The socio-political dimensions of critical information infrastructure protection (CIIP)

Myriam Dunn

Center for Security Studies,
ETH Zürich (Swiss Federal Institute of Technology),
ETH Center, SEI, Seilergraben 49-53, 8092 Zürich
E-mail: dunn@sipo.gess.ethz.ch
Websites: www.fsk.ethz.ch www.isn.ethz.ch/crn

Abstract: At present, the topic of critical information infrastructure protection (CIIP) is mainly discussed in the domain of engineers, consultants, and IT security experts. All these communities address important aspects of the problem complex, but hardly ever deal with socio-political ones. This paper addresses the need for a greater role of the social sciences in the field, due to a range of important socio-political issues that have newly emerged. From a comparison of protection policies compiled in the recently published CIIP Handbook, it distills theoretical key issues and major challenges for the CIIP community with socio-political dimensions. In the process, it particularly targets the extensive problem of 'conceptual sloppiness' that the community is culpable of. This conceptual negligence often leads to analytical negligence – with negative consequences for approaches to the issue in general and for the design of protection measures in particular.

Keywords: critical (information) infrastructure protection; comparative policy studies; interdisciplinary research; future challenges; socio-political issues; homeland security.

Reference to this paper should be made as follows: Dunn, M. (xxxx) 'The socio-political dimensions of critical information infrastructure protection (CIIP)', *Int. J. Critical Infrastructures*, Vol. x, No. x, pp.xxx–xxx.

Biographical notes: Myriam Dunn is a researcher at the Center for Security Studies. She is part of the Center's Comprehensive Risk Analysis and Management Network (CRN) team and specialises on the impact of the information revolution on security policy issues in general, and on critical information infrastructure protection (CIIP) in specific. Together with her colleague Isabelle Wigert, she is the author of the *International CIIP Handbook*, a compilation of protection policies in a range of countries. Currently, she is writing a study on the impact of threat perception of key actors on national CIIP policies. Dunn holds a degree in Political Science, History, and International Law from the University of Zurich.

1 Introduction

Key sectors of modern society, including those vital to national security and to the essential functioning of industrialised economies, rely on a spectrum of highly interdependent national and international software-based control systems for their smooth, reliable, and continuous operation. This *critical information infrastructure* (CII) underpins many elements of the *critical infrastructure* (CI), as many information and communication technologies (ICT) have become all-embracing, connect other infrastructure systems, and make them interrelated and interdependent.

Not only are information systems exposed to failures, they are also potentially attractive targets for malicious attacks. The CI delivers a range of services that individuals, and society as a whole, depend on. Any damage to or interruption of the CI causes ripples across the technical and the societal systems – a principle that has held true in the past, and even more so today due to much greater interdependencies. Attacking infrastructure, therefore, has a 'force multiplier' effect, allowing even a relatively small attack to achieve a much greater impact. For this reason, CI structures and networks have historically proven to be appealing targets for a whole array of actors (OCIPEP, 2003).

Driven by a growing concern for the potential vulnerability of networked societies together with an increasing number of disruptions in the cyber-domain, many countries have taken steps to better understand the vulnerabilities of and threats to their (information) infrastructure, and have proposed measures for the protection of these assets (*critical infrastructure protection* (CIP)/*critical information infrastructure protection* (CIIP)). For fourteen countries, such protection policies have been compiled in a recent publication, constituting a substantive collection of material that can be used as a starting point for more in-depth research[1] (Dunn and Wigert, 2004). Despite their substantial differences, these governmental protection policies offer a wealth of empirical material from which a variety of lessons can be distilled for the benefit of the CIP community.

Rather than attempting an empirical analysis, this paper is essayistic and descriptive in nature. Its main aim is to point out pervasive key issues and major future challenges for the CIIP community. Such challenges include a range of practical as well as more theoretical issues and exist in such large quantities that we clearly need to filter them systematically for the benefit of this paper. Without passing judgement on the importance of said challenges, we want to focus on the more theoretical issues, even though the nature of the subject is such that it is very difficult to draw a clear line between the two sets, as there is no practical issue without a theoretical perspective and vice versa.

