17. The concept of critical infrastructure protection

Jan Metzger

I. Introduction

The US Department of Homeland Security (DHS) was established on 1 January 2003, following the largest administrative restructuring undertaken in the United States since World War II. The task of the 170 000 DHS employees, in over 20 agencies and under the leadership of Secretary of Homeland Security Tom Ridge, is to protect the nation against the threat of terrorist attacks. A sizeable portion of the budget for fiscal year 2003 of nearly $38 billion will be allocated to the area of Information Analysis and Infrastructure Protection, one of the four main DHS directorates. A major task of the Assistant Secretary for Infrastructure Protection, Robert P. Liscouski, will be to conduct a comprehensive analysis of critical infrastructures and to put in place a national protection plan.[1]

What does critical infrastructure protection (CIP) entail? Is CIP a feasible concept for the pursuit of traditional security policy goals, such as 'independence', 'territorial sovereignty' and 'national security'?[2] This chapter begins by defining the term CIP. It then assesses the concept, applying the following criteria: (*a*) linguistic usage compared with actual practice (the operational perspective), and (*b*) analytical and terminological precision (the conceptual perspective).

II. CIP from an operational perspective

The concept of 'critical infrastructure' was the subject of political debate in the United States even before the current focus on terrorism. There was a lively debate on infrastructure security in the 1980s, but there was no generally accepted definition or common understanding of the term.[3] The 1997 report of

[1] The Department of Homeland Security was established on 1 Jan. 2003. See the DHS Internet site at URL <http://www.dhs.gov>. On the Information Analysis and Infrastructure Protection Directorate see URL <http://www.dhs.gov/dhspublic/display?theme=13>.

[2] For the Swiss context see Article 2 (Purpose) of the Swiss Federal Constitution, available on the University of Bern Internet site at URL <http://www.oefre.unibe.ch/law/icl/sz00000_.html>; and *Security through Cooperation: Report of the Federal Council to the Federal Assembly on the Security Policy of Switzerland*, no. 97.667e, 7 June 1999, URL <http://www.vbs-ddps.ch/internet/vbs/en/home/publikationen/berichte.html>. Other security policy goals, such as 'solidarity' or 'stability and peace beyond the borders', are deliberately excluded in this context.

[3] 'With no standard or agreed definition, the concept of infrastructure in policy terms has been fluid, as it appears to be today.' Moteff, J., Copeland, C. and Fischer, J., *Critical Infrastructures: What Makes an Infrastructure Critical?*, Report for Congress (Library of Congress, Congressional Research Service:

the President's Commission on Critical Infrastructure Protection (PCCIP) presented a broad definition of critical infrastructures, reflecting a multitude of requirements and perspectives.[4] After a process of policy transposition—that is, after transferring and adapting a political paradigm to a different national context—many countries launched CIP initiatives that focused more or less exclusively on the Internet or cyber communications.[5] For example, efforts to meet the requirements for a US national CIP plan included a strategic Internet security plan which was presented in 2000, although it largely neglected physical infrastructure protection.[6]

It is important to distinguish between the protection of critical infrastructure in general and the protection of critical information and telecommunication infrastructures—critical information infrastructure protection, CIIP—as a subordinate task. The distinction is often not obvious or easy to make because of the crucial role of CIIP in an overall CIP strategy. In official publications, both terms are often used to refer to CIIP. However, it is important to note that CIP comprises *all* critical sectors of a nation's infrastructure, while CIIP is only a subset of a comprehensive protection effort.[7]

The *International CIIP Handbook* defines CIIP as 'a subset of CIP. CIIP focuses on the protection of systems and assets including components such as telecommunications, computers/software, Internet, satellites, fiber optics, etc., and on interconnected computers and networks, and the services they provide'.[8] This task is particularly important for three reasons: first, as an economic sector, these infrastructures represent a major component of economic value creation. Second, they act as a crucial interconnecting link between other areas of infrastructure. Even under normal conditions, they are essential for the proper functioning of all other infrastructures. Third, in a crisis situation they are a crucial tool for managing risk factors and re-establishing normal conditions.[9]

Washington, DC, Updated 29 Jan. 2003), p. CRS-1, available at URL <http://www.fas.org/irp/crs/RL31556.pdf>.

[4] *Critical Foundations: Protecting America's Infrastructures*, *The Report of the President's Commission on Critical Infrastructure Protection*, Oct. 1997, URL <http://www.ciao.gov/resource/pccip/PCCIP_report.pdf>.

