Towards a Global Culture of Cyber-Security

By Myriam Dunn and Victor Mauer

The information infrastructure – the combination of computer and communications systems that serve as the underlying infrastructure for organizations, industries, and the economy – has become a key asset in today's security environment.[1] All critical infrastructures are increasingly dependent on the information infrastructure for a variety of information management, communications, and control functions. This dependence has a strong national security component, since information infrastructure enables both economic vitality and military and civilian government operations. In particular, the government and military information infrastructures depend on commercial telecommunications providers for everything from logistics and transport to various other functions.[2] Current trends, such as the opening and liberalization of the markets, globalization processes that stimulate the cross-national interconnection of infrastructures, and the widespread access to telecommunications networks, are heightening the security requirements of the infrastructures in countries across the globe.

In addition, there are a number of observations that indicate the danger arising from society's dependence on complex, vulnerable, and critical systems:

- Many of the networks and systems have been built piecemeal by many different people and organizations using a wide assortment of information technologies, and with a wide range of functionalities in mind. Very few have been designed or implemented with assurance or security as primary considerations.[3]
- On the technical level, security will hardly evolve naturally or by the forces of the free market alone, because there are substantial obstacles

[1] Computer Science and Telecommunications Board, National Research Council,. Trust in Cyberspace (Washington, D.C.: National Academy Press, 1999).

[2] Personick, Stewart D. and Cynthia A. Patterson (eds.). Critical Information Infrastructure Protection and the Law: An Overview of Key Issues (Washington, D.C.: National Academies Press, 2003), p. 1.

[3] Goodman, Seymour. E. "The Protection and Defense of Critical Information Infrastructures". Paper presented at the 43rd Annual IISS Conference, "The Strategic Implications of the New Economy" (Geneva, 12–15 September 2001), pp. 3–4.

to IT security: there is no direct return on investment, time-to-market impedes extensive security measures, and security mechanisms often have a negative impact on usability.[4]

- There is a historic lesson to be learned: It is a recurring phenomenon that the conveniences of a new technology are embraced long before its unwanted side-effects are systematically dealt with. The resulting "convenience overshoot" may last for decades.[5] Today, this approach might just be a trifle too dangerous: Too much depends on smooth, reliable, and continuous operation of the CII.
- Historically, many critical national infrastructures have been physically separate systems with little interdependence. Today, however, due to the CII, physical large-scale infrastructures are highly interconnected. But so far, attempts to understand the inter- and intra-connectedness among the various subsystems are completely lacking.
- Credibility, trust, and confidence are key assets in our volatile world.[6] One of the unforeseeable consequences of disruptions in the information infrastructure is likely to manifest itself in indirect and non-quantifiable ways: the destabilization of basic trust among citizens in the mechanisms that govern them.[7]
- In his book on "Normal Accidents", Charles Perrow argues that in an interactively complex system, two or more discrete failures can interact in unexpected ways, thereby affecting supposedly redundant sub-systems. A sufficiently complex system can in fact be expected to have many such unanticipated failure mode interactions, making it vulnerable to inevitable accidents, even without external triggers.[8]

[4] 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, Volume 7, (2001), pp. 104–18.

[5] Examples are: The introduction of the Ford Model T in 1909 and the widespread use of seat belts; the 70-year delay between the introduction of steam locomotives and the first use of pneumatic brakes.

[6] Dunn, Myriam. Information Age Conflicts: A Study on the Information Revolution and a Changing Operating Environment. Zürcher Beiträge zur Sicherheitspolitik und Konfliktforschung, No. 64 (Zurich: Center for Security Studies, 2002), pp. 33–41.

[7] 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. 74–75.

[8] Perrow, Charles. Normal Accidents: Living with High-Risk Technologies (New York: Basic Books, 1984).

- Even as our knowledge and competence as regards system reliability increases, new demands of functionality will likewise increase, and thereby system complexity. An inevitable "ingenuity gap" arises.[9]

Seen from this viewpoint, a robust ICT-dependent society requires active intervention, at a stage when a major, society-threatening chain reaction of IT-related events is still only fiction. Active intervention in this case means taking adequate measures to make those systems, and thus society, more secure, which can only be done based on a better and more thorough understanding of the problems we face.