In the following, we focus on those issues and challenges that demand an integration of a variety of disciplines – and especially the integration of the social sciences. The relevance of this is obvious: The question of CIIP has received little attention from large parts of academia up to now. At present, CIIP is in the capable hands of engineers, consultants, practitioners, and IT security experts. All these communities address important aspects, but often miss crucial key features of the complex systems at hand – namely their socio-political dimensions. This has become especially important in the current homeland security and terrorism debate, in which CIP/CIIP are key issues. In bringing the social sciences' perspective into the debate, we hope to spur a much needed dialogue between the different disciplines and provoke a discussion of a set of issues that have not gotten much attention even though they are of central importance.

Below, we address five separate points. In the first section, we ask ourselves whether a meaningful comparison of policies of such vast differences is at all possible and also address one major reason for these differences: that of conflicting perspectives key actors have of the problem. In the second section, we address the need for a distinction between the CI and the CII, because the future challenges mainly lie with the *emerging* CII. The third one is mainly concerned with the extensive problem we want to call 'conceptual sloppiness', a negligence that also results in analytical negligence. The fourth is also concerned with a conceptual difficulty: that the question of what to include in lists of critical assets, and why. The fifth and final section addresses current approaches to assessing various aspects of the CII, and points out the inadequacies of this methodological toolbox.

2 CIIP policies: comparing apples and oranges?

The USA, due to, among other factors, its leading role as an IT nation, was the first state to address the problem of CIP in earnest. The former US President Bill Clinton started developing a national protection strategy with his Presidential Commission on Critical Infrastructure Protection (PCCIP) in 1996, and the issue has retained high priority ever since (PCCIP, 1997; US Department of Homeland Security on CIP, 2004). The work of the PCCIP gave a boost to most other national protection efforts and even acted as a trigger in some cases. This resulted in the establishment of interdepartmental committees, task forces, and working groups, whose efforts resulted in policy statements and reports laying down basic policy elements of CIIP. These policies entail a variety of factors such as definitions of 'critical' elements, organisational issues, guiding principles, legislative factors, etc.

A study of the *International CIIP Handbook* reveals that these governmental CIIP policies are at various stages of implementation – some are enforced, while others are just a set of suggestions – and come in various shapes and forms, ranging from a regulatory policy focus concerned with the smooth and routine operation of infrastructures and questions such as privacy or standards, to the inclusion of CIIP into more general counter-terrorism efforts (Dunn and Wigert, 2004).

The differences in the state and quality of the protection practices in the 14 countries are in fact so substantial that we must reasonably ask ourselves whether we do not run the risk of comparing apples and oranges when trying to learn something from them. Additionally, the constant and rapid advancement of existing policies gives the impression of 'unfinished business', and many countries are still struggling to define their own 'CIIP identity'. What we are looking at are, therefore, mere snapshots of a very dynamic policy field with fuzzy boundaries.

One major reason why a comparison of protection policies is so difficult is that CIIP has become an issue of high relevance to many different, very diverse, and often overlapping communities. These different groups, be they private, public, or a mixture of both, usually do not agree on the nature of the problem or on what needs to be protected. Depending on their influence or on the resources at hand, various key players shape the issue in accordance with their view of the problem.

Within governments, turf battles are just as frequent. Only in a few countries have central governmental organisations been created to deal specifically with CIIP issues. Mostly, responsibility lies with multiple authorities and organisations in different

governmental departments. Very often, responsibility for the issue is given to well-established organisations or agencies that appear suitable for the task (Dunn and Wigert, 2004). Depending on their key assignment, these agencies bring their own perspective to bear on the problem and shape the policy accordingly. Among the fourteen studied countries, we can roughly distinguish between three resultant protection typologies:

- *CIIP is an issue of national security*. The entire society and its core values are perceived as endangered due to their dependence on ICT. Action against the threat is taken at a variety of levels (e.g., at the technical, legislative, organisational, or international levels). The main actors come from the security establishment.
- *CIIP is an issue of economics*. CIIP is seen as an issue of 'business continuity', especially in the context of e-business, which requires permanent access to IT infrastructures and permanently available business processes to ensure satisfactory business performance. The main actors are representatives of the private sector.
- *CIIP is an issue of law enforcement*. CIIP is seen as an issue of protecting society against (cyber-) crime. Cybercrime is a very broad concept that has various meanings, ranging from technology-enabled crimes to crimes committed against individual computers. The main actors are part of the law enforcement establishment.