[5] See Wenger, A., Metzger, J. and Dunn, M. (eds), *International CIIP Handbook: An Inventory of Protection Policies in Eight Countries* (Swiss Federal Institute of Technology, Center for Security Studies: Zurich, 2002), available at URL <http://www.isn.ethz.ch/onlinepubli/publihouse/misc/ciip>.

[6] *Defending America's Cyberspace: National Plan for Information Systems Protection, Version 1.0, An Invitation to a Dialogue* (The White House: Washington, DC, 2000), available at URL <http://www.ciao.gov/publicaffairs/np1final.pdf>. For the more recent version of Feb. 2003, see the US Department of Homeland Security Internet site, 'The National Strategy to Secure Cyberspace', URL <http://www.dhs.gov/interweb/assetlibrary/National_Cyberspace_Strategy.pdf>.

[7] Dunn, M. and Wigert, I., *The International CIIP Handbook 2004: An Inventory of Protection Policies*, eds A. Wenger and J. Metzger (Swiss Federal Institute of Technology, Center for Security Studies: Zurich, forthcoming 2004), Introduction.

[8] See Wenger, Metzger, and Dunn (note 5), glossary of key terms, p. 178.

[9] Wenger, A., Metzger, J. and Dunn, M., 'Critical information infrastructure protection: eine sicherheitspolitische Herausforderung' [A challenge for security policy], eds K. R. Spillmann and A. Wenger, *Bulletin zur Schweizerischen Sicherheitspolitik* [Bulletin on Swiss security policy] (Swiss Federal Institute of Technology, Center for Security Studies: Zurich, 2002), pp. 119–42 (in German).

Clearly, the observable tendency to reduce CIIP (or even CI) to an issue of computer security—with its attendant exclusive focus on isolated, often technological aspects, as illustrated by terms such as 'cyber terrorism', 'cyber crime' and 'cyber warfare'—is problematic and short-sighted. Terrorists do not tend to restrict their range of options or to operate solely in one dimension of threat. The perpetrators of political violence are not exclusively 'cyber' terrorists but choose the particular area or specific tool with which they can best achieve their political objectives. In order to combat the challenge of terrorism successfully, Western information societies must endeavour to think like the perpetrators of terrorist attacks—and hence to think not illogically, but according to the logic of terrorists. It is the nature of the threat, not the instruments through which the threat manifests itself (physical, network-based or biological agents), which must be taken as the basis for analysis and should serve as a guidance for institutional preparedness and defence.

Several features make CIIP a special case of CIP, meriting modern societies' serious concern and attention. For one thing, the system characteristics of the emerging information infrastructure differ radically from those of traditional structures, including earlier information infrastructures: in terms of scale, of connectivity and of dependencies. This is especially important because understanding them will require new analytical techniques and methodologies. Second, the subject of cyber-network security is evolving rapidly in terms of technological capabilities and modern societies' vulnerabilities.[10] The cyber threat has thus become a prototype for studying the asymmetric nature of 'new' or 'emerging' risks and institutional response policies.

Moreover, several driving forces are likely to aggravate the problem of critical information infrastructures in the future: namely, the interlinked aspects of market forces, technological evolution and emerging risks.[11] On the one hand, the dynamic globalization of information services, combined with technological innovation (e.g., localized wireless communication), will result in a dramatic increase in the level of connectivity, lead to poorly understood systems behaviour and create new vulnerabilities. Added to this is the fact that security has never been a driver of design. Since pressure to reduce the time from designing a product or service to marketing it is intense, a further dramatic increase in computer and network vulnerabilities can be expected. There is therefore a risk of the potential emergence of infrastructures with built-in instabilities, critical points of failure, and extensive interdependencies. In addition, increasingly large parts of the critical infrastructure of a given territory will be in the hands of the private sector, or even another state, since the injection of sufficient capital and cost-effective development is a prevailing market driver.[12]

[10] Dunn and Wigert (note 7).

[11] Dennis, I. and Conroy, R., *New Technology as a Threat and Risk Generator: Can Countermeasures Keep Up with the Pace?*, ed. G. Jervas (Swedish Defence Research Agency: Stockholm, Mar. 2001).

[12] Dunn and Wigert (note 7).

