the models are too large. Furthermore, such models generally do not capture the characteristics of emergent behavior, a key element of interdependency analysis.

CIIP as Major Future Research Challenge

The differences in the state and quality of the protection practices in the fourteen studied countries are substantial. They are so great that we must even ask ourselves if we are perhaps comparing apples and oranges, especially in the view of the fact that "CIIP" is just one of many labels among many in use for the securing of information, and not even the most suitable term for what it wants to describe. The main problem with the term is the same as with its twin concept, "CIP": It originated in the technical context of limited or "closed systems", and is now used in the totally different context of networks and systems whose boundaries are no longer clearly discernible. When we add socio-political and cognitive dimensions to the equation, it becomes clear that we are dealing with a "new" problem that requires new analytical techniques and methodologies that are not yet available.

Maybe it is necessary to compare apples and oranges in a field that is still emerging. Whether "CIIP" will be the label that sticks remains to be seen. Despite the differences, 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. The first is the apparent difficulty to distinguish between CIP and CIIP, the second deals with the implications of diverse viewpoints of what is "critical" for current and future protection practices. From both these points, and from our lack of understanding of complex interdependencies, arises an urgent future challenge for interdisciplinary research.

The need for more research into methodologies for the analysis of CII and CIIP is acknowledged. However, puzzles persist – such as the functioning of interdependencies; identifying what is critical to whom, when, and why; vulnerabilities and dispersions of disturbances; the influence of threat perceptions; or even the consequences of specific risks to the information infrastructure. Solving them requires an integrated set of methods and tools for analysis, assessment, protective measures, and decision-making. Research on interdependencies and cascading effects in case of failures is especially essential. Moreover, more research into the question of what is critical is

necessary, with a strong focus on the socio-political dimension, including terrorism research, while we must keep in mind that vulnerability-centered analyses that blend out the actor dimension are insufficient. There is a clear need for computer models for all protection phases – such as state-of-the-art-evaluation, the definition of potential improvements, assessment, and to some extent implementation and control.

This points to one fundamental issue and major challenge in terms of research: Only interdisciplinary approaches do sufficient justice to an issue that is *inherently* interdisciplinary due to its multifaceted nature. However, the question of CIIP and related topics has received little attention from large parts of academia up to now. Research is generally focused on aspects of IT-security, on the technical level, and on local or closed subsystems. These aspects are important – but they often miss crucial key features of the complex systems at hand and are inadequate for problem solution.

It is true that the putative new societal risks and vulnerabilities are directly or indirectly related to the development and utilization of new technologies. However, it is likely that critical vulnerabilities, and even the worst consequences of infrastructure disruptions, will not be traceable in any useful way to single technical subsystems – as a consequence of an already overwhelming complexity of open socio-political systems. Also, in view of the rapid technological developments constantly taking place, and the particular nature of their implementations, even if one carefully examines a relatively localized subsystem from the point of view of risks and threats, thereby identifying certain of its vulnerabilities, these insights can hardly be generalized and established in order to utilize them "beyond" the subsystem itself and on a higher system level.

Effective protection for critical infrastructures, therefore, calls for holistic and strategic threat and risk assessment at the physical, virtual, and psychological levels as the basis for a comprehensive protection and survival strategy, and will thus require a comprehensive and truly interdisciplinary R&D agenda encompassing fields ranging from engineering and complexity sciences to policy research, political science, and sociology.