While all typologies can be found in all countries, the emphasis given to one or more of them varies to a considerable degree. The dominance of one or several typologies has vital logical implications for the shape of the protection policies and, subsequently, in determining appropriate protection efforts, goals, strategies, and instruments for problem solution.

Having said all this, we are still stuck with the question of how sensible it is to compare policies that are so vastly different. Not only are we looking at a policy field that is only emerging, we can also be certain that the diversity as described above is here to stay. The shape of any policy field is largely dependent on factors such as institutional settings, actor constellations, and the nature of the policy design process itself, mainly in terms of the actors' choice of the arena to be engaged, and the behaviour and interaction of actors within that arena (Bleiklie et al., 2003). If any of these variables change, or an external event influences the perception of the key actors in a substantial way, a change in the direction and shape of the policy is also very likely.

This means that we have to be very careful when comparing policies, so as not to over-interpret the collected information. Rather than comparing details, we should aim to compare a more holistic picture and conceptualisation of the entire CIIP system. In this paper, we address questions that are mainly of conceptual nature – and conceptual shortcomings are in fact one common denominator in all countries. 'Conceptual sloppiness' is also the focus of the subsequent sections.

3 Achieve a focus on the emerging CII

The first conceptual difficulty is that of distinguishing between CIP and CIIP. 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, or even whether this is at all desirable, since we mainly find the term CIP in use in official publications, even if the

document is actually referring to something closer to CIIP. Also, definitions of CI and CIP can be found in abundance, while CII and CIIP are hardly ever defined, neither on the policy level nor in academia.

That the two concepts are closely interrelated is apparent from the current debate on protection necessities: The debate jumps from a discussion of 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 (Porteous, 1999). 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 dimension 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 largely 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 their invaluable and growing role in the economic sector, their interlinking position between various infrastructure sectors, and their essential role for the functioning of other infrastructures at all times (Wenger et al., 2002).
- On the threat side, cyber-threats are evolving rapidly both in terms of their nature and of their capability to cause harm, so that protective measures require continual technological improvements and new approaches, which means constant attention on the CII.
- The system characteristics of the emerging information infrastructure differ radically from traditional structures in terms of scale, connectivity, and dependencies (Parsons, 2001). 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. And since pressure to reduce time-to-market is intense, a further explosion of computer and network vulnerabilities is to be expected (Näf, 2001). We are therefore faced with the potential emergence of infrastructures with in-built instability, critical points of failure, and extensive interdependencies.
    - *Technological evolution*. On the other hand, we are facing an ongoing dynamic globalisation of information services, which in connection with technological innovation (e.g., localised wireless communication) will result in a dramatic increase of connectivity and lead to ill-understood behaviour of systems, as well as barely understood vulnerabilities.

This 'prospective' view clearly indicates a need to distinguish conceptually between the two concepts of CIP and CIIP, without treating them as completely separate concepts, especially in view of the fact that one of the major difficulties with current protection

practices is that they are aimed at the present status of existing CII – and thus always lag at least one step behind.

4 Towards conceptual and analytical clarity

The careless use of terms as shown in Section 3 points to deficiencies in understanding important conceptual differences between the models and is a direct consequence of substantial flaws in the existing terminology. The components of the term 'CIP' 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' (Metzger, 2004), or are borrowed, as in the case of 'infrastructure', from man-made technical infrastructures, such as railways, roads, or airports (Moteff et al., 2002), to name far more elusive complex, interdependent, open systems.

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. The design of adequate and cost-effective protection measures naturally demands an understanding of what it is that needs to be protected. Most 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 (Metzger, 2004).

But even though the need for conceptual sharpness 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, narrowband, 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 (Dunn and Wigert, 2004).

In addition, a preoccupation with technologies risks disregarding one rather central element of the information infrastructure – people. They 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 cognisant 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' (Lewis, 2002) – meaning that an element that is part of the information infrastructure can also be its greatest danger.