This forward-looking perspective points clearly to a need to distinguish conceptually between the CIP and CIIP concepts. However, the two concepts cannot and should not be completely isolated from each other. As stated above, CIIP is an essential part of CIP. An exclusive focus on cyber threats that ignores important traditional physical threats is just as dangerous as neglecting the aspect of cyber-network security. What is needed is sensible handling of both concepts as interrelated but conceptually separate.[13]

III. CIP from a conceptual perspective

If there is no general, standardized usage and broad-based mutual understanding of the term CIP, what can be said about its analytical and terminological precision? In order to answer this question, the terms 'infrastructure', 'critical' and 'protection' must be examined more closely.

The term 'infrastructure' describes the underlying basis of an organization or system, for example, a country. Information and telecommunications systems; banking and financial institutions; water, electricity, oil and gas supplies; transportation and logistics structures; and health and emergency services are all essential infrastructures.

The essential nature of these infrastructures also presents a central problem. If it is assumed that security policy, as a 'policy for extraordinary circumstances' or as a policy for existential threats, is something removed from the realm of everyday politics—or at least represents a special form of policy—a purely practical question of definition arises: when is critical infrastructure protection an issue of maintaining 'business continuity' for an individual, corporate or local actor and when is it the subject of national and, where necessary, even international security policy?[14] The problem of distinguishing between everyday operations and regulatory policy, on the one hand, and defence and security policy, on the other hand, is further exacerbated by the fact that many of the above-mentioned infrastructures are privately owned and controlled, in some cases from abroad. Some may not even be located within the territory of the state in question.

The fact that CIP is a multifaceted issue of high relevance to many different, very diverse and often overlapping communities is a major obstacle to academic and practical dialogue. Because different groups do not necessarily agree on what the problem is or what needs to be protected, the actual meaning ascribed to critical information infrastructure depends to a great extent on the group. To complicate the picture, the boundaries between the different perspectives are by no means clear-cut.

The following list presents the most important perspectives as ideal types and in simplified form.[15]

[13] Dunn and Wigert (note 7).

[14] Buzan, B., Weaver, O. and de Wilde, J., *Security: A New Framework for Analysis* (Lynne Rienner: London, 1998), p. 24.

[15] Dunn and Wigert (note 7).

The system-level, technical perspective: CIP is approached as a question of information technology (IT) security or information assurance, with a strong focus on Internet security.

The business perspective: CIP is seen as a question of 'business continuity'.

The law-enforcement perspective: CIP is seen as a question of protecting society against (cyber) crime.

The defence perspective: This perspective is centred on either military or civil protection.

The regulatory policy perspective: The smooth and routine operation of infrastructures and questions such as privacy, or hardware and software standards, must be regulated.

The national and international security policy perspective: This perspective is addressed in this chapter.

Thus infrastructures are viewed as objects to be protected against crime, as competitive advantages in the private sector, as technical/operative systems, as defence-relevant strategic assets, and as objects that are relevant for the formulation of national and international security policy. One final aspect—and one that is frequently ignored—is that infrastructures are also objects of individual cognition and of public reflection and perception. As objects of both historical consciousness and contention in current political debates, they are inextricably associated with such notions as 'risk', 'threat', 'trust', 'crisis', 'disaster' and 'catastrophe'.

If the perspective is widened accordingly, a fundamental question must be asked: whether it is primarily the actual infrastructures that need to be protected. In fact, the real focus of interest in protection is the services, the physical and electronic flows of information as well as their role and function, and in particular the core values symbolized by infrastructures. Whereas infrastructures are constructed, maintained and operated by people, and have relatively clear organizational and institutional hierarchies, it is much more difficult to represent and comprehend the services, flows and especially the core values they give rise to because of their intricate significance and interconnections. In order to take into account the system dynamics involved and interests in protection, it would make more sense to speak of 'critical services robustness' or 'critical services sustainability' rather than CIP.

IV. Criticality

The word 'critical' is more appropriate than 'infrastructure' for making a conceptual distinction between normal operating procedures and strategic security policy. For example, the German Federal Office for Information Security dis-

tinguishes between protecting 'critical infrastructures' and protecting 'business-critical infrastructures'.[16]

Is this also appropriate for the distinction between everyday routines and crisis situations? There are two trends: first, in the public perception, there are increasingly fewer genuinely 'natural' catastrophes about which we can do nothing. Such events are more often seen as the result of policy failure, or the failure of politicians, and personal responsibility is increasingly called for. Second, the criterion for what constitutes 'good' policy is changing: the future career of political decision makers is not determined by their administrative competence during routine periods, but by their management efficiency before, during and after a crisis.