The Challenge of Interdisciplinary Research

At present, however, open, pressing, but unanswered questions abound in the field of CIIP. As a result, there is not just a research gap — there is a veritable Grand Canyon of lacking knowledge to be filled; and the research community is only just beginning to single out the correct and the most important questions that need to be asked. The research field is also highly dynamic, mainly due to the rapid changes in the technological environment. In such a dynamic field, we need to pinpoint the underlying urgent questions that are not subject to erratic change. Also, the question of generalizing and establishing over time the results of studies involving information infrastructure protection is in itself a fundamental issue: Does the topic of CIIP have a classifiable structure and content that is sufficiently stable in time to provide a foundation for durable protection and preparedness planning?[10] At present, it would appear that the answer to this question is "no". In fact, it seems as if the problem complex itself were in flux to a degree that calls for constant observation until this area of research has gained a more stable scientific and methodological base. Academia and practitioners will have to work hand in hand to resolve that problem.

In addressing the topic of critical infrastructures and their protection, one has to understand and assess the relevance of various factors. Issues that demand special attention have become apparent through in-depth analysis

[9] An ingenuity gap is a shortfall between rapidly rising need of complex societies for initiative and innovation and the inadequate supply of it. See: Homer-Dixon, Thomas. The Ingenuity Gap (New York: Knopf, 2000), p. 1.

[10] Westrin, op. cit., p. 77.

of the subject matter and cross-country comparison of protection practices. The trickiest of these issues are those that demand an integration of various disciplines. These include a number of policy issues, which are addressed in this volume, but also diverse issues such as inter-linkages between CI, the working of complex systems, consequences of interdependencies, possible cascading effects of failures, and newly emerging, insufficiently understood threats and vulnerabilities.

There is no question that technology is one of a number of mediating factors in human behavior and social change, which both affects and is affected by other phenomena. However, one must be very careful not to succumb to technological determinism. The technological determinist view is a technology-led theory of social change: technology is seen as the prime mover in history. Technology, however, is not an abstract, exogenous variable, but rather inherently endogenous to politics.[11] This embeddedness means that ICTs and people can only be fully examined through an overarching theoretical perspective that encompasses an understanding of the social, economic, political, and technical dimensions inherent in it. Therefore, only frameworks that combine socio-economic, socio-political, and socio-technical knowledge can give satisfactory answers to many of the issues at hand, because they alone offer insights into how individual practices are linked to wider socio-political regimes and socio-technical landscapes that evolve in particular cultural and geographical contexts.

However, the interdisciplinarity that this implies is not easily realized. Conceptual frameworks to analyze how digitalization, infrastructures, and various other aspects of CIIP shape a diversity of social processes, and vice versa, are not readily available. In general, research that cuts across disciplines meets with considerable obstacles. Much of the difficulty of interdisciplinarity has to do with the fact that attention, recognition, and authority are channeled by academic institutions of the individual disciplines.[12] A discipline is a scientific domain that has a specific methodology, specific implicit hypotheses justify-

[11] Chandler, Daniel. “Technological or Media Determinism”. Online resource, created on 18 September 1995. http://www.aber.ac.uk/media/Documents/tecdet/tdet02.html; Herrera, Geoffrey. “Technology and International Systems”. In: Millennium, Vol. 32, No. 3, (2003), pp. 559–94; Mackenzie, Donald and J. Wajcman (eds.). The Social Shaping of Technology: How the Refrigerator Got its Hum (Buckingham: Open University Press, 1994, reprint).

