Understanding Critical Information Infrastructures: An Elusive Quest

By Myriam Dunn

Introduction

Today, it is becoming increasingly important to enhance the security of communication networks and information systems, some of which are more essential than others and are therefore called critical information infrastructures (CII). This urgency is due to their invaluable and growing role in the economic sector, their interlinking position between various infrastructure sectors, and their essential role for the functioning of many of the critical services that are essential to the well-being of developed societies.

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 in reality, such an understanding is still lacking, mainly because the complex behavior of infrastructure networks and their environment presents numerous theoretical and practical challenges for the various stakeholders that are involved: Apart from the interlinking of the computer networks that now underpin most productive activity, the privatization process that gathered strength in the 1990s in many parts of the world has caused a wide range of economic activities that had previously been under state control to be transferred to the private sector, leading to fragmentation and a dire need for coordination. Furthermore, the globalization process, which extends beyond frontiers and creates increasing overlap and dependency, means that critical infrastructure in a given country may be controlled by companies in a neighboring country. Strategic supply chains may also become highly dependent on external markets.[1] The tasks of managing and protecting the infrastructure are thus becoming increasingly difficult, and the "threshold of insecurity" has risen significantly in our developed societies over recent years.

[1] Narich, Richard. "Critical Infrastructure Protection: Importance, Complexity, Results". In: Défense Nationale et Sécurité Collective, No. 11 (November 2005). http://www.defnat.com/naviref/aff_numresume.asp?cid_article=20051133&ctypenecours=0&ccodeoper=1&cidr=200511.

In this chapter, we analyze how states approach the issue of CIIP analytically and what these approaches teach us about the general understanding of the CIIP problem complex. We believe that an assessment of approaches for analyzing various aspects of the CII and a glimpse into the methodological toolbox can serve as an indicator of the current comprehension of key CIIP issues and point us towards key issues in this matter.[2] In addition, by critically assessing these approaches, we point out the major current shortcomings both in practical evaluation and in the general understanding of the issue.[3]

Below, we first address questions that are mainly of a conceptual nature. We believe that a clear and stringent distinction between the two key terms "CIP" and "CIIP" is desirable, but not easily achieved. In official publications, both terms are used inconsistently, with the term CIP frequently used even if the document is only referring to CIIP. This has concrete implications for the evaluation of these systems. The majority of methods and models are designed and used for the larger concept of CI, and not for CII in particular – due partly to conceptual sloppiness, partly to the use of old tools that were developed for completely different applications, and partly to the fact that the CII is often treated as one special part of the overall CI.

Approaches exist for all of the four hierarchies of CI systems, namely the system of systems, individual infrastructures, individual systems or enterprises, and technical components. This means that most of the approaches can only be applied to certain limited aspects of the problem. However, we can group approaches into two broad categories: They either attempt to define critical sectors and assets and seek to understand the working of CI(I) systems in greater or lesser detail – methods that we address in our second chapter –, or to understand the level of risk to these systems, taking into consideration outside influence and the planning of countermeasures, issues that are addressed in the third section.

[2] Dunn, Myriam. "The Socio-Political Dimensions of Critical Information Infrastructure Protection (CIIP)". In: International Journal for Critical Infrastructure Protection, Vol. 1, No. 2/3 (2005), pp. 58–68.

[3] The analysis is based on the detailed description of approaches as described in Part II of the 2002 and 2004 editions of the CIIP Handbook: Dunn, Myriam and Isabelle Wigert (eds.). The International CIIP Handbook 2004: An Inventory and Analysis of Protection Policies in Fourteen Countries (Zurich: Center for Security Studies, 2004); Wenger, Andreas, Jan Metzger, and Myriam Dunn (eds.). The International CIIP Handbook: An Inventory of Protection Policies in Eight Countries (Zurich: Center for Security Studies, 2002).

From Conceptual Sloppiness Towards Conceptual and Analytical Clarity

A self-imposed focus on CIIP creates immediate difficulties for any researcher, since the basis for distinguishing between CIP and CIIP is far from clear. That the two concepts are closely interrelated is apparent from the current debate on protection requirements: The debate keeps jumping from a discussion on defending critical physical infrastructure – telecommunications trunk lines, power grids, and gas pipelines – to talk of protecting data and software residing on computer systems that operate these physical infrastructures.[4] This indicates that the two cannot and should not be discussed as completely separate concepts. Rather, CIIP seems an essential part of CIP: 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. The lesson from this seems to be that an exclusive focus on cyber-threats that ignores important traditional physical threats is just as dangerous as the neglect of the virtual aspect of the problem.

One could therefore be tempted to argue that the distinction between CIP/CIIP is overly artificial or simply an academic fad. However, not only would more reflection on terminology bring about a much-needed sharpening of the conceptual apparatus, there are also a number of persuasive indicators that the main future challenges lie with the emerging CII, so that the CIP community would benefit significantly from a clear conceptual distinction between CI/CII that permits a better understanding of these challenges:

- The protection of the CII has generally become more important due to the invaluable and growing role of the infrastructure elements in the economic sector, their interlinking position between various infrastructure sectors, and their essential role for the functioning of other infrastructures at all times;
- On the threat side, cyber-threats are evolving rapidly both in terms of their nature and of their capability to cause harm, so that protec-

[4] Porteous, Holly. "Some Thoughts on Critical Information Infrastructure Protection". In: Canadian IO Bulletin, Vol. 2, No. 4 (October 1999). http://www.ewa-canada.com/Papers/IOV2N4.htm.

tive measures require continual technological improvements and new approaches, which means giving constant attention to the CII;

- The system characteristics of the emerging information infrastructure differ radically from traditional structures in terms of scale, connectivity, and dependencies.[5] Additionally, the interlinked aspects of market forces and technological evolution will likely aggravate the problem of CII in the future:
- Market forces: security has never been a design driver. Since pressure to reduce time-to-market is intense, a further surge of computer and network vulnerabilities is to be expected.[6] We are therefore faced with the potential emergence of infrastructures with inherent instability, critical points of failure, and extensive interdependencies;
- Technological evolution: On the other hand, we are facing an ongoing dynamic globalization of information services, which in connection with technological innovation (e.g., localized wireless communication) will result in a dramatic increase of connectivity and lead to ill-understood behavior of systems, as well as barely understood vulnerabilities.