The definition of 'critical' is highly dependent on the author of the definition, but the concept itself is also undergoing constant change. A survey of the literature on critical infrastructure protection, and of the general definitions for and lists of critical infrastructures, shows a great variety. The main reason is that the criteria for qualifying infrastructures as critical have expanded over time; the PCCIP, for example, defined critical infrastructures as assets whose prolonged disruption could cause significant military and economic dislocation.[17] Today the term also includes national monuments where an attack might cause a large number of casualties or adversely affect the nation's morale. This development permits a typology of two different but interrelated ways of understanding criticality.

Criticality as a symbolic concept. An infrastructure is inherently critical because of its role or function in society. This means that an existential security policy objective, such as territorial sovereignty, cannot be achieved in the event of the collapse of or damage to the infrastructure. In this case, it is basically the national interest, rather than the infrastructure itself, that is critical. In theory, the question whether, or to what degree, the infrastructure is interconnected with other areas is irrelevant—the inherent symbolic meaning of certain infrastructures per se makes them potential targets. For example, the US Congress building and the White House represent attractive targets for various groups of terrorists because they are symbols of national power.[18]

Criticality as a systemic concept. An infrastructure is critical because of its *structural positioning* in the whole system of infrastructures, especially when it is an important link between other infrastructures or sectors. Electric power

[16] See the Internet site of the Bundesamt für Sicherheit in der Informationstechnik (Federal Office for Information Security) at URL <http://www.bsi.bund.de/fachthem/kritis/index.htm>, and in English: 'BSI IT security topic briefing: critical instrastructures in state and society', at URL <http://www.bsi.bund.de/literat/faltbl/kritis_e.htm>.

[17] *Critical Foundations: Protecting America's Infrastructures* (note 4).

[18] For an example of this view of a 'criticality' assessment, without reference to the aspect of networking, see US General Accounting Office (GAO), *Homeland Security, Key Elements of a Risk Management Approach,* Statement of Raymond J. Decker, Director, Defense Capabilities and Management, Testimony before the Subcommittee on National Security, Veterans Affairs, and International Relations, House Committee on Government Reform (GAO: Washington, DC, 2001), p. 6, available at URL <http://www.gao.gov/new.items/d02150t.pdf>.

and information/telecommunication networks are of special importance in terms of interconnection and dependability. Accordingly, in its final report of 1997, the PCCIP defined infrastructures as 'a network of independent, largely private-sector owned, technical (man-made) systems and processes.'[19]

The concept of symbolic criticality allows non-networked and non-technical objects, systems and processes to be integrated into protection and emergency planning. Human targets, such as the president of a country, or national heritage sites with a strongly symbolic character are 'critical' targets not because of their networking significance, but because of their function and importance for national pride, that is, for their significance for the identity of a people as a nation.

The typology described above is of course an idealized, even artificial one: in reality, infrastructures can rarely be separated from one another. Energy generation is dependent on transport, while transportation methods are, in turn, dependent on energy; both require functional information networks, while information networks are dependent on energy, and so on. The example of the New York World Trade Center (WTC) shows how different types of criticality are likely to be combined in certain objects. In the case of the attacks of 11 September 2001, there was an accumulation of different 'criticalities': the importance of the WTC within the financial system as a juncture of global monetary flows, as a large workplace, as an administrative centre and tourist site, and for its symbolic significance as *the* World Trade Center.

It would be fair to say that the systemic understanding of criticality, with its understanding of infrastructures as 'complex, adaptive systems', provides a more satisfactory representation of everyday reality in all its complexity. It is also more amenable than symbolic criticality to an empirical analysis based on statistical data. Security policy analysts hold that systemic criticality has a disadvantage in that it is more difficult to make a distinction between optimizing routine emergency management and a 'policy for existential threats', whereas symbolic criticality is, by definition, placed in a security policy context. This approach allows the national security analyst and researcher to define relevant assets more easily than the systemic one, because it is not the interdependencies as such that are definitive in a socio-political context, but the role, relevance and symbolic value of specific infrastructures.