[12] Sperber, Dan. “Why Rethink Interdisciplinarity?”. Online Seminar on Interdisciplinarity, Paper (no date)., a Available at http://www.interdisciplines.org/interdisciplinarity/papers/1/4.

ing it, and a specific vocabulary. Attempts to build interdisciplinary bridges logically lead to the "intersection/union" problem: in order for a result to be accepted by two disciplines, one has to reduce their implicit hypotheses to a set of common ones (intersection), and to extend the justifications to include a complete justification in both disciplines (union). Relaxing the implicit hypotheses, although increasing the generality of the result, will limit its "practical" consequences, and may result in too general a statement.[13]

These obstacles are hard to overcome. However, if we are aware of the need for interdisciplinarity, much might already have been won. In specific areas, disciplinary boundaries and routines stand in the way of optimal research. Openness to interdisciplinarity is thus the most sensible recommendation at this point.[14] The goal is to go ahead with new research programs, and, for this, to reshape the institutional landscape. More generally, it is conceivable that the advancement of science will involve so much reshaping of its institutional forms that the disciplines as we know them will have to go.

In this volume, we have offered an in-depth analysis of key issues in three parts, covered by authors from different disciplines so as to incorporate the viewpoints of an interdisciplinary group of scholars. Rather than wrapping up each of the chapters in this volume individually, we choose to tackle one of the most prominent overarching questions in this concluding chapter of Volume II: What role can and should the state play in protecting these infrastructure systems within their broader environment? More specifically with regard to the three parts of this volume, how can the state foster much-needed research? How can we overcome the problem posed by the differing viewpoints in CIIP? How can governments gain more knowledge on the threat environment? What role can they play in early warning and public outreach, in public-private-partnerships, and concerning legal issues?

[13] Mendez, Patrice Ossona de. "The Risks and Challenges of Interdisciplinarity". Online Seminar on Interdisciplinarity, online comment (2 April 2003)., a Available at http://www.interdisciplines.org/interdisciplinarity/papers/1/2#_2.

[14] Laudel, Grit. "Collaboration, Creativity and Rewards: Why and How Scientists Collaborate". In: International Journal of Technology Management, Vol. 22, (2001), pp. 762–81.

Finding the Right Role of the State in CIIP

The developments of the past decade have led many observers to assume that the forces driving global change are acutely undermining the state and its political freedom of action. What is clear already is that any conception of security capable of dealing with the current world order needs to be linked to a much wider notion of governance than that which characterized the Cold War. In the realm of CIIP, governments are challenged to operate in unfamiliar ways, sharing influence with experts in the IT community, with businesses, and with nonprofit organizations, because the ownership, operation, and supply of the critical systems are in the hands of a largely private industry. We are thus confronted with a case in which governments cannot carry out their most basic mission, providing security, without the cooperation of the private sector.

The fact that the maintenance of "business continuity" for an individual, corporate or local actor and security efforts in terms of national or even international security often exist side by side in the realm of CIIP and homeland security seems to be a long-term trend rather than an exception. This points to the changing nature of security practices in a world in which the state sees itself as being unable "to go it alone". In fact, the state practice of security is moved from the outside of the border into domestic space: Security is domesticated and privatized, while the private realm is securitized. On the one hand, the practice of securing society is privatized by putting the responsibility partially on the shoulders of the owners and operators of critical infrastructure. On the other hand, the goal or philosophy of the state is still the same, whereby national security practices spill into society.

This development also means that even though the issue of cyber-threat is clearly linked to national security, no measures are envisaged that would traditionally fall within the purview of the national security apparatus. In general, national-security countermeasures stress deterrence and prevention of attacks, while the investigation and pursuit of the attackers is only of secondary importance, since the concept of compensatory or punitive damage is rarely meaningful in a national-security context. Private-sector countermeasures, however, are frequently oriented toward detection, which means developing audit trails and other chains of evidence that can be used to pursue attackers in the courts.[15] This means that even if we consider CIIP to be a national-

[15] National Academy of Sciences, Computer Science and Telecommunications Board. Computers at Risk: Safe Computing in the Information Age (Washington D.C.: National Academy Press, 1991), p. 19.

security issue, the tools available to the state are not part of its traditional national security arsenal — on the contrary: In the majority of countries, the law-enforcement/cyber-crime perspective has emerged as the most prominent one, due to the nature of the threat, the resources available to the law enforcement community, and cultural and legal norms that restrict the number of available strategies.