This prospect clearly indicates a need to distinguish conceptually between CIP and CIIP, without treating them as completely separate concepts. Moreover, the careless use of terms points to deficiencies in understanding important differences between the two concepts and is a direct consequence of substantial flaws in the existing terminology. This can be illustrated using the components of the term “CIP”, which are either quite carelessly introduced into the political agenda from a technical-scientific or system-theoretical expert level without adaptation to the socio-political context, as is the case for “critical”, or are borrowed, as in the case of “infrastructure”, from man-made technical infrastructures, such as railways, roads, or airports,[7] as a label for far more elusive complex, interdependent, open systems.

[5] Parsons, T.J. “Protecting Critical Information Infrastructures. The Co-ordination and Development of Cross-Sectoral Research in the UK”. Plenary address at the Future of European Crisis Management conference (Uppsala 2001).

[6] Näf, Michael. “Ubiquitous Insecurity? How to ‘Hack’ IT Systems”. In: Wenger, Andreas (ed.). The Internet and the Changing Face of International Relations and Security, Information & Security: An International Journal, Vol. 7 (2001), pp. 104–118.

[7] Moteff, John, Claudia Copeland, and John Fischer. Critical Infrastructures: What Makes an Infrastructure Critical? CRS Report for Congress RL31556 (Updated 29 January 2003).

But even though the need for conceptual precision is obvious, it is still very difficult to understand what exactly the (national or global) information infrastructure is. This is due to the fact that technologies have not only a physical component that is fairly easily grasped – such as high-speed, interactive, narrow-band, and broadband networks; satellite, terrestrial, and wireless communications systems; and the computers, televisions, telephones, radios, and other products that people employ to access the infrastructure – but they also have an equally important immaterial, sometimes very elusive component, namely the information and content that flows through the infrastructure, the knowledge that is created from this, and the services that are provided. As a result, we are caught in the tangled web of inadequate terminology, which will likely have an impact on how we perceive and ultimately approach the issue.

More often than not, the actual objects of protection interests are not static infrastructures, but rather the services, the physical and electronic (information) flows, their role and function for society, and especially the core values that are delivered by the infrastructures. This is a far more abstract level of understanding essential assets, with a substantial impact on how we should aim to protect them. This fact is widely acknowledged, but it remains to be seen in the following two chapters how these observations are reflected in current approaches to analyzing CI/CII systems.

Sectors and Beyond: Analyzing what is Critical

Approaches discussed in this chapter mainly deal with the questions of "what is critical" and "how do we establish what is critical". In designating a list of "sectors" as critical units,[8] many countries have followed the 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.[9] The choice of the sector as a unit of analysis is a pragmatic approach that roughly follows the boundaries of existing business/industry

[8] See Abele-Wigert, Isabelle and Myriam Dunn. International CIIP Handbook 2006, Vol. I.: An Inventory of 20 National and 6 International Critical Information Infrastructure Protection Policies (Zurich: Center for Security Studies, 2006).

[9] President's Commission on Critical Infrastructure Protection (PCCIP). Critical Foundations: Protecting America's Infrastructures (Washington, DC, October 1997). This publication is quoted in the following as PCCIP.

sectors, a division that mirrors the fact that the majority of infrastructures is owned and operated by private actors. In general, though the exact definitions vary from country to country, sectors are deemed critical when their incapacitation or destruction would have a debilitating impact on the national security and on the economic and social well-being of a nation.[10]

There are many aspects that might be analyzed in connection with individual sectors, such as how and why they are critical, or which of their components are particularly vulnerable. In general, sector analysis adds to an understanding of the functioning of single sectors by highlighting various important aspects such as underlying processes, stakeholders, or resources needed for crucial functions. Approaches that examine the vertical structure of sectors (sectors, sub-sectors, processes, functions, etc.) are discussed in our first subchapter.

To determine how critical sectors function, what the influencing parameters are in particular sectors, and how important specific sectors are to the economy, including the identification of core functions, value chains, and dependency on information and communication technology in each critical sector, is a prerequisite for subsequent interdependency analysis. In our second subchapter, we will investigate approaches that focus on the horizontal structure, especially on interdependencies between sectors.

Sectors and Subsectors – the Vertical Dimension

A sector is deemed "critical" if a breakdown or serious disruption of that sector could lead to damage on a national scale, or in other words, if the impact of a disruption would be sufficiently severe. Usually, a component or a whole infrastructure is defined as "critical" due to its strategic position within the whole system of infrastructures, and especially due to interdependencies between the component or the infrastructure and other infrastructures. In a broader view, some infrastructures or components of infrastructures have come to be seen as critical due to their inherent symbolic meaning.[11]

It is broadly acknowledged, however, that the focus on sectors is far too restricted to represent the realities of complex infrastructure systems. For a

[10] See differing definitions in CIIP Handbook 2006, Vol. I.

[11] For more details, see Metzger, Jan. "The Concept of Critical Infrastructure Protection (CIP)". In: A.J.K. Bailes/I. Frommelt (eds.). Business and Security: Public-Private Sector Relationships in a New Security Environment (Oxford, 2004).

more meaningful analysis, it is therefore deemed necessary to evolve beyond the conventional sector-based focus and to look at the services, the physical and electronic (information) flows, their role and function for society, and especially the core values that are delivered by the infrastructures. Therefore, experts groups often focus on four steps in the identification of what is critical: 1) critical sectors, 2) sub-sectors for each sector on the basis of organizational criteria, 3) core functions of the sub-sectors, and 4) resources necessary for the functioning of the sub-sectors.[12] The CII plays important roles in all four areas.

To identify sectors, products, and services comprising the national critical infrastructure requires input from private-sector experts as well as experts and officials at various levels of government. In the view of many countries, an effective way of getting information on various aspects of CI/CII is to circulate a questionnaire among key persons and experts, or to interview them. A questionnaire may contain multiple-choice answers that can be assessed with the help of an evaluation key, or questions can be phrased to leave more latitude for semi-structured answers. The information thus collected will need to be augmented and refined in workshops with representatives of vital public and private sectors.[13]

Since such a process always involves different people from different communities, a common understanding and definition of the term “critical” is crucial. First of all, the classification of what is “critical” lies mainly in the eye of the beholder, and such an assessment is shaped to a large degree by subjective viewpoints and organizational backgrounds. Therefore, unless a minimum agreement can be reached on the precise topic of the discussion and on standardization of the assets to be considered prior to any attempted assessment, owners and operators of potentially critical assets might not all agree on a common language nor a common level of granularity.[14] In addition,

[12] Dunn, Myriam. “Part II: Overview of Methods and Models to Assess Critical Information Infrastructures”. In: Dunn and Wigert, op. cit., p. 227f.