A key problem is that the notion of 'critical infrastructure' has over the past few years moved away from a technical scientific or at best system-theory expert level, and has been introduced into the political agenda, without intellectually adapting the CIP concept to this very different socio-political context. The term 'critical' is etymologically related to the word 'crisis'. Crises are, by their very nature, social events: they affect individuals, a group, an

[19] *Critical Foundations: Protecting America's Infrastructures* (note 4).

organization, a society and/or a state. They are characterized by the very fact that 'critical' decisions are (or must be) taken when they arise.[20]

It is possible to measure system criticality, resilience and robustness with a certain degree of objectivity: first, as part of the process of 'optimizing the normal case'; and second, at the level of technical infrastructure. At the security policy level, however, risks, threats and crises can be neither quantified nor objectively compared with one another. Given the degree to which criticality manifests itself in every crisis, there is little point in excluding non-technical and non-networked items requiring protection. It is not the networking aspect, but rather the significance of the infrastructure per se that is the decisive criterion for categorizing an infrastructure as 'critical' on a security policy level. Crises with relevance for security policy are *by definition* critical and complex events, in terms of when and where they take place, the interaction between the institutions involved on a vertical (federal, state and municipal) and horizontal (inter-ministerial) level, the identification of the problems that arise, and the information needs and surpluses that are revealed.[21]

Even where quantitatively exact measurement is not possible, this does not necessarily mean that the situation is of no importance, and this certainly does not prevent its being dealt with by means of preventive risk reduction measures based on risk awareness. One example illustrates this well: at the individual level, the risk of being hit by an automobile represents one of the most extreme events of all. There are detailed statistics on how many pedestrians are run over each year in different countries, but the average citizen is unaware of these empirical data. Yet, every day, people perceive this risk as relevant and adopt an appropriate risk-reduction strategy by using pedestrian crossings. This example illustrates that the statement 'you can only improve what you can measure' is false. It is not primarily a quantitative but rather a qualitative knowledge of risks and vulnerabilities that is needed, not only to protect pedestrians and other road users, but also to protect infrastructures against terrorist threats. Recently, three risk analysts asserted: 'Understanding and reducing vulnerability does not demand accurate predictions of the incidence of extreme events'.[22]

For security policy analysis, the task ahead is not so much to measure crises precisely, but rather to determine under what circumstances they *start, develop and end*. Taking a broad contextual and a methodologically interdisciplinary approach, the characteristics of crises, the detailed structural circumstances that lead to them and their consequences must be revealed. Extreme events are created and characterized *by their context*:

[20] On the definition of 'crisis' see Stern, E. K., Crisis Management Europe Research Program, *Crisis Decisionmaking: A Cognitive–Institutional Approach* (Swedish National Defence College: Stockholm, 2001), pp. 4–6.

[21] Stern (note 20), pp. 14–16.

[22] Sarewitz, D., Pielke, R. and Keykhah, M., 'Vulnerability and risk: some thoughts from a political and policy perspective', *Risk Analysis,* vol. 23, no. 4 (Aug. 2003), p. 807, URL <http://www.cspo.org/products/articles/Vulnerable.pdf>.

The character of an extreme event is determined not simply by some set of characteristics inherent in the physical phenomena (e.g., a hurricane, or monsoon rains), but by the interaction of those characteristics with other systems . . . A focus on vulnerability management would require a clear-eyed view of the limits of predictive science to guide the way to an uncertain future and instead focus on the design of healthy decision processes flexible enough to learn from experience and intelligent enough to assess alternative approaches to vulnerability management.[23]

In contrast to technical infrastructure analysis, security policy research is less concerned with identifying objective crisis thresholds than with investigating *actors* and *events*, as well as *when, in what context, how and with what result* a crisis occurred. This is based on the conviction that the principal concern of strategic policy direction must be *not to overlook* any risk, rather than to *precisely measure* those risks that have already been identified. People, and also collective groups of people such as states, do not react directly to an objectively constituted environment, but rather according to their own perception of reality. For that reason, it is not helpful, either politically or analytically, to attempt to identify 'real security' in isolation from a political context.[24] In German-speaking countries, the difficulty of distinguishing between a technically operational CIP analysis and a socio-political one is exacerbated by the fact that *Sicherheit* can be translated as both 'safety' and 'security'.