Even more, because CIIP and economic growth are so closely interrelated, any involvement of the state in cyber-security matters is subject to much scrutiny. It has in fact been argued that one solution to the problem of cyber-security is to focus on economic and market aspects of the issue rather than on suitable technical protection mechanisms.[16] If we apply this viewpoint, we quickly realize that the insecurity of the internet can be compared to environmental pollution and that cyber-security in fact shows strong traits of a "public good" that will be underprovided or fail to be provided at all in the private market.

Cyber-Security – A Public Good?

In economics, a public good is a good that is hard or even impossible to produce for private profit, because the market fails to account for its large beneficial externalities. By definition, a public good possesses two properties[17]:

- **Non-rivalrous:** its benefits fail to exhibit consumption scarcity; once it has been produced, everyone can benefit from it without diminishing others' enjoyment.
- **Non-excludable:** once it has been created, it is very difficult, if not impossible, to prevent access to the good.

Public goods provide a very important example of market failure, in which individual behavior seeking to gain profit from the market does not produce efficient results. The production of public goods results in positive externalities,

[16] Andersson, Ross. "Why Information Security is Hard: An Economic Perspective". In: IEEE Computer Society (ed.). Proceedings of the 17th Annual Computer Security Applications Conference, New Orleans, 10–14 December 2001. http://www.ftp.cl.cam.ac.uk/ftp/users/rja14/econ.pdf.

[17] Stiglitz, Joseph E. and Carl E. Walsh. Principles of Microeconomics (New York, W. W. Norton & Company, 2004, 4th Edition), pp. 236–238; Wikipedia, The Free Encyclopedia. s. v. "Public Goods". Available at: : http://en.wikipedia.org/wiki/Public_goods.

which are not remunerated. In other words, because private organizations cannot reap all the benefits of a public good that they have produced, there will be insufficient incentives to produce it voluntarily. At the same time, consumers can take advantage of public goods without contributing sufficiently to their creation. This is called the free-rider problem, because consumers' contributions will be very small.[18]

Is cyber-security a public good? We can in fact observe that the security of the entire internet is affected by the security employed by all internet users[19]: Insecure nodes not only jeopardize the integrity of their own systems, but also compromise the security of all users, for instance by spreading worms unintentionally and by irresponsibly tolerating distributed attacks from their computers. On the other hand, when a firm or individual has a greater level of cyber-security, their computers are less likely to be hacked into and used to launch spam or other denial of services attacks. The security that the computer owner provides thus benefits other computer users by reducing the probability that they will be attacked through the first owner's computer. However, since individuals are not generally liable for the damage caused when a hacker takes over their computer, they do not benefit from the increased security. Since users do not therefore bear the full costs of their actions, individuals have no incentive to upgrade the security of their systems.[20]

This could, in theory, lead to the free-rider problem. There are in fact various levels on which free-riding could take place: first, individuals are likely to free-ride. Second, companies might also be free-riders, even though some researchers have pointed out that there is little empirical evidence for this in the financial sector, for example.[21] And third, nation states are also prone to free-ride. Because any externality created by unsecured computers is not limited by national boundaries, it is unlikely that any country could respond to such an externality on its own. Pursuing its own interest, each country, state, or region has insufficient incentive to safeguard the global information infrastructure. Cyber-security thus shows some important features of a public

[18] Ibid.

[19] Anderson, Why Information Security is Hard.

[20] Anderson, Ross. "Unsettling Parallels Between Security and the Environment". Economics and Information Security Workshop, Berkeley, 16–17 May 2002. Available at: http://www.sims.berkeley.edu/resources/affiliates/workshops/econsecurity/econws/37.txt.

[21] Powell, Benjamin. "Is Cyber-Security a Public Good? Evidence from the Financial Services Industry" The Independent Institute Working Paper, 14 March 2005., a Available at: http://www.independent.org/pdf/working_papers/57_cyber-.pdf.

good, even if it might not be a “pure” one. In addition, cyber-security is fast becoming a global public good.

