and vulnerabilities or reducing the probability of successful attacks by publishing security alerts.

In some countries, permanent analysis and intelligence centers have been developed in order to make tactical or strategic information available to the decision-makers within the public and private sectors more efficiently. Tasks of early-warning system structures include analysis and monitoring of the situation as well as the assessment of technological developments. Examples can be found in Canada (*Integrated Government of Canada Response Systems*), in Switzerland (*Reporting and Analysis Center for Information Assurance*, MELANI), and in the US (*Directorate for Information Analysis and Infrastructure Protection*, IAIP). Furthermore, there is cross-border cooperation in early warning between Australia and New Zealand. Such international cooperation is sensible when considering the cross-boundary nature of cyberthreats, which are inherently transnational.

Analysis and Conclusion Part II: Analysis of Methods and Models for Critical (Information) Infrastructure Assessment

Part II of the Handbook describes methods, models, and approaches used to analyze and evaluate various aspects of CII in the surveyed countries. Even though the focus of the Handbook is on CII, the majority of the discussed methods and models are designed and used for the larger concept of CI. This reflects the practice of addressing CIP as a comprehensive set of issues, of which CIIP is only a sub-category.

The huge variation in the granularity of methods and models makes a meaningful comparison rather difficult, also because they exist for all of the four hierarchies of CI systems, namely the system of systems, individual infrastructures, individual systems or enterprises, and technical components. A pragmatic approach was chosen in the Handbook by distinguishing between the most important or most-used approaches, which are (1) sector analysis; (2) interdependency analysis; (3) risk analysis; (4) threat assessment; (5) vulnerability assessment; (6) impact assessment; and (7) system analysis. Each is briefly recapitulated below after some general remarks on the state of the art in CII assessment.

General Thoughts

The need for assessment of CII is indisputable, and new vulnerabilities due to society's dependence on CII are acknowledged by all surveyed countries. In order to plan adequate and cost-effective protection measures, the working of these systems and their role for society should be sufficiently understood. But such an understanding is not at all given today, mainly because the complex behaviors of infrastructure networks present numerous theoretical and practical challenges for various stakeholders.

In addition, current methodologies for analyzing CII often prove to be insufficient. A lot of conceptual shortcomings become apparent when it comes to addressing the systems that have become vital to modern society, of which the major manifestation is the failure to understand interdependencies and possible cascading effects. Besides, the available methods are either too sector-specific or too focused on single infrastructures and do not take into account the strategic, security-related, and economic importance of CII.

Each of the methods and models used for the assessment of CII can only be applied to certain limited aspects of the problem, meaning that no single one is sufficient to address the whole range of CIIP issues. This requires a combination of different methodological elements, as shown in the patchwork application and multi-step approaches used in certain countries, such as Australia, Canada, or the Netherlands. Additionally, only few approaches have been developed for the purpose of analyzing CII specifically – most methodological elements originate in risk analysis.

Expert involvement in CII analysis is predominant, where an expert is usually a person closely familiar with the infrastructures in question. This means that crucial knowledge often resides in actors that are outside the state's direct sphere of influence. As a rule, this knowledge is not "academic", but generated directly for problem-solving. The pivotal role of academia in clarifying various crucial CIIP issues is only slowly evolving, and it may still take some time until CIIP issues gain ground in various disciplines.

Finally, CIIP efforts currently face one major problem: Protection is aimed at the present status of existing CII – and thus always lags one step behind. This is problematic as a lot of the challenges and problems are only just emerging, so that the system characteristics of future information infrastructures will differ fundamentally from traditional structures. Understanding them will require new analytical techniques and methodologies that are not yet available. Their development will, in turn, require great efforts in unconventional and forward thinking.

Sector Analysis

Sector analysis is a "grab-bag" label for approaches that aim to identify which aspects of the CI/CII are critical and why. They further the understanding of the working of sectors by highlighting important aspects such as the economic environment, underlying processes, stakeholders, or resources needed for crucial functions.

The choice of the "sector" as a unit of analysis is a pragmatic approach that roughly follows the boundaries of existing business/industry sectors. Many countries have followed the path-breaking and hugely influential example of the *Presidential Commission on Critical Infrastructure Protection* (PCCIP), which was the first official publication to equate critical infrastructures with business sectors or industries. This division also mirrors the fact that the majority of infrastructures is owned and operated by private actors and government officials acknowledge the need for partnerships between infrastructure owners and operators on the one hand and the government on the other.

However, the focus on sectors is far too artificial to represent the realities of complex infrastructure systems. For a more meaningful analysis, it is therefore necessary to evolve beyond the conventional 'sector'-based focus and to look at processes, functions, and services. This is done in the Netherlands, for example. Often, sector analysis is preparatory work for more in-depth analysis such as interdependency analysis and is also used to raise awareness of the CIIP problem among stakeholders.

Interdependency Analysis

Due to the explosive growth of information technology, the study of interdependencies and possible cascading effects in case of failures has become one of the most pressing, but least understood issues in CIIP. Most countries have so far approached the issue from qualitative, expert-based perspectives. These rough analyses of dependencies and interdependencies often aim to primarily determine the criticality of infrastructures or sectors. Often, this is done with the help of interdependency matrices that visualize the strength of interdependencies between sectors with different colors that represent values such as "high", "medium", "low", or "none". In this view, an asset is deemed the more critical the more interdependent it is.

Interdependencies serve as a benchmark for CII methods and models because the major shortcomings of present approaches become particularly apparent in their inability to cope with the problem of interdependencies. This is true for risk analysis methodologies as well as for technical security

models – in fact, for practically all of the approaches currently in use. What becomes abundantly clear is that it will be necessary to move beyond mere estimates of interdependencies, towards sophisticated modeling of cause-and-effect relationships and possible cascading failures.

