Abele-Wigert

Outline

- What is Critical Information Infrastructure Protection (CIIP) about?
- Conclusions from the CIIP Handbooks 2006 (now two volumes!)
- Major actors in the field of CIIP…
- …and their different perspectives on CIIP
- Challenges governments face when implementing an effective CIIP policy

Why Focus on Critical **Information** Infrastructure Protection (CIIP)?

- Modern societies rely heavily upon infrastructure, *particularly* ICT
- CII links other critical infrastructure systems together: (Inter-)Dependencies!
- “Drivers of change” that aggravate problem in the future (market forces - technological evolution - emerging risks)
- Internet, preparations for Y2K problem, e-Government, e-Commerce etc. triggered national protection efforts (CIIP and information security)

Conclusions from the **International CIIP Handbook 2006**, Vol. I

Volume I contains:

20 Countries

Australia	Malaysia
Austria	The Netherlands
Canada	New Zealand
Finland	Norway
France	Russia
Germany	Singapore
India	Sweden
Italy	Switzerland
Japan	United Kingdom
Republic of Korea	United States

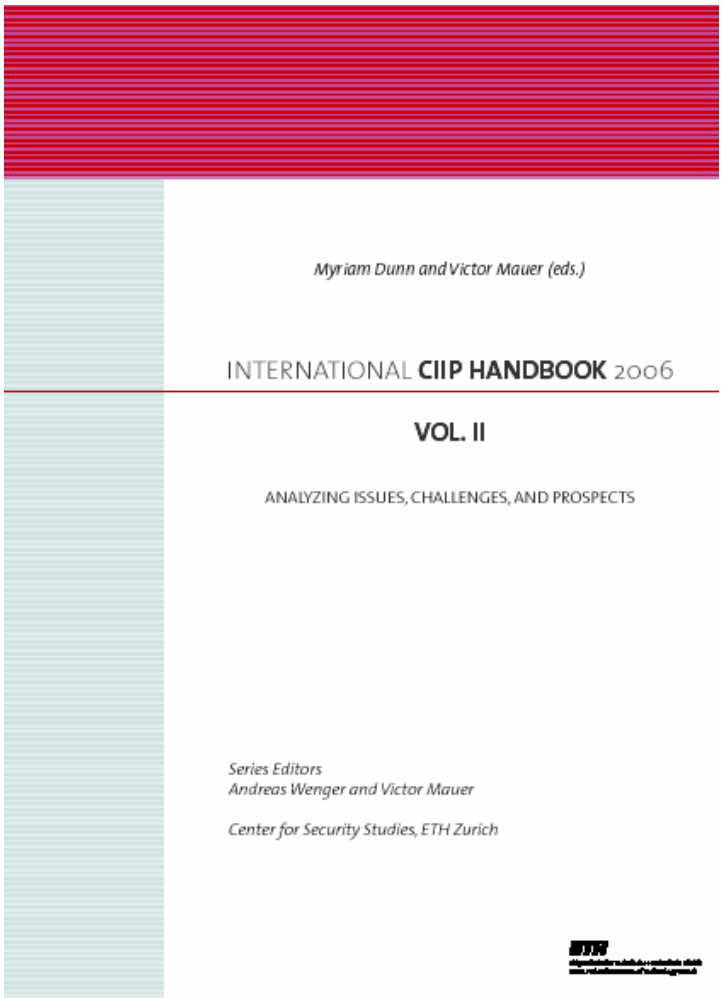
6 International Organizations

EU, G8, NATO, OECD,
UN (ITU), World Bank Group

Vol. I: Country Surveys

- **Volume I** provides an overview of what national approaches to critical information infrastructure protection (CIIP) exist.
- **Country Surveys**:
  - Definition of critical sectors
  - Past and Present CIIP Initiatives and Policies
  - Organizational structures
    - Public Agencies and Public Private Partnerships
  - Early warning approaches
  - Law and Legislation

Conclusions from the **International CIIP Handbook 2006**, Vol. II



Volume II offers in-depth analysis of key issues related to CIIP from various authors, covering:

CIIP Conceptual Issues

(e.g. Understanding critical information infrastructures; **Challenges governments face**)

CIIP Threat Issues

(e.g. Terrorist capabilities for cyber-attack; System complexitiy; Early warning)

CIIP Public Policy Issues

(e.g. Public Private Partnerships; The relevance of International Organizations)

Conclusion and Recommendations

Towards a Global Culture of Cyber-Security

Major Actors involved in CIIP

- **Private sector** (private infrastrucutre operators, companies)
- **Public sector/government agencies**
- **Academic community**
- **Individual users**

→ Differing positions **within** governments / the private sector, and **between** governments and the private sector complicate the assignment of responsibility with it comes to CIP and CIIP.

Four Different perspectives

- System-level, technical perspective
- Business perspective
- Law-enforcement perspective
- National-security perspective

→ The differing positions demand different allocation to **responsibility** and countermeasures

→ **Question:** Is CIIP an issue of ordinary day-to-day politics or a (inter)national security issue?

Example: Switzerland‘s main CIIP actors at government level

Perspec-tives / Actors	IT Security Perspective	Business Perspective	Law-enforcement Perspective	National security Perspective
Fed. Council				X
Fed. Chancellery				X
Task Force				X
Strategy Unit	X	X		X
Melani	X	X	X	X
Cybercrime Unit			X	
Economic Suppl.	(X)	X		X
Inf. Operations	(X)			X
Armasuisse	X			X
Commun. Office	X	X		(X)
PPP	X	X		

Conclusion I

- To address all aspects of CIIP, all perspectives should be taken into account
- Organizations with the same perspective(s) should cooperate and exchange information
- Government actors have national security perspective (unlike private sector)
- PPP: governments could provide (intelligence) information about threats/risks, and the private sector has a lot of practical experience in assuring information to share with governments

Conclusion II: Government roles in the field of CIIP

- Assessing risks and threats
- Enhancing vulnerability detection and response
- Promoting more secure products and services
- Raising awareness and information sharing
- Developing an adequate legal framework
- Emergency preparedness and crisis management

Conclusion III: Challenges for Governments

- How can governments effectively protect critical information assets that are owned and operated by the private sector?
- Should information exchange between government and private infrastructure operators (PPP) be informal or institutionalized?
- What kind of information should be exchanged between different stakeholders?
- What are incentives for the private sector to share sensitive information with governments?
- Which actors should take responsibility and pay in case of an incident?
- ……..

Final Conclusion

- Governments should consider key actor‘s different perspectives for effective CIIP policy
- In some governments, key CIIP organizations were established with important coordination roles
- Governments challenged to share influence and power with non-state actors
- CIIP has global origins and implications, requiring transnational institutions → Effective national protection policies must be backed by efforts in the international arena

Thank you!

Isabelle Abele-Wigert
Comprehensive Risk Analysis and Management Network (CRN)
Center for Security Studies at ETH Zurich
ETH Zentrum
CH-8092 Zürich
Switzerland
wigert@sipo.gess.ethz.ch
www.crn.ethz.ch