The question of the criticality of an infrastructure is inseparable from the issue of how the impact on an infrastructure is politically perceived, capitalized, dealt with and exploited. When does the image of a threat become a security policy issue, and when does it not? Eriksson and Noreen cite various factors that influence individual perceptions of threat images. Taken as a whole, these factors to some extent determine whether threats appear on the political agenda, disappear from it, persist or are even given higher priority. They include the crisis experiences of a community, aspects of identity, the political and institutional context and the influence of public opinion.[25] In this context, it is interesting to note that different political parties place priority on different threat images. Typically, political parties oriented on environmental issues tend to have a broader concept of security, while the perception of conservative parties traditionally focuses on military threats.

This aspect is also of crucial importance in the current debate over the fight against terrorism. Terrorism could be said to be primarily, although not exclusively, a form of communication. The actual goal of terrorists is not primarily to commit acts of violence against their victims per se, but to influence the

[23] Sarewitz, D. and Pielke, R., 'Vulnerability and risk: some thoughts from a political and policy perspective', Discussion paper prepared for the Columbia–Wharton/Penn Roundtable on Risk Management Strategies in an Uncertain World, 4 Apr. 2002, p. 4, URL <http://www.ldeo.columbia.edu/res/pi/CHRR/Roundtable/Pielke_Sarewitz_WP.pdf>; and Sarewitz, D. and Pielke, R., 'Extreme events: a research and policy framework for disasters in context', forthcoming in *International Geology Review*, URL <http://www.cspo.org/products/articles/xepaperfinal.pdf>.

[24] Buzan, Weaver and de Wilde (note 14), p. 31.

[25] Eriksson, J. and Noreen, E., *Setting the Agenda of Threats: An Explanatory Model*, Uppsala Peace Research Paper no. 6 (Uppsala University, Department of Peace and Conflict Research: Uppsala, 2002), pp. 12–15, available at URL <http://www.pcr.uu.se/publications/UPRP_pdf/uprp_no_6.pdf>.

consciousness of a broad spectrum of the public who witness their attacks in their 'theatre of operations'.[26]

It follows that CIP studies on a security policy level should focus primarily on the subjects of political culture, political debate and political (party) constellation. CIP research seen in this way is first and foremost an analysis of the political context in which infrastructures can be identified, analysed and protected. It is not the CIP analyst but rather the political actors, and especially the general public, who determine whether a threat is accepted as 'critical'.

It is important to note that this political context also includes the politically motivated perpetrator or terrorist who consciously and deliberately attacks an infrastructure. Many infrastructure studies use a largely 'intra-system' determination of criticality, by considering which infrastructures are linked to one another, and how and where. The approach of the German Federal Office for Information Security is an example of a problematic approach: its analysis consciously looks at vulnerabilities 'independently of the type of threat'.[27] However, vulnerabilities manifest themselves only in their particular context, in other words in relation to the threats relevant for decision making. This analytical approach thus needs to be extended if criticality is to be determined not purely by structure, but also by violence and symbolism. As Doron Zimmermann explains, terrorism is a 'people business' that is intrinsically non-quantifiable. 'We should first know who (actors, motives and objectives) and what (organizations and capabilities) we are dealing with, before jumping to conclusions, comparing and referencing with a known, but possibly inapplicable, body of knowledge and committing resources to protect and counteract on that basis.'[28]

Even though criticality cannot be measured objectively, indicators can be established to determine whether damage to an infrastructure is critical or not. For example, US Presidential Decision Directive 63 (PDD-63) of May 1998 states that: 'Any interruptions or manipulations of these critical functions must be brief, infrequent, manageable, geographically isolated and minimally detrimental to the welfare of the United States'.[29]

In addition, the criticality of an infrastructure can also be analysed in terms of another factor: the measure of loss of *trust* suffered by the state when a

[26] Hoffmann, B., *Inside Terrorism* (Columbia University Press: New York, 1998), available in German translation as *Terrorismus: Der unerklärte Krieg, Neue Gefahren politischer Gewalt* [The undeclared war: new dangers of political violence], (Fischer: Frankfurt am Main, 2001), p. 48.

[27] Blattner-Zimmermann, M., 'Schutz Kritischer Infrastrukturen in Deutschland' [Protection of critical infrastructures in Germany], Speech at the Lucerne meeting on information security (Luzerner Tage für Informationssicherung, LUTIS), 24 June 2003, Transparency 7, URL <http://www.infosurance.ch/de/lutis_downl.htm> (in German). See also Bundesamt für Sicherheit in der Informationstechnik, 'Kritische Infrastrukturen' [Critical infrastructures], URL <http://www.bsi.bund.de/fachthem/kritis/kritis.htm>.