[13] Luiijf, Eric A.M., Helen H. Burger, and Marieke H.A. Klaver. “Critical Infrastructure Protection in The Netherlands: A Quick-scan”. In: Gattiker, Urs E., Pia Pedersen, and Karsten Petersen (eds.). EICAR Conference Best Paper Proceedings 2003. http://www.tno.nl/instit/fel/refs/pub2003/BPP-13-CIP-Luiijf&Burger&Klaver.pdf.

[14] For example, a representative of the electric power generation business might identify generating stations or dams as critical, while others might extend that assessment to the level of turbines or bearings. Cf. Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP). Tool to Assist Owners and Operators to Identify Critical Infrastructure Assets (19 December 2002), p. 2.

most critical sectors have different structures and requirements, so that the appropriate level of detail might vary considerably from sector to sector.[15]

The potential damage impact of loss or disruption of vital products and services is measured with the help of indicators derived from definitions of national security and national interest. Generally, all societies are said to have three fundamental core values: (1) the protection of citizens and territory; (2) the protection of political independence and autonomy; and (3) the protection of national economic safety.[16] National security is often defined as the absence of threats to these core values.[17] In accordance, a product or a service is defined as vital if it provides an essential contribution to one of these core values. For example, it is "vital" if it is necessary for maintaining a defined minimum quality level of (1) national and international law and order, (2) public safety, (3) economic activity, (4) public health, (5) the ecological environment, or (6) if the loss or disruption of the product of service would affect citizens or the government administration at a national scale.[18] Depending on national particularities, these indicators might vary. In general, however, in defining "vital" sectors, all countries take the potential loss of life as well as economic, social, and political consequences into consideration.

From a national-security perspective, it is the government that must determine the level of damage impact that is acceptable to society. In addition, it is necessary to distinguish between products and services that are vital to the nation and those that are merely very important. A relatively high threshold is needed when one attempts to identify something as truly critical: For instance, many important systems are self-repairing or self healing, such as the

[15] Reinermann, Dirk and Joachim Weber. "Analysis of Critical Infrastructures: The ACIS Methodology (Analysis of Critical Infrastructural Sectors)". Paper presented at the Critical Infrastructure Protection (CIP) Workshop (Frankfurt, 29–30 September 2003).

[16] Berkowitz, Bruce D. American Security (Yale: Yale University Press, 1986).

[17] Wolfers, Arnold. "National Security as an Ambiguous Symbol". In: Id. Discord And Collaboration: Essays on International Politics (Baltimore: Johns Hopkins, 1962), pp. 147–165

[18] Examples are: National Contingency Planning Group. Canadian Infrastructures and their Dependencies (March 2000), Preface; Charters, David. "The Future of Canada's Security and Defence Policy: Critical Infrastructure Protection and DND Policy and Strategy". Research paper of the Council for Canadian Security in the 21st Century. http://www.ccs21.org/ccspapers/papers/charters-CSDP.htm. Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. Critical Infrastructure Protection in the Netherlands: Quick Scan on Critical Product and Services (April 2003).

internet, which redirects traffic to avoid damaged infrastructure elements.[19] Thus, despite the fact that breakdowns in banking and payment systems can have nation-wide consequences, or that disruptions in a subway system can affect millions, such disruptions are, essentially, local occurrences. That is, the disruptions are contained within a given, restricted system. In such cases, a certain delimited, more or less well defined function or service is affected, and there are usually more or less acceptable reserve procedures or backup-functions. In short, there are ways to get around such problems, and one can hardly maintain that they constitute a serious threat to society, let alone threaten society's very existence.[20]

This points to the fact that it is very difficult to establish the criticality of an asset without taking into account its extended environment and various other factors such as threats, impact, control mechanisms, etc. In addition, the question of criticality in the socio-political context is always inextricably linked to the question of how damage or disruption of an infrastructure would be perceived and exploited politically. Actual loss (monetary loss or loss of lives) would be compounded by political damage or loss in basic public trust in the mechanisms of government, and erosion of confidence in inherent government stability.21 From this perspective, the criticality of an infrastructure can never be identified preventively based on empirical data alone, but only ex post facto, after a crisis has occurred, and as the result of a normative process.

Interdependencies — the Horizontal Structure

Critical infrastructures are frequently connected at multiple points through a wide variety of mechanisms, so that the conditions for any given pair of infrastructures are mutually reinforcing. This means that CI are highly interdependent, both physically and in their greater reliance on the information infrastructure, resulting in a dramatic increase of the overall complexity and posing significant challenges to the modeling, prediction, simulation, and analysis of CI. The information infrastructure plays a crucial role, as most of

[19] Cukier, Kenneth Neil, Viktor Mayer-Schoenberger, and Lewis Branscomb. "Ensuring (and Insuring?) Critical Information Infrastructure Protection". KSG Working Paper No. RWP05-055 (October 2005). Available at: http://ssrn.com/abstract=832628.

[20] Westrin, Peter. "Critical Information Infrastructure Protection". In: Wenger, Andreas (ed.): The Internet and the Changing Face of International Relations and Security. Information & Security: An International Journal, Vol. 7 (2001), pp. 67–79.

the critical infrastructures are either built upon or monitored and controlled by ICT systems, a trend that has been accelerating in recent years with the explosive growth of information technology.[22]

Due to the explosive growth of information technology, the study of interdependencies and possible cascading effects in case of failures has become the focal point in CIIP discussion. At an initial stage, most countries have opted for qualitative, expert-based approaches to mapping interdependencies. Expert opinions are collected by means of working groups, roundtables, workshops, or questionnaires.[23] The identification of nodes and linkages between sectors helps to establish the degree of interdependency: Interdependencies can exist between components, but also between functions or resources; they can have different characteristics (i.e., physical, virtual, related to geographic location, or logical in nature) and may differ in degree. Other important factors to be considered include the impact of the effect caused by the dependency, time lags, redundancy, etc. The extent of direct dependency between infrastructure elements is described using values such as "high", "medium", "low", and "none".[24] While experts are usually able to evaluate direct dependency relationships, calculating the potential cascading impact of degradation to any level of depth in the maze of dependency relationships is a more difficult matter and requires the help of software.[25]

It is generally recognized, however, that it is necessary to move beyond mere qualitative understanding of interdependencies and towards sophisticated

[21] Ibid.