Solutions, Policy Options, and Recommendations

In the economic literature, there are a number of possible solutions to the free rider problem. Some public choice theorists advocate government intervention and state provision of public goods by providing the difference between the optimal level of cyber-security and the level the private sector voluntarily provides. Also, if voluntary provision of public goods will not work, then the obvious solution is to make their provision mandatory.[22] One general solution to the problem is for governments or states to impose taxation to fund the provision of public goods. A government may also subsidize the production of a public good in the private sector.[23]

However, there is widespread agreement that governments should not get involved too much. Specifically, it is agreed that regulation may not produce optimal results due to various factors:

- Governments are inherently slow to respond or adapt to new situations.
- Governments usually place the emphasis on the tools they know best, in the shape of top-down regulation, which may not be the most effective approach.
- Government regulations are ineffective, since the technology changes too quickly: Often, governments lag behind the private sector in understanding the threats and the state of technology to address them.
- Governments tend to politicize issues rather than remain focused on the substance.
- Governments are always regulating in response to earlier developments and thus lagging behind.

[22] Grady, Mark and Francesco Parisi. “The Law and Economics of Cyber-security: An Introduction”. George Mason University School of Law and Economics Working Paper Series No 04-54, (November 2004).

[23] Wikipedia, The Free Encyclopedia, s. v. “Public Goods”., a Available at: http://en.wikipedia.org/wiki/Public_goods.

In addition, because public goods are not bought and sold on the market, it is impossible to determine the optimal level of cyber-security and then compare it to what the private market has provided. The information problem — figuring out how much provision is optimal — and the incentive problem — making it worth someone's while to provide exactly that amount — are thus unsolved issues in practice. Therefore, public goods will still tend to be produced at suboptimal levels even when the government provides them, though the error will often be in the other direction: In general, many argue the public goods such as national defense tend to be overproduced by governments.[24]

Indeed, there is a fair amount of hype surrounding the topic, in part fueled by government officials: "cyber-war" and related issues are en vogue and have even become a growth market. Producers of information security technology may benefit financially if they can scare more people into purchasing security products. Similarly, professionals competing for the latest homeland security grants may face incentives to overstate the problem. Especially when it comes to CIIP as a national security issue, so-called "professionals of security"[25] also play a considerable role. The institutions that father these professionals of security are bureaucratic ramifications of the state; deprived of their Cold War exterior enemy, these bureaucracies need to legitimize their existence by constantly redefining their role of society's protector and do so by adding new threats to the political agenda, when old ones disappear.[26]

In fact, to look at cyber-security as a mainly economic problem helps to "desecuritze" the issue. Desecuritization as the "unmaking of security" has been considered a technique for "defining down" threats, in other words, a "normalization" of threats previously constructed as extraordinary, as they are when looked upon as a national security issue.[27] This points to the fact that one must be careful not to foment "cyber-angst" to an unnecessary degree and to ensure that threats are seen in appropriate proportions by all involved could be one important role for the state.

[24] Goodman, John C. and Philip K. Porter. "Political Equilibrium and The Provision of Public Goods". In: Public Choice, Vol. 120, No. 3–4, (September 2004), pp. 247–266.

[25] Aradau, Claudia. "Migration: The Spiral of (In)Security". In: Rubikon, March 2001., a Available at: http://venus.ci.uw.edu.pl/~rubikon/forum/claudia1.htm.

[26] Ibid.; Huysmans, Jef. "Revisiting Copenhagen: Or, On the Creative Development of a Security Studies Agenda in Europe". In: European Journal of International Relations, Vol. 4, No. 4, (1998), pp. 479–506.

[27] Aradau, Claudia. "Beyond Good and Evil: Ethics and Securitization /Desecuritization Techniques". In: Rubikon, December 2001., a Available at: http://venus.ci.uw.edu.pl/~rubikon/forum/claudia2.htm.http://venus.ci.uw.edu.pl/~rubikon/forum/claudia2.htm.