A different question concerns the identification of parts of the national or global information infrastructure as 'critical'. The following is a definition expressing the fact that the CII is an essential part of the CI and mainly responsible for the interdependencies, and it leaves room for the integration of the human factor: The CII is that part of the global or national information infrastructure that is essentially necessary for the continuity of a country's critical infrastructure services. However, such a

definition does not necessarily simplify the difficult question for practitioners of what to actually include in lists of critical entities.

5 The socio-political dimension of 'criticality'

One of the key questions in CIP/CIIP is what to include in a list of 'critical' assets for what reasons, and many countries have developed expert-based procedures to create these lists (Dunn and Wigert, 2004). In their attempt to define a number of so-called 'sectors' as critical, most countries follow the example of the PCCIP, which was the first official body to equate critical infrastructures with business sectors or industries. The definition of what constitutes a critical sector is an ongoing process. Not only can we observe that the list of critical sectors initially released by the PCCIP is constantly being tailored to meet country-specific needs, peculiarities, traditions, and concepts of criticality, but we can also observe that the definition of criticality is continuing to change, for example due to events such as 9/11 or general changes in the conceptualisation of CIIP.

The choice of business sectors as units for lists of critical assets is a pragmatic approach that mirrors the fact that the majority of infrastructures is owned and operated by private actors. However, the focus on sectors is far too artificial to represent the realities of complex infrastructure systems. Again, we find ourselves in the 'tangled web of an inadequate vocabulary', with implications for protection policies and analysis. The impression of literally 'sectorised' and closed entities makes some experts blind to the fact that reality is far more complex – and that interdependencies between sector functions are what really needs to be addressed.

Sector or industry roundtables might well further an understanding of how individual sectors work, especially when they are used to highlighting such aspects as the economic environment, underlying processes, stakeholders, or resources needed for crucial functions, as is done, for example, in the Netherlands, or in a less developed form, in Switzerland (Quick-Scan, 2003; InfoSurance, 2002). Yet, for a more meaningful analysis, it is absolutely necessary to move beyond the conventional 'sector'-based focus and to look at interdependencies between processes, functions, and services provided.

One would think that criticality, due to its importance in the CIIP debate, is a well-defined concept – but it is not. This is partly due to the fact that the classification of what is 'critical' lies in the eye of the beholder, and partly due to the constant change that the concept of criticality is undergoing. A survey of CIP documents and of the many definitions and lists of critical infrastructures reveals a great variety of conceptions (Dunn and Wigert, 2004). The main reason is that criteria for determining which infrastructures qualify as critical have expanded over time; the PCCIP, for example, defined as critical such assets whose prolonged disruptions could cause significant military and economic dislocation (PCCIP, 1997). Today, critical infrastructures in the USA and Canada also include national monuments (e.g., the Washington Monument), where an attack might cause a large loss of life or adversely affect the nation's morale (Metzger, 2004; Moteff et al., 2002).

With only a few exceptions, criticality is not understood as a socio-political issue, even though it is *predominantly* one. The level of damage impact that is acceptable to society is more of a political question than a system-technical one: The crucial question is how damage or the disruption of an infrastructure would be perceived and exploited politically. It is also to be expected that actual loss, be it monetary loss or the loss of

lives, would be compounded by political damage or by the loss of basic public trust in the mechanisms of government and the erosion of confidence in inherent government stability (Westrin, 2001).

From this perspective, the criticality of an infrastructure or service 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 (Metzger, 2004).

6 The inadequacy of current assessment tools

In general, an assessment of approaches for analysing various aspects of the CII is very enlightening. In effect, the methodological toolbox can serve as an indicator of the current understanding of key CIIP issues. Again, the huge variation in the granularity of methods and models used to analyse and evaluate aspects of the CII in the surveyed countries makes a meaningful comparison rather difficult. In addition, the majority of methods and models are designed and used for the larger concept of CI, and not for the CII in particular. This is 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.

Comparison is also unfeasible because these approaches exist for all 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. Examples of such patchwork applications include sector analysis; interdependency analysis; risk analysis; threat assessment; vulnerability assessment; or impact assessment. Exceptions are mathematical models and simulation tools to model various aspects of the larger CII – mostly, their interdependent behaviour (Dunn and Wigert, 2004). However, existing efforts are not yet sufficient for satisfactory models of cause-and-effect relationships and the impact of cascading failures in complex networks.