[22] "Interdependency" can be understood as a "bidirectional relationship between two infrastructures through which the state of each infrastructure influences or is correlated to the state of the other." "Dependency", on the other hand, denotes a unidirectional relationship. Rinaldi, Steven M., James P. Peerenboom, and Terrence K. Kelly. "Complex Networks. Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies". IEEE Control Systems Magazine, Vol. 21 (6 December 2001), p. 14.

[23] Dunn, Myriam. „Part II: Overview of Methods and Models to Assess Critical Information Infrastructures". In: Dunn, Myriam and Isabelle Wigert. International CIIP Handbook 2004: An Inventory and Analysis of Protection Policies in Fourteen Countries (Zurich: Center for Security Studies, 2004), pp. 229–42.

[24] Ibid.

[25] An application known as Relational Analysis For Linked Systems (RAFLS) has been developed in Canada for measuring and modeling the cascading effects of these direct dependencies. RAFLS, which is based on an algorithm, uses scored interdependencies and iteratively determines dependencies and impacts. It shows high and medium degrees of dependencies and can reveal second-, third-, fourth-, and fifth-level dependencies. It also helps to trace linkages and potentially to interdict a path in time of crisis.

modeling of cause-and-effect relationships and possible cascading failures. A comprehensive analysis of interdependencies is a daunting challenge, though, mainly because the science of infrastructure interdependencies is relatively immature. Many models and computer simulations have been developed in the past for specific aspects of isolated infrastructures. However, these efforts are not sufficient for modeling cascading failure in complex networks. Simulation frameworks that allow the coupling of multiple interdependent infrastructures to address infrastructure protection, mitigation, response, and recovery issues are only beginning to emerge.

The problem of interdependencies is complex and difficult to analyze, not least because the nature of interdependencies is still very little understood. Besides technical aspects, the larger environment also needs to be taken into account, especially the interrelated factors and system conditions that complicate the challenge of identifying, understanding, and analyzing interdependencies. According to a much-cited article, at least six aspects can be distinguished:[26]

- Environment: Examples for parameters related to the environment are: Economic and business opportunities and concerns, public policy, government investment decisions, legal and regulatory concerns, and social and political concerns. The environment influences normal system operations, emergency operations during disruptions and periods of high stress, and repair and recovery operations.
- Coupling/Response Behavior: The degree to which the infrastructures are coupled, or linked, strongly influences their operational characteristics. Some linkages are loose and thus relatively flexible, whereas others are tight, leaving little or no flexibility for the system to respond to changing conditions or failures that can exacerbate problems or cascade from one infrastructure to another.
- Infrastructure Characteristics: Infrastructures have key characteristics that figure in interdependency analyses. Principal characteristics include spatial (geographic) scales, temporal scales, operational factors, and organizational characteristics.
- Types of Interdependencies: These linkages can be physical, virtual, related to geographic location, or logical in nature.

[26] Rinaldi and Peerenboom, op. cit.

- State of Operation: The state of operation of an infrastructure can be thought of as a continuum that exhibits different kinds of behavior during normal operating conditions (which can vary between peak and off-peak conditions), during times of severe stress or disruption, or during times when repair and restoration activities are under way. At any point in the continuum, the state of operation is a function of the interrelated factors and system conditions.
- Type of Failure: Infrastructure disruptions or outages can be classified as cascading, escalating, or common-cause failures.[27]

Developing a comprehensive architecture or framework for interdependency modeling and simulation requires the coupling of multiple interdependent infrastructures. Furthermore, a comprehensive architecture or framework should be able to address all aspects of CIP/CIIP, including mitigation, response, and recovery issues. Generally speaking, simply "hooking together" existing infrastructure models is not feasible, as the differences between the models would be too large. Furthermore, such models generally do not capture emergent behavior, a key element of interdependency analysis.[28] The idea behind emergent behavior is that from simple interactions and/or rules, complex behavior can emerge at the group level that would not occur at the individual level. An emergent property is one that appears as the unpredictable result of the complex interactions of parts that themselves obey simple rules or laws.[29]

Today, many experts believe that CI interdependencies can be investigated most efficiently by comparing infrastructures to Complex Adaptive Systems (CAS), which are populations of interacting agents where an agent is an entity with a location, capabilities, and memory. CAS are real-world systems that are characterized by apparently complex behavior, which emerges as a result of often nonlinear spatial-temporal interactions among a large number of component systems at different levels of organization. With this perspective, each

[27] Ibid.

[28] Ibid., p. 23.

[29] Crutchfield, James P. "Is Anything Ever New? Considering Emergence". In: Cowan, G., D. Pines, and D. Melzner (eds). Complexity: Metaphors, Models, and Reality, SFI Series in the Sciences of Complexity XIX (Addison-Wesley: Redwood City, 1994), pp. 479–497; Mihata, Kevin. "The Persistence of 'Emergence'". In: Eve, Raymond A., Sara Horsfall, and Mary E. Lee (eds.). Chaos, Complexity, and Sociology: Myths, Models, and Theories (Thousand Oaks (etc.): Sage Publications, 1997), p. 33.

component of an infrastructure constitutes a small part of the intricate web that forms the overall infrastructure. This approach offers benefits for modeling and simulation, such as agent-based modeling and simulation (ABMS), and is able to explain emergent behavior.[30]

Modern simulation technology capitalizes on recent technological advances in evolutionary learning algorithms and massive parallel computing. Agent-based models are computer-driven tools to study the intricate dynamics of CAS. The primary assumption is that system behavior can be explained by individual traits, as the agents interact and adapt to each other and their environment. In agent-based models, complex interactions are emergent, whereas in other models, the types of interactions must be anticipated and written into the model.31 In situations with sparse or non-existent macro-scale information, as is the case for infrastructure interdependencies, agent-based models may utilize rich sources of micro-level data to develop interaction forecasts. The big disadvantage of these simulation models is that the complexity of the computer programs tends to obscure the underlying assumptions and inevitable subjective input, so that faulty assumptions can distort results significantly.