There is another role for government, linked to a third solution to the free-rider problem that might, in combination with some state intervention where truly needed, produce promising results: The Coasian solution, named after the economist Ronald Coase.[28] The Coasian solution proposes a mechanism by which potential beneficiaries of a public good band together and pool their resources based on their willingness to pay to create the public good. For such solutions, governments can serve as the convener to bring parties to the table. They can compel — either through persuasion or regulation where necessary — the sort of behavior that many believe is needed. Moreover, governments can use purchasing criteria to create a market for products that conform to certain specifications, like security standards. All in all, this points to the fact that global economic development, steered into the right direction, may be the force that best addresses the problem. Below, we will look at how a market for security could be created, and how governments could promote best practices, information sharing, and additional research.

Create a Market for Security: The Role of Insurance

Some commentators have proposed using liability rules and cyber-insurance as solution to cyber-security and CIIP at least at the national level. In fact, economist Hal Varian identifies the situation of responsibility attribution as the main source of weak security.[29] He argues that, in a first step, liability for losses due to security breaches should be transferred to the party who could reduce the risk most easily. Accordingly, manufacturers would be liable for vulnerabilities in their products, but also network nodes – up to the end user — could be called to account if they do not comply with their maintenance duties. Ideally, civil liability allows a victim to recover losses from third parties if such parties were negligent or engaged in intentional misconduct and if such negligence or misconduct was the proximate cause of the loss. As a second step, cyber-risks should be made transferable, so that all parties can buy insurance coverage against possible losses and indemnification claims. The introduction of insurance might thus provide a foundation for market-based

[28] Coase, Ronald. "The Lighthouse in Economics". In: Journal of Law and Economics, Vol. 17, no. 2, (1974), pp. 357–376.

[29] Varian Hal R. "Managing Online Security Risks". In: New York Times, 1 June 2000., a Available at: http://www.sims.berkeley.edu/~hal/people/hal/NYTimes/2000-06-01.html.

risk analysis and cooperation among infrastructure operators, and can foster best practices.[30]

In this view, a mechanism for gauging the value of stolen information is of critical importance. If companies can assess the value of information, then insurance companies can insure information. In turn, the insurance companies will push companies to better protect their information. However, how to measure the value of information? In general, there is a very limited understanding of the costs of cyber-security attacks and the benefits of preventive measures, for a variety of reasons, not least the fact that it is highly unlikely that detailed access to more than a few such systems will be available to research directed towards this end. Systems for such services as finance and security exchange, or data communication in general, will most probably remain inaccessible for analysis. Governments could play a significant role in sponsoring research on this subject, research that, up to this point, the private sector has been unwilling or unable to conduct. It should also develop mechanisms for systematically collecting information from firms (with appropriate privacy protections) that would allow the government to help develop a better strategy for addressing cyber-security in the future.

Promote Best Practices

Apart from thinking about reforming IT liability to further the development of a cyber-security market, governments might want to promote operational best practices for network administrators and users, combined with ongoing training and enforcement of the practices through random tests, and consider developing standards for software protocols that are more secure than current ones. In addition to playing a role in liability determinations, best practices can also serve as a benchmark against which firms could be audited. Routine audits based on well-accepted principles of testing and analysis can help firms avoid litigation or reduce liability.[31] Such standards could be voluntary or enforced through regulations. At least, governments could serve as an "honest broker", developing and disseminating information that could be expensive

[30] Kesan, Jay P.Ruperto P. Majuca, and William J. Yurcik. "Cyber-Insurance as a Market-Based Solution to the Problem of Cyber-Security — A Case Study". 4th Workshop on the Economics of Information Security (WEIS), Harvard University, 2–3 June 2005, a. Available at: http://infosecon.net/workshop/pdf/42.pdf.

[31] Personick and Patterson, op. cit., p. 4.

for an individual locality to acquire, but crucial to the prospects of any joint operating agreement. Adopting a nationally or even internationally recognized computer security standard is not, however, a simple process, owing to the evolving nature of security vulnerabilities and the diverse players that have an internet presence.[32] The crucial point is, therefore, to establish "best practices" for industry and government that can be flexible for a variety of users but still provide a basis for liability.