Generally speaking, current methodologies for analysing CII are insufficient in a number of ways: One of the major shortcomings is that the majority of them do not pass the ‘interdependency test’. In other words, they fail to address, let alone understand, the issue of 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 (Schmitz, 2003). The methodological toolbox at hand is filled with old tools – often with a fixation on that which is quantifiable – often hurriedly adapted to a new set of problems. If this toolbox is to serve as an indicator of the level of comprehension, then comprehension of the CIIP problem is very low.

The majority of approaches originate in risk analysis. This is most likely due to the knowledge and experience that already exists in this field and has been applied by the engineering sciences to system analysis for decades. 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. Furthermore, one of the main difficulties facing risk analysis involves the theoretical and practical difficulties of estimating the probabilities and consequences of low-probability high-impact events – since no useful statistics for possible damage and failure

probabilities exist (Reinermann and Joachim, 2003). It also appears that there is no way of cataloguing objects, vulnerabilities, and threats on a strategic policy level, such as the economy at large, in a meaningful way. Additionally, risk analysis clearly does not pass the 'interdependency test'.

Further, there is a danger that risk analysis, especially because it is so well established and used in different communities, may become a 'false friend'. It is easy to deceive oneself through over-confidence: when looking at relatively limited systems, many factors are known, and sufficient data may be available. In the process, non-quantifiable factors are often forgotten. Also forgotten are a range of socio-political issues, even though 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 (Rinaldi et al., 2001). This points to one fundamental issue and major challenge in terms of research: Only interdisciplinary approaches pay sufficient tribute to an issue that is *inherently* interdisciplinary due to its multifaceted nature.

7 Conclusion

A Canadian once said about CIIP that it was

> "a Gordian knot around which many stakeholders circle, pulling on the strands that seem most promising and causing the entire thing to tighten even more snugly rather than loosen to reveal its internal structure." (Porteous, 1999)

Even though this quote dates back to 1999, it still rings true today. CIIP deeply puzzles a great many actors from a variety of communities and is far from revealing its inner secrets.

In this paper, we have pointed out a variety of theoretical challenges that become apparent from an evaluation of current protection policies. Tackling the right ones will help the CIIP community to loosen some of the knot's strands, so that we might be able to catch a glimpse of that elusive internal structure. The most tricky strands to unravel, but also the most rewarding if we should succeed, are those to do with what we call 'conceptual sloppiness', meaning a careless use of terms with repercussions for how the issue is approached, analysed, and ultimately how protection is planned.

The main problem with the term 'CIIP' is the same as with its twin concept, 'CIP': It originated in the technical context of limited or 'closed systems', and is now used in the totally different context of networks and systems whose boundaries are no longer clearly discernible. It is not static infrastructures as such that are the objects of protection, despite the terminology of critical *infrastructure* protection, but rather the *services* and their *role and function* for society. This is a far more abstract level of understanding essential assets that again demands new analytical tools and mindsets.

While single infrastructures can be illustrated relatively easily in terms of organisational and institutional hierarchies, it is true that services, flows, and values are a lot more complex, harder to capture, and far more difficult to understand. When we add socio-political and cognitive dimensions to the equation, it becomes clear that we are dealing with a 'new' problem that requires new analytical techniques and methodologies.

In fact, many challenges and problems are only just arising with the emerging CII, as the system characteristics of future information infrastructures will differ fundamentally from traditional structures. As of today, CIIP efforts face one major problem: Protection is aimed at the present status of existing CII – and thus always lags at least one step behind. Again, understanding these new realities will require new analytical techniques and methodologies that are not yet available. Their development will, in turn, require great efforts in unconventional and proactive thinking.

The need for more research into methodologies for the analysis of CII and CIIP is acknowledged. As there is no sword at hand that can undo the knot at a stroke, a careful identification of the key structure, or in effect the key puzzles, is necessary. Solving them requires an integrated set of methods and tools for analysis, assessment, protective measures, and decision making. In fact, 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, and will thus require a comprehensive and truly interdisciplinary R&D agenda encompassing fields ranging from engineering and complexity sciences to policy research, political science, and sociology. Equipped with such an extensive toolbox, the many stakeholders will no longer have to pull on the strands that seem most promising, but will be able to systematically undo those strands that have hitherto kept the knot from revealing its internal structure.