In addition, there are severe limits to the system paradigm, the main problem being one of system ontology: calculation and modeling inherently rely on our ability to define the variables of the system. This is dependent on our ability to describe the system, or more specifically, on our ability to describe the system boundaries by distinguishing between factors external to a system that may affect it (exogenous) and those internal to the system (endogenous).[32] An object, and in particular a system, can only be defined by its cohesion in a broad sense, that is, in terms of the interactions of the component elements.[33] However, it is one of the hallmarks of critical infrastructures that we may not know how to define these systems, not least because we cannot know whether a variable is part of a system, unless we already know all the variables it interrelates with, which we do not.

[30] Rinaldi and Peerenboom, op. cit.

[31] http://www.cas.anl.gov.

[32] Bertalanffy, Ludwig von. General Systems Theory: Foundations, Development, Applications (New York: George Braziller Publishing, 1968), p .141.

[33] Id. Perspectives on General System Theory: Scientific-Philosophical Studies (New York: George Braziller Publishing, 1975), pp. 165f.

Risk Analysis: Analyzing What is Threatened and How to Counter the Threats

As we have mentioned above, understanding how systems work is not sufficient for estimating what exactly to protect. In this chapter, we will focus on approaches that take into account the broader environment surrounding these infrastructures, including possible threats. These approaches are subsumed under the label of "risk analysis": Risk is a function of the likelihood of a given threat source displaying a particular potential vulnerability, and the resulting impact of that adverse event.[34] Risk analysis refers to the processes used to evaluate those probabilities and consequences, and also to the study of how to incorporate the resulting estimates into the decision-making process. The risk assessment process also serves as a decision-making tool, in that its outcomes are used to provide guidance on the areas of highest risk, and to devise policies and plans to ensure that systems are appropriately protected.[35]

The risk estimate is produced mainly from the combination of threat and vulnerability assessments. It analyzes the probability of destruction or incapacitation resulting from a threat's exploitation of the vulnerabilities in a critical infrastructure. At the very least, risk analysis encompasses risk identification, risk quantification, and risk measurement, according to the three classic questions:

[34] Stoneburner, Gary, Alice Goguen, and Alexis Feringa. Risk Management Guide for Information Technology Systems. Recommendations of the National Institute of Standards and Technology. NIST Special Publication 800-30 (Washington, January 2002), p. 8, available at: http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf.

[35] Commonwealth of Australia, Information Security Group. Australian Communications-Electronic Security Instruction 33 (ACSI 33) Handbook 3, Risk Management (draft version). http://www.dsd.gov.au/_lib/pdf_doc/acsi33/HB3p.pdf. The Australian government is currently developing a new manual: http://www.dsd.gov.au/library/acsi33/acsi33.html; Methods to Achieve Information Systems Security. Expression of Needs and Identification of Security Objectives (EBIOS). Memo - Version 1.4. http://www.ssi.gouv.fr/en/confidence/documents/memo-gb.html; Gran, Bjørn Axel. The CORAS Methodology for Model-Based Risk Assessment, version 1.0, WP2, Deliverable 2.4. (29 August 2003); New South Wales Office of Information and Communications Technology's (OICT), Information Security Guideline for NSW Government Part 1 — Information Security Risk Management. no. 3.2, first published in September 1997, current version: June 2003. http://www.oit.nsw.gov.au/pages/4.3.16-Security-Pt1.htm; Alberts, Christopher and Audrey Dorofee, OCTAVESM Method Implementation Guide, version 2.0, vols. 1–18 (Carnegie Mellon University, June 2001). http://www.cert.org/octave/pubs.html. See also: Alberts, Christopher and Audrey Dorofee. An Introduction to the OCTAVESM Method. http://www.cert.org/octave/methodintro.html.

a) What can go wrong?
b) What is the likelihood of it going wrong?
c) What consequences would arise?[36]

Often, this is followed by risk evaluation, risk acceptance and avoidance, and risk management, according to the following questions:

a) What can be done?
b) What options are available, and what are their associated trade-offs in terms of cost, benefits, and risks?
c) What impact do current management decisions have on future options?[37]

As can be easily seen, risk assessment methodologies are step-by-step approaches. The number of steps may vary and can also be adjusted to the specific needs. In the following, we show a possible nine-step approach, which is an amalgamation of various approaches currently in use.[38] Systems-based approaches often include standard security safeguards, implementation advice, and aids for numerous IT configurations typically found in IT systems today. In the context of CIP/CIIP, risk analysis could theoretically address any degree of complexity or size of system. However, when the boundaries of the evaluated system are set too wide, the lack of available data makes accurate assessment difficult or even impossible. In most cases, measures are applied locally with a focus that is confined to a business, agency, or organizational context. These approaches are based on the supposition that sufficient protection at the technical system level nullifies threats to the larger system of CI.

[36] Haimes, Yacov Y. Risk Modeling, Assessment, and Management (New York, 1998).
[37] Ibid., pp. 54–55.
[38] Stoneburner et al., op. cit.

Step 1: System Characterization

Step 1 is to define the scope of the effort and the boundaries of the system assessed. The term “system” can be defined in many different ways: It often refers to a combination of related elements organized into a complex whole, or to any collection of component elements that work together to perform a task. In the engineering disciplines, the term is often applied to an assembly of mechanical or electronic components that function together as a unit. In computing, it describes a set of computer components – an assembly of computer hardware, software, and peripherals functioning together. In the context of CIP/CIIP, a system can be seen as a compound of several CI, a single infrastructure, an infrastructure-dependent enterprise, or a particular system within a given infrastructure, according four hierarchy levels: 1) System of systems; 2) Individual infrastructures; 3) Individual system or enterprise; and 4) Technical components.[39] Once again, the larger the system we want to address, the less sure we can be of our ability to define system boundaries in any meaningful way.