Promote Information Sharing

In addition, governments have a strong role to play in raising awareness and educating all stakeholders about the importance of properly configured systems and available network protection tools as well as about the threat. However, although the sharing of information has been the centerpiece of both the governments' and the private sectors' efforts to protect critical information systems over the past several years, most information sharing still occurs through informal channels. These networks have been plagued by the traditional problems of any "Prisoner's Dilemma", in that members are afraid to cooperate and divulge information because of worries about increased liability due to disclosure, risk of antitrust violations, and the loss of proprietary information.[33]

As a first step, information sharing requires a permissible legal framework, for example regarding both antitrust and liability concerns.[34] In addition, recent research suggests that the membership of these networks should be restricted, making them less broadly based than they presently are. This would allow norms to be developed among actors who have preexisting business connections that would facilitate enforcement, as opposed to the broad networks that currently exist and cannot enforce disclosure.[35] In addition, government

[32] Berkowitz, Bruce and Robert W. Hahn. "Cyber-security: Who's Watching the Store?", Iin: Issues in Science and Technology (Spring 2003), a. Available at http://www.issues.org/19.3/berkowitz.htm.

[33] Cukier, Kenneth Neil, Viktor Mayer-Schoenberger and Lewis Branscomb. "Ensuring (and Insuring?) Critical Information Infrastructure Protection". KSG Working Paper No. RWP05-055 (October 2005).

[34] Personick and Patterson, op. cit., p. 2.; Benson, Bruce L. "The Spontaneous Evolution of Cyber-Law: Norms, Property Rights, Contracting, Dispute Resolution and Enforcement Without the State of Law". In: Journal of Law, Economics and Policy, Vol. 1, No. 2 (2005), a. Available at: http://www2.sjsu.edu/depts/economics/faculty/powell/docs/econ206/Cyber-Law-Evolution.pdf.

[35] Grady and Parisi, op. cit.

officials can provide intelligence information about new computer-security threats that might benefit companies involved in information sharing, as is the case for certain early-warning measures.

Promote Research

Finally, governments can fund long-term research into CIIP.[36] They need to spend money to get better information about the threats and about what the available countermeasures can actually achieve. Since the putative new societal risks and vulnerabilities are directly or indirectly related to the development and utilization of new technologies, it would seem natural to follow a chain of analysis beginning with technical specifications and casually running "up" through systems, actors, threats, vulnerabilities, consequences, and finally, countermeasures and mitigation. However, in view of the rapid technological developments constantly taking place, and the particular nature of their implementations, one can raise certain objections to such a synthetic scheme. If, for instance, one carefully examines a relatively localized subsystem from the point of view of risks and threats, thereby identifying certain of its vulnerabilities, in what way can these insights be generalized and established in order to utilize them "beyond" the subsystem itself, on a higher system level?[37]

It may very well be that critical vulnerabilities, and even the worst consequences of infrastructure disruptions, will not be traceable in any useful way to single technical subsystems — perhaps as a consequence of an already overwhelming system complexity of open socio-political systems. Also, in view of the rapid technological developments constantly taking place, and the particular nature of their implementation, even if one carefully examines a relatively localized subsystem from the point of view of risks and threats, thereby identifying certain of its vulnerabilities, these insights can hardly be generalized and established in order to utilize them "beyond" the subsystem itself and on a higher system level.

Effective protection for critical infrastructures, therefore, calls for holistic and strategic threat and risk assessment at the physical, virtual, and psychological levels as the basis for a comprehensive protection and survival strategy, and will thus require a comprehensive and truly interdisciplinary research and development agenda encompassing fields ranging from engineering and

[36] Berkowitz and Hahn, op. cit.
[37] Westrin, op. cit., p. 74.

complexity sciences to policy research, political science, and sociology. There is no doubt that CIIP will be a major R&D challenge in the future. R&D in the field of CIIP is undertaken by a large variety of actors in each country: research institutes at universities, private-sector research institutes and laboratories, networks of excellence, national research councils, etc. However, so far, there has been rather little coordination and cooperation between R&D actors at the national level.