A satisfactory set of metrics or models that can articulate the risk of failures, either due to natural causes or human-induced, for highly interdependent infrastructures will have to include a range of economic, social, and national-security considerations. This is particularly true because the importance of laws, regulations, policies, and other socio-political concerns to the infrastructure environment make it indispensable to study their impacts on interdependent infrastructures. The ideal way to approach the issue of interdependencies would therefore be a mix between qualitative and quantitative approaches. Additionally, to arrive at a broader understanding of interdependencies, we will require a comprehensive and truly interdisciplinary R&D agenda encompassing fields ranging from engineering and complexity sciences to policy research, political science, psychology, and sociology.

Risk Analysis

The majority of approaches used for CII analysis originate in risk analysis. The latter appears in a variety of forms, and some processes have been adapted specifically for the analysis of CI/CII. This is most likely due to the knowledge and experience that already exists in this field and has been applied by the engineering sciences to system analysis for decades.

Risk analysis could theoretically address any degree of complexity or size of system. When the boundaries of the evaluated system are set too wide, however, a lack of available data will make accurate assessment difficult or even impossible. For IT systems, there may be a very large number of approaches with a focus on information security. However, most of them are business-oriented and centered on organizational information systems, which does not make them applicable to larger systems.

Even though there are different methods of conducting a risk analysis, they often entail a very similar structure under which objects, threats, vulnerabilities, and probabilities are catalogued and links between them are defined. One of the main difficulties is that there are both theoretical and practical difficulties involved in estimating the probabilities and consequences of low-probability high-impact events – since no useful statistics for possible damage and failure probabilities exist. It also appears that there is no way of cataloguing objects, vulnerabilities, and threats on a strategic policy level, such as the economy at large, in a meaningful way. Risk analysis methodol-

ogy further fails to address interdependencies directly, which is a major shortcoming.

Additionally, there is a danger that risk analysis, especially because it is so well established and used in different communities, becomes a "false friend". Methodologies that have proven useful in the past are not necessarily good enough for the future. New sets of problems require new analytical tools. A fixation on quantifiable factors may be severely misleading.

Threat Assessment

Threat assessment can be seen as one part of risk analysis. In the risk analysis sense, threat assessment includes the determination of (1) the nature of external and internal threats, (2) their source, and (3) the probability of their occurrence, which is a measure of the likelihood of the threat being realized. However, when dealing with human actor-based threats such as terrorism, we are dealing with phenomena that are simply non-quantifiable and thus make traditional risk analysis aproaches obsolete.

Qualitative threat assessment has traditionally been very important in security policy. It is perceived by decision-makers today that the threat environment has changed substantially. Since the ability to estimate threats to critical infrastructure has been dependent upon the ability to evaluate the intent of an actor, coupled with the motivation and the capability to carry out the action, new problems arise with the advent of rapidly evolving and little-known cyberthreats, characterized by a number of elements that make them both difficult to predict and detect.

In general, threat assessment in connection with actor-centered research has been largely neglected in the field of CIIP. Many aspects of the threat appear unsubstantiated at a closer look: due to the lack of experience, statements on the scope of the danger often seem purely speculative. This could be resolved with more research into the changes in the threat environment and its impacts on CIIP.

Vulnerability Assessment

Vulnerability assessment can be seen as a specific step in the overall risk analysis methodology. It aims at identifying flaws in the design, implementation, or operation of critical infrastructures that make them susceptible to injury or attack, and attempts to determine the adequacy of security measures in place. Assessing the vulnerabilities of a relatively restricted IT-system such as a business network is far easier than doing the same on a higher system level.

Due to system complexity, it is likely that vulnerabilities and infrastructure disruptions will no longer be traceable in any useful way to single technical subsystems and vice versa.

There is much emphasis on vulnerability assessment in CIIP. However, it is easy to deceive oneself through over-confidence: when looking at relatively limited systems, many factors are known, and data may even be available. This may create a false sense of accuracy. However, very often the threat side of the equation is neglected in the process. This is a treacherous trend, because a vulnerability on its own does not represent a risk when there is no threat. Additionally, there is no certainty that potential malicious actors consider the same points as targets that we have identified as being vulnerable. Wrong assumptions, and hence wrong protection measures, are therefore one possible outcome of a misled vulnerability assessment.

Impact Assessment

There are few approaches to impact assessment. As one specific step within the whole risk analysis process, impact assessment aims to determine the impact resulting from a successful threat exercise of a vulnerability. The problem with current approaches to impact assessment is similar to the problems outlined above: when conducted for limited systems, i.e. IT-systems, consequences can be described in terms of loss or degradation of the IT-security objectives (integrity, availability, and confidentiality). However, when dealing with more abstract systems, measuring impacts becomes a major challenge. Some tangible impacts can be measured quantitatively in lost revenue, the cost of repairing the system, or the level of effort required to correct problems caused by a successful threat action. Other major impacts, such as loss of trust, cannot be measured in specific units, but will have to be described qualitatively.

System Analysis

System analysis employs mathematical models and simulation tools to model various aspects of CII – mostly, their interdependent behavior. Existing efforts are not yet sufficient for modeling cascading failure in complex networks.

Developing a comprehensive architecture or framework for interdependency modeling and simulation is a major challenge. A comprehensive architecture or framework should be able to address all aspects of CIP/CIIP, mitigation, response, and recovery issues. Simply "hooking together" existing infrastructure models generally does not work, as the differences between

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