Step 1 further includes the identification of all kinds of resources, assets, and information that constitute the system. An “asset” can be a tangible item (such as hardware), or a grade or level of service, staff, or information. The strategic, organizational, and risk management contexts in which the rest of the process will take place are also established in this first step. Furthermore, criteria for evaluating risk should be established , and the structure of the analysis has to be defined.[40]

[39] Schmitz, Walter. ACIP D6.4 Comprehensive Roadmap - Analysis and Assessment for CIP. Work Package 6, Deliverable D6.4, Version 1 (European Commission Information Society Technology Program, May 2003), p. 52.

[40] Emergency Management Australia. Critical Infrastructure Emergency Risk Management and Assurance Handbook (Mt. Macedon, 2003). http://www.disaster.qld.gov.au/publications/pdf/Critical_Infrastructure_handbook.pdf.

Step 2: Threat Identification

Step 2 includes the determination of (1) the nature of external and internal threats, (2) their source, and (3) the probability of their occurrence.[41] Threats can originate from a variety of sources:[42]

Natural Threats: Floods, earthquakes, tornadoes, landslides, avalanches, electrical storms, and other such events.

Environmental Threats: Long-term power failure, pollution, chemicals, liquid leakage.

Human Threats: Humans may be threat-sources through intentional acts (such as deliberate attacks by malicious persons) or unintentional acts (such as negligence and errors). A deliberate attack can be either (1) a malicious attempt to gain unauthorized access to an IT system (e.g., via password guessing) in order to compromise system and data integrity, availability, or confidentiality, or (2) a benign, but nonetheless purposeful, attempt to circumvent system security.

Individuals that have the necessary motivation and resources for carrying out an attack are potentially dangerous threat-sources. Table 1 shows an overview of common human threats, their possible motivations, and the methods or threat actions by which they might carry out an attack against the CII. This information is considered useful to organizations studying their human threat environments and customizing their human threat statements:

[41] Stoneburner et al., op. cit.

[42] Ibid., p. 13.

Human Threat-Sources	Motivations	Methods/Threat Actions
Hacker, cracker	Challenge, ego, rebellion	Hacking Social engineering System intrusion, break-ins Unauthorized system access
Computer criminal	Destruction of information Illegal information discolsure Monetary gain Unauthorized data alteration	Computer crime (e.g. cyber-stalking) Fraudulent act Information bribery Spoofing System intrusion
Terrorist	Blackmail Destruction Exploitation Revenge	Bomb/terrorism Information warfare System attack (e.g., distributed denial of service) System penetration System tampering
Industrial espionage (companies, foreign governments, other government interests)	Competitive advantage Economic gain	Economic exploitation Information theft Intrusion on personal privacy Social engineering System penetration Unauthorized system access (access to classified, proprietary, and/or technology-related information)
Insiders (poorly trained, disgruntled, malicious, negligent, dishonest, terminated employees)	Curiosity Ego Intelligence Monetary gain Revenge Unintentional errors and omissions (e.g., data entry error, programming error)	Assault on employee; Blackmail; Browsing of proprietary information; Computer abuse; Fraud and theft; Information bribery; Input of falsified, corrupted data; Interception; Malicious code (e.g., virus, logic bomb, Trojan horse); Sale of personal information; System bugs; System intrusion; System sabotage; Unauthorized system access

Table 1: Human Threats — Threat Source, Motivation, and Threat Actions[43]

However, while there is data especially for natural and environmental threats, data for human threats is hard to come by. Quantitative information on the nature and source of external threats can be derived from police reports, computer security surveys and bulletins, reports of an audit analysis, or actuarial studies. Information on internal threats can be estimated using previous experience and data, generic statistical information, or a combination of both. But it is generally acknowledged that in order to truly know how vulnerable critical infrastructures are to cyber-attacks, we would require much more information,

[43] Ibid., p. 14.

including a detailed assessment of redundancy for each target infrastructure, normal rates of failure and response, the degree to which critical functions are accessible from public networks, and the level of human control, monitoring, and intervention in critical operations.[44] However, there is no public or even readily available data on how vulnerable critical systems might be. Defense-related computers are buried under layers of secrecy and classification, and private companies are not likely to volunteer such information.[45]

Especially when dealing with actor-based threats such as terrorism, we are dealing with a "people business" that is intrinsically non-quantifiable and thus poses significant problems for a traditional risk analysis aproach.[46] But various types of uncertainties make it difficult for the intelligence community to effectively analyze the changing nature of the threat and the degree of risk involved. These uncertainties are linked to inherent characteristics of cyber-threats — characteristics that they share with a whole set of "new" threats to security.

Step 3: Vulnerability Identification

Step 3 is the development of a list of system vulnerabilities that could be exploited by the potential threat sources. Vulnerability can be defined in the context of CIP/CIIP as "a characteristic of a critical infrastructure's design, implementation, or operation that renders it susceptible to destruction or incapacitation by a threat".[47] When considering limited, technical subsystems, a vulnerability may be seen as a "flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy".[48]

[44] Lewis, James A. Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats (Center for Strategic and International Studies, 2002), p 10. http://www.csis.org/tech/0211_lewis.pdf. Haimes, Yacov Y. and Pu Jiang. "Leontief-Based Model of Risk in Complex Interconnected Infrastructures". In: Journal of Infrastructure Systems, 7, 1 (2001), pp. 1–12.

[45] Chapman, Gary. "National Security and the Internet". Paper presented at the Annual Convention of the Internet Society, Geneva, July 1998.

[46] Zimmermann, Doron. The Transformation of Terrorism. The "New Terrorism," Impact Scalability and the Dynamic of Reciprocal Threat Perception. In: Zürcher Beiträge zur Sicherheitspolitik und Konfliktforschung No. 67 (Zurich, 2003), p. 61. http://www.isn.ethz.ch/crn/extended/docs/ZB67.pdf and Metzger, op. cit.

[47] PCCIP, op. cit., Appendix, B-3.

[48] Stoneburner et. al., op. cit., p. 15.

Vulnerability assessment involves the systematic examination of critical infrastructure and the interconnected systems on which it relies (including information and products) to identify those critical infrastructures or related components that may be at risk from an attack.[49] Recommended methods for the identification of system vulnerabilities are the use of vulnerability sources, the performance of system security testing, and the development of a security requirements checklist. Again, it is far easier to assess the vulnerabilities of a relatively restricted IT system such as a business network than to do so at a higher system level.