Furthermore, the inherently transnational nature of CII and the growing international dependency on CII, as well as threats and vulnerabilities to the national CI (a good example is the big blackout in Italy's electric power system in October 2003) make the topic an obvious issue for international cooperation[38] — an issue we turn to in our last chapter.

From the National to the Global

We end this volume as we have ended the first one, by reflecting on what has been called "a global culture of cyber-security". The 2003 WSIS Declaration of Principles calls for such an effort in order to strengthen the trust framework, including information security and network security, authentication, privacy, and consumer protection, all prerequisites for the development of a strong Information Society, a goal pursued in many countries around the world.[39] But, once again, how are we to get there? How can a global culture of cyber-security be fostered? The WSIS Plan of Action proposes to reach that goal mainly by promoting cooperation among governments and by getting them, in close cooperation with the private sector, to prevent, detect, and respond to cyber-crime and the misuse of information and communication technologies by developing guidelines and considering legislation, by strengthening institutional support, and by encouraging education and raising awareness.[40]

[38] The rationale for strategic coordination of R&D at the international level was outlined at a December 2001 EU-US workshop on R&D in the field of CIIP. Cf. EU-US Workshop Report, "R&D Strategy for a dependable information society: EU-US collaboration", 1–2 December 2001 (Düsseldorf, Germany), a. Available at: http://www.ddsi.org.

[39] World Summit on the Information Society. "Declaration of Principles Building the Information Society: A Global Challenge in the New Millennium",. D document WSIS-03/GENEVA/DOC/4-E, 12 December 2003, a. Available at: http://www.itu.int/wsis/docs/geneva/official/dop.html.

[40] World Summit on the Information Society, "Plan of Action". Document WSIS-03/GENEVA/DOC/5-E, 12 December 2003., a Available at: http://www.itu.int/wsis/docs/geneva/official/poa.html.

Solutions to international public-goods problems should consider furnishing an international organization with sufficient funds to subsidize abatement, and empowering it with sharp enough teeth to penalize non-compliance. At the World Summit on the Information Society 2005 held in Tunis, it was suggested that the UN for example could govern the internet, and devise treaties to address issues such as cyber-security. Some support the idea, others feel that it will add more bureaucracy and further delay dealing with cyber-security issues, as UN treaty-making is inordinately cumbersome and certainly unduly time-consuming if the treaty-making effort were to start from scratch. An alternative method for moving towards a global framework would be to take an existing treaty and broaden its affiliation: This procedure is advocated by many who refer to the model of the Council of Europe Convention on Cyber-crime. For the existing convention with its broad coverage to be put to a more global use and thus to save precious negotiation time, it would be necessary to focus on its intrinsic merits and built-in flexibilities.[41]

In addition, governments should make sure that "cyber-crime havens" cease to exist. Different nationalities have different legal systems and criminal laws; therefore, arrangements and cooperation mechanisms between enforcement agencies are the appropriate way to deal with cyber-crime that crosses borders. States should review their laws in order to ensure that abuses of modern technology that are deserving of criminal sanctions are criminalized and that problems with respect to jurisdiction, enforcement powers, investigation, training, crime prevention, and international cooperation with respect to such abuses, are effectively addressed. Liaison between law enforcement and prosecution personnel of different states should be improved, including the sharing of experience in addressing these problems. These measures will ensure that the international community can move swiftly towards a much-needed international and global culture of cyber-security.

[41] World Federation of Scientists Permanent Monitoring Panel on Information Security. "Information Security in the Context of the Digital Divide: Recommendations submitted to the World Summit on the Information Society at its Tunis phase" (16 to 18 November 2005)". , Document WSIS-05/TUNIS/CONTR/01-E, 2 September 2005, p. 23., a Available at: http://www.itu.int/wsis/docs2/tunis/contributions/co1.doc.