References

Bleiklie, I., Malcolm, G. and Christine, R. (Eds.) (2003) *Comparative Biomedical Policy: A Cross-Country Comparison*, Routledge.

Dunn, M. and Wigert, I. (2004) *The International CIIP Handbook 2004: An Inventory and Analysis of Protection Policies in Fourteen Countries*, Center for Security Studies.

InfoSurance (2002) 'Wirtschaftliche Landesversorgung, Informatikstrategieorgan Bund', *Sektorspezifische Risikoanalysen: Methodischer Leitfaden*.

Lewis, J.A. (2002) *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats*, Center for Strategic and International Studies, available at http://www.csis.org/tech/0211_lewis.pdf.

Metzger, J. (2004) 'The concept of critical infrastructure protection (CIP)', in Bailes, A.J.K. and Frommelt, I. (Eds.): *Business and Security: Public-Private Sector Relationships in a New Security Environment*, Oxford, pp.197–209.

Moteff, J., Claudia, C. and Fischer, J. (2002) *Critical Infrastructures: What Makes an Infrastructure Critical?*, CRS (Congressional Research Service) Report for Congress RL31556.

Näf, M. (2001) 'Ubiquitous insecurity? How to 'hack' IT Systems', in Wenger, A. (Ed.): *The Internet and the Changing Face of International Relations and Security, Information and Security: An International Journal*, Vol. 7, pp.104–118.

Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP) (2003) *Threat Analysis*, No. TA03-001, available at: http://www.ocipep-bpiepc.gc.ca/opsprods/other/TA03-001_e.pdf.

Parsons, T.J. (2001) 'Protecting critical information infrastructures. The coordination and development of cross-sectoral research in the UK', *Plenary Address at the Future of European Crisis Management*, Uppsala, Sweden.

Porteous, H. (1999) 'Some thoughts on critical information infrastructure protection', *Canadian IO Bulletin*, October, Vol. 2, No. 4, available at: http://www.ewa-canada.com/Papers/IOV2N4.htm.

President's Commission on Critical Infrastructure Protection (PCCIP) (1997) *Critical Foundations: Protecting America's Infrastructures*, Washington DC.

Quick-Scan (2003) 'Ministerie van Binnenlandse Zaken en Koninkrijksrelaties', *Critical Infrastructure Protection in the Netherlands: Quick Scan on Critical Product and Services*.

Reinermann, D. and Joachim, W. (2003) 'Analysis of critical infrastructures: The ACIS methodology (Analysis of critical infrastructural sectors)', *Proceedings of the Critical Infrastructure Protection (CIP) Workshop*, Frankfurt, A.M., 29–30 September.

Rinaldi, S.M., Peerenboom, J.P. and Kelly, T.K. (2001) 'Complex networks. identifying, understanding, and analyzing critical infrastructure interdependencies', *IEEE Control Systems Magazine*, December, Vol. 21, No. 6, pp.11–25.

Schmitz, W. (2003) *ACIP D6.4 Comprehensive Roadmap – Analysis and Assessment for CIP – Work Package 6, Deliverable D6.4, Version 1*, European Commission Information Society Technology Programme.

US Department of Homeland Security on CIP (2004) Available at: http://www.dhs.gov/dhspublic/display?theme=31.

Wenger, A., Metzger, J. and Dunn, M. (2002) 'Critical information infrastructure protection: eine sicherheitspolitische herausforderung', in Spillmann, K.R. and Wenger, A. (Eds.): *Bulletin zur Schweizerischen Sicherheitspolitik*, pp.119–142.

Westrin, P. (2001) 'Critical information infrastructure protection', in Wenger, A. (Ed.): *The Internet and the Changing Face of International Relations and Security*, *Information & Security: An International Journal*, Vol. 7, pp.67–79.

Note

[1]The following countries are included in the 2004 edition: Australia, Austria, Canada, Finland, France, Germany, Italy, Netherlands, New Zealand, Norway, Sweden, Switzerland, United Kingdom, and the United States (Dunn and Wigert, 2004).