[28] Zimmermann, D., *The Transformation of Terrorism: The 'New Terrorism', Impact Scalability and the Dynamic of Reciprocal Threat Perception*, Zurich Contributions to Security Policy and Conflict Research no. 67 (Swiss Federal Institute of Technology, Center for Security Studies: Zurich, 2003), p. 61.

[29] 'The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63', White Paper, 22 May 1998, section III, A national goal, URL <http://www.fas.org/irp/offdocs/paper598.htm>.

service is disrupted. This is a useful yardstick in that public demands for government to take responsibility, even in cases involving private sector control of ownership, are a clear indication that a vital service has been affected. Despite the fact that baggage controls for domestic flights were largely the responsibility of private companies at US airports on 11 September 2001, public opinion blamed the terrorist attacks on negligence on the part of federal authorities and thus, by extension, the government. In other words, it is the perception of risk and the reaction to risk on the part of the public, and not the analyst, that ultimately determines whether an event represents a catastrophe, whether an attack triggers an existential crisis and whether an infrastructure or service is 'critical'. From this perspective, the criticality of an infrastructure cannot be determined in a preventive manner, based on empirical data, but only on an *ex post facto* basis as the result of a normative process.

The term 'protection', creating a mental image of 'all or nothing', is also not appropriate for addressing the complexity of modern infrastructure vulnerabilities, because it is impossible to ensure full protection. For this reason, it would be better to use a word from the vocabulary of the natural sciences, such as 'robustness' or 'resilience', and in general to use the terms 'survival capability' or 'regenerative capability', 'availability', 'stability' or 'reliability'.

It thus becomes apparent that CIP describes a natural, age-old, ultimately biological phenomenon—not a new technical phenomenon. For example, trees undergo a process in the autumn that could also be described as critical infrastructure protection: they reduce their activities to the minimum level required to survive a period of stress, the winter. This is also a familiar concept from military contexts: Switzerland's defence strategy in World War II, withdrawal to the 'Alpine recess' (*réduit*) was based on the same strategy and philosophy.

V. Conclusions and recommendations

'Critical infrastructure protection' is an unfortunate term: it is often used incorrectly and analysed from inappropriate perspectives. The main problem is that it originated in the technical–scientific context of closed systems. Since 1996, CIP has been used indiscriminately in the security policy debate and without regard to the different contexts of open systems. As a result, infrastructure analysis is still often understood as a precise instrument, which largely ignores the socio-political and cognitive context of the power relationships, actors, cultures and interests involved. For example, the threat of terrorism is often either excluded—because it cannot be measured—or considered as a 'black box', without any attempt to draw on the expertise of intelligence services to verify the plausibility of attacks from a terrorist actor's point of view. A British Government report came to a similar conclusion: some applications of the risk management concept were too mechanical and were insufficiently adapted to decision making at the highest strategic level. The higher the assessment of the risks was, the more difficult it was to identify and quan-

tify them, the more destructive the effects and the more unstable the situation. Accordingly, the report recommended that risk identification, or 'horizon scanning', should be broadly defined, and that risk analysis should be based more on judgements than on empirical facts.[30] Extreme events or 'mega-risks', also known as 'wild cards' in scenario technique terms, combine low probability with large-scale damage: they represent existential risks, by definition; and they are typically unforeseeable events. For this reason, and specifically in relation to the threat of terrorism, infrastructure may be critical for strategic protection and defence planning even when the risks cannot be measured exactly.

Over the past few years, a series of methods have been developed for the analysis of critical infrastructure interdependencies. For example, Rinaldi, Peerenboom and Kelly use a conceptual framework with six dimensions: (*a*) the infrastructure characteristics (organizational, operational, temporal, spatial); (*b*) the type of interdependency (physical, network-based, logical and geographical); (*c*) the environment (political/social, technical, legal, economic); (*d*) the characteristics of the dynamic feedback; (*e*) the type of disruption; and (*f*) the state of operation.[31]

Owing to the fact that there is effectively no limit to vulnerabilities, risk analyses are by definition never complete or exact. Even Yacov Haimes, of the US Society for Risk Analysis, points out in his textbook on risk analysis: 'To the extent that risk assessment is precise, it is not real. To the extent that risk assessment is real, it is not precise'. According to Haimes, this applies in particular to the risk of extreme and catastrophic events, which should not be assessed in the same way as high-probability, low-consequence events.[32]