There is a lot of emphasis on vulnerabilities in the current CIP/CIIP debate, resulting in a variety of vulnerability assessment methods and tools. However, these vary considerably in terms of the size and nature of the system they can evaluate. In the US in particular, there is a tendency to substitute vulnerability assessments for risk assessments, as exemplified in the CIAO Vulnerability Assessment Process/Project Matrix. 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. Especially when considering human threats, for example terrorism, a sole focus on vulnerabilities, sensible though it may be with respect to cost-benefit considerations, often implicitly assumes that terrorist actors will also recognize and identify the same infrastructures as priority targets — an assumption that might backfire.[50] Wrong assumptions, and hence wrong protection measures, are therefore one possible outcome of a misled vulnerability assessment.

Step 4: Control Analysis

In step 4, planned or implemented controls are analyzed in order to minimize or eliminate the likelihood (or probability) of a threat exploiting any existing system vulnerability. Security controls encompass the use of technical and non-technical methods: Technical controls are safeguards incorporated into computer hardware, software, or firmware. Non-technical controls include management and operational controls, such as security policies; operational procedures; and personnel, physical, and environmental security.

[49] PCCIP, op. cit., Appendix, B–3.

[50] Zimmermann, op. cit., pp. 61–65.

Technical protection manuals recommend security measures for selected IT systems.[51] The aim of these recommendations is to achieve a reasonable security level for IT systems that is adequate to protection requirements ranging from normal to high degrees of protection. Others provide models for the design, development, or implementation of secure IT systems, taking into consideration the four IT-security objectives: availability (of system and data for intended use only); integrity of system or data; confidentiality of data and system information; accountability.[52] Most of these objectives are business-oriented and centered on organizational information systems, which precludes them from being directly applicable to larger systems.

Step 5: Likelihood Determination

In determining the likelihood of a threat, one must consider threat sources (step 2), potential vulnerabilities (step 3), and existing controls (step 4). There are several techniques for estimating probabilities in risk analysis, such as statistical inference, scenario technique, fault trees, and event trees, which we will not discuss in more detail here. Apart from quantitative measures, the likelihood that a potential vulnerability could be exploited by a given threat source can also be described in terms of different qualitative categories (e.g., high, medium, low), based on subjective expert knowledge.

Step 6: Impact or Harm Analysis

In step 6, the adverse impact resulting from a successful threat exploitation of a vulnerability is determined. An isolated vulnerability and an isolated threat are not enough to cause harm or damage to CI/CII. Rather, the convergence of a threat with a specific vulnerability, combined with the possibility of a harmful impact, produces the risk. Such impacts represent disruptive challenges of different types, durations, and levels of severity, and can be measured using different parameters such as economic loss or social and political damage. The term "impact" is also used interchangeably with the terms "harm", "effect", or "consequence".

[51] Bundesamt für Sicherheit in der Informationstechnik. IT Baseline Protection Manual. Standard Security Safeguards (updated July 2001). http://www.bsi.de/gshb/english/menue.htm.

[52] Stoneburner et. al., op. cit.

The impact of possible harm to an asset is best determined by a business executive, an asset owner, or an asset manager. The adverse impact of a security event in an IT system can be described in terms of loss or degradation of any, or of a combination, of the IT-security objectives. Other categories might be applied if risk analysis is conducted for more abstract systems: The impact of the loss or disruption of such assets can be assessed by the use of impact factors such as area of impact, severity of impact, and time.[53] For some events (such as electronic attacks), occurrence, detection, and remedial action may all take place within a matter of days. Others will have a much longer timeframe: for example, the impact of global warming will be felt over decades and centuries. Also, impact categories that correspond to indicators used to measure criticality can be used, such as service delivery, public, economic, political, environmental, interdependency.

Some tangible impacts can be measured in a quantitative manner in terms of lost revenue, the cost of repairing the system, or the level of effort required to correct problems caused by a successful threat action. Other effects (e.g., loss of public confidence, loss of credibility, damage to an organization's interest) cannot be measured in specific units, but can at least be qualified or described in terms of high, medium, and low impact.[54] However, in interdependent systems, assessing the result of the loss of a critical asset becomes fairly complex.

Step 7: Risk Determination

The purpose of step 7 is to assess the level of risk to the system. The determination of risk is a function of the likelihood that a given threat source will attempt to exploit a given vulnerability (step 5) and the magnitude of the impact, should a threat source successfully exploit the vulnerability (step 6).

Step 8: Countermeasure Priority Rating

The countermeasure rating expresses the difference between the required risk (desired "risk level" as set by the management authority of the system) and the resultant risk (step 7). It is used to provide guidance as to the importance

[53] Public Safety and Emergency Preparedness Canada (PSEPC). Assets criteria. http://www.psepc-sppcc.gc.ca/prg/em/nciap/assets_criteria-en.asp.

[54] Stoneburner et. al., op. cit., p. 22.

that should be placed on security countermeasures. Again, applied values and categories may vary widely.

Table 2 is an example of a Risk Assessment Table, which helps to calculate the level of the Countermeasure Priority Rating (column 7). Column 7 is simply the difference between the resultant risk and the required risk (Columns 6 and 5 in the example) expressed as a numerical value.

Column 1 Asset Identification	C 2 Threat to the Asset	C 3 Threat Likelihood	C 4 Harm	C 5 Resultant Risk	C 6 Required Risk	C 7
Row 1: Reliability of e-commerce-related web-site	Accidental electrical power or equipment failure	Medium	Grave	Critical	Nil	4
Row 2: Accuracy of publicly available web information	Loss of confidence or goodwill due to "hacking" of web page	High	Minor	Medium	Low	1
Row 3: Secure access to internal network services by authorized staff, from external networks	Loss of crypto token or keys required to access the secure channel(s)	Very Low	Serious	Medium	Low	1

Table 2: Risk Assessment Table[55]

Step 9: Risk Mitigation

Step 9 is about risk mitigation and involves prioritizing, evaluating, and implementing the appropriate risk-reducing controls suggested by the risk assessment process. Because the elimination of all risk is usually impractical or near-impossible in reality, the stakeholders themselves must use the least-cost approach and implement the most appropriate controls to decrease mission risk to an acceptable level.[56]

[55] Commonwealth of Australia. ACSI 33. Handbook 3, Risk Management, Appendix. http://www.dsd.gov.au/_lib/pdf_doc/acsi33/HB3Ap.pdf.