In the field of counter-terrorism, a fundamental asymmetry can be discerned between terrorists' apparent ability to strike anywhere and at any time, and the inability of security forces to protect every imaginable target.[33] However, this situation does not mean that it is impossible to prioritize infrastructures in relation to the terrorist threat, but it requires a national and international comprehensive risk analysis and management dialogue.[34]

Effective protection for critical infrastructures 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. This makes

[30] British Cabinet Office, Strategy Unit, *Risk: Improving Government's Capability to Handle Risk and Uncertainty*, Strategy Unit Report, Nov. 2002, p. 29, URL <http://www.number-10.gov.uk/SU/RISK/REPORT/01.HTM>

[31] Rinaldi, S. M., Peerenboom, J. P. and Kelly, T. K., 'Identifying, understanding, and analyzing critical infrastructure interdependencies', *IEEE Control Systems Magazine*, Dec. 2001, pp. 11–25.

[32] Haimes, Y. Y., *Risk Modeling, Assessment, and Management* (Wiley-Interscience: New York, 1998), p. 45. On the Society for Risk Analysis see URL <http://www.sra.org/>.

[33] Hoffmann (note 26), p. 76.

[34] E.g., the Comprehensive Risk Analysis and Management Network (CRN), run by the Center for Security Studies of the Swiss Federal Institute of Technology, in cooperation with several international partner institutions. URL <http://www.isn.ethz.ch/crn>. See also Braun, H., 'The non-military threat spectrum', *SIPRI Yearbook 2003: Armaments, Disarmament and International Security* (Oxford University Press: Oxford, 2003), pp. 33–43, which describes the Comprehensive Risk Analysis Switzerland project.

partnerships essential. Close public–private sector partnerships are frequently encouraged at present, and rightly so, because they are an important prerequisite for such a strategy. Less often discussed, either in practice or in specialist literature, is the need for partnerships between the social and natural sciences. Based on the understanding that absolute security does not exist, lessons must be learned from unfamiliar fields of knowledge, and also from the past. If the study of history is to present options instead of ruling them out, it must be remembered that many of the consequences associated with specific events seem plausible today only because those events actually occurred. Decades before September 2001, Kahn and Wiener held that future events need not always be taken from the restricted list of what is possible, and that we must be prepared for further surprises.[35] Bearing this in mind, there are lessons to learn just as much from the future as from the past in the current fight against terrorism—the key notion being the 'scenario technique'. This approach calls for institutional and individual creativity, bearing in mind that creativity, as opposed to knowledge, has no limits.

Specifically, we must ensure that infrastructure analyses are no longer carried out without an understanding of the motive, the potential and the modus operandi of politically motivated actors.

Recent US Congress policy papers also conclude that analyses of threats, vulnerability and criticality should not be performed separately, but should complement one another as part of a comprehensive risk management approach.[36] This necessitates a modification to the analytical approach, which must assess different aspects not so much on the basis of their measurability as of their relevance to decision making, whether they are of a quantitative or a qualitative nature. There are many such analyses, but very few comprehensive studies on a strategic level. This point is also made by Gebhard Geiger: namely, that the research and development task for international security, and ultimately for security policy, is not to create a new applied research discipline, but to apply existing approaches, models and methods in an appropriate manner to the problems of social infrastructure protection.[37]

[35] Kahn, H. and Wiener, A. J., *Ihr werdet es erleben: Voraussagen der Wissenschaft bis zum Jahre 2000* [You will live to see it: predictions on science up to the year 2000], (Oldenburg: Vienna, Munich and Zurich, 1967), p. 254.

[36] See, e.g., 'A good risk management approach includes three primary elements: a threat assessment, a vulnerability assessment, and a criticality assessment.' US General Accounting Office (note 18), p. 1.

[37] Geiger, G., *Information und Infrastruktursicherheit: Grundzüge eines sicherheits- und technologiepolitischen Forschungs- und Entwicklungsprogramms* [Information and infrastructure security: outline for a security and technology policy research and development programme], (Stiftung Wissenschaft und Politik, Forschungsinstitut für Internationale Politik und Sicherheit: Ebenhausen, May 2000), p. 33.