[56] Stoneburner et. al., op. cit.

Different kinds of security controls, or a combination of such controls, can be applied at the technical, management, and operational levels with the goal of maximizing the effectiveness of controls for IT systems and organizations.

- Technical security controls for risk mitigation can be configured to protect against given types of threats. These security controls may range from simple to complex measures. They usually involve system architectures; engineering disciplines; and security packages with a mix of hardware, software, and firmware.
- Management security controls, in conjunction with technical and operational controls, are implemented to manage and reduce the risk of loss and to protect an organization's mission. Management controls focus on the stipulation of information protection policy, guidelines, and standards.
- Operational controls, implemented in accordance with a basic set of requirements (e.g., technical controls) and good industry practices, are used to correct operational deficiencies that could be exploited by potential threat sources.

This concludes our exemplified risk analysis approach.

Analysis of Methods in Use and Conclusion

In order to cost-effectively prioritize means of preparing for, mitigating, and responding to possible risks against crucial assets, a variety of issues need to be evaluated and analyzed. A review of current methodologies for analyzing CII – both for information systems as well as for the larger set of critical infrastructures –shows that they often prove to be insufficient. In fact, it is obvious that various methodological approaches fall short in a number of substantial areas, mainly due to the ever-more complex risk environment and the dynamically changing characteristics of the systems under consideration.

Many conceptual shortcomings become apparent when the discussion moves to the systems that have become vital to modern society. The greatest of these shortcomings 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. At the moment, our "methodological toolbox" is filled with old tools, which have, in some cases, been hurriedly adapted to a new set of problems. However, both the systems and the risk environment have become qualitatively different in a way that demands new analytical techniques and methodologies for their evaluation:

Unbounded systems: Risk assessment originated in the technical context of limited or "closed" systems. Today, however, we are no longer dealing with closed systems in a centrally networked environment, but systems that are part of global network environment that knows no bounds, no central control, and offers only limited insight into the underlying system structure. These unbounded systems also lack well-defined geographic, political, cultural, and legal and jurisdictional boundaries.[57]

Complex, interdependent systems: Risk assessment breaks problems down into smaller parts. However, both infrastructures and information infrastructures are highly complex and interdependent systems. One of the hallmarks of complex systems is that they display emergent behavior that is a property of the system as a whole and that cannot be studied by taking it apart.[58] Due to system complexity, vulnerabilities and infrastructure disruptions are no longer traceable in any useful way to single technical subsystems and vice versa. Therefore, even if one carefully examines a relatively localized subsystem from the point of view of risks and threats, these insights can hardly be generalized and formalized for application "beyond" the subsystem itself or at a higher system level.

Interdependency: In addition, current assessment methods fail to address the crucial issue of (bi-) directional relationships between infrastructure components, subsystems, or systems (interdependencies) in any meaningful way. In this way, 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,

[57] Ellison, R. J., D. A. Fisher, R. C. Linger, H. F. Lipson, T. Longstaff, and N. R. Mead. Survivable Network Systems: An Emerging Discipline (technical report, November 1997). CMU/SEI-97-TR-013. ESC-TR-97-013, pp. 4–6. http://www.cert.org/research/97tr013.pdf; Allen, Julia H. and Carol A. Sledge. "Information Survivability: Required Shifts in Perspective". In: CrossTalk: The Journal of Defense Software Engineering, July 2002: pp. 7–9. http://www.stsc.hill.af.mil/crosstalk/2002/07/allen.html.

[58] Crutchfield, op. cit., pp. 479–97.

it applies to 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 sole focus on technical systems and subsystems is misleading: The importance of laws, regulations, policies, and other economic, social, and national-security considerations for the infrastructure environment makes it indispensable to study their impacts on interdependent infrastructures at all times.[59] In addition, the level of damage impact that is acceptable to society is determined more by political criteria than by system-technical standards: One of the crucial questions is how damage to or the disruption of an infrastructure would be perceived and exploited politically.[60] Risk assessment, however, does not offer any method for cataloguing objects, vulnerabilities, and threats at a strategic policy level, such as the economy at large, in a meaningful way. In addition, a preoccupation with technologies risks disregarding one rather central element of the information infrastructure – people. Humans are, in effect, one of the most substantial parts of the information "infrastructure", as they provide, manage, and generate new information, operate, maintain, and occasionally even subvert other elements of information infrastructure. As the cognizant agent in the game, they also play a major part on the threat side of the equation. This is especially interesting since experts consider the threat emanating from "insiders" to be far greater than that of anonymous "cyber-terrorists"[61] — meaning that an element that is part of the information infrastructure can also constitute the greatest danger to it.

Lack of data for many important threats: Even though there are various methods of conducting a risk assessment, 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 there are no useful statistics for possible damage and failure probabilities.

[59] Rinaldi and Peerenboom, op. cit.

[60] Metzger, op. cit.

[61] Lewis, op. cit.

Static approach: Even though a risk assessment could theoretically be carried out on a daily basis, it is a static approach aimed at evaluating current systems and vulnerabilities. Since the process is time-consuming, there is always a delay until its results can be determined and implemented. This is especially worrying in view of the continuous rapid technological developments and because many related challenges and problems are only just emerging; the system characteristics of the emerging information infrastructure will, in fact, differ radically from traditional structures in terms of scale, connectivity, and dependencies. The interlinked aspects of market forces, technological evolutions, and newly emerging risks forces analysts to constantly look ahead and to develop new analytical techniques, methodologies, and mindsets. Their development will, in turn, require great efforts in unconventional and proactive thinking.

In conclusion, effective security demands a far more profound understanding of various crucial aspects of the communication networks and information systems under consideration, such as their behavior under normal circumstances and under stress, as well as their role and criticality for the economy and society. We should therefore aim to widen the focus of our enquiry in order to understand emerging risks in their appropriate technological and socio-political context. In addition, governments could help to encourage dialog between experts from various disciplines, ranging from engineering and complexity sciences to policy research, political science, psychology, and sociology.