Available online at www.sciencedirect.com
ScienceDirect
Safety Science 45 (2007) 415–430
SAFETY SCIENCE
www.elsevier.com/locate/ssci

Critical infrastructure and systemic vulnerability: Towards a planning framework

Tomas Hellström *

Institute for Management of Innovation and Technology, Chalmers University of Technology, 412 96 Göteborg, Sweden

Received 29 September 2004; received in revised form 8 July 2006; accepted 21 July 2006

Abstract

This article presents an analytical planning framework for hypothesizing, formulating and mitigating vulnerability in critical infrastructures. The point of departure is that because technological change plays a significant role in the development of critical infrastructures, the dynamics of such change must be taken into account when assessing how such structures advance a state of vulnerability over time. A second key notion is that while underlying interdependencies are characteristic of developing technological systems in general, these relationships receive a new significance in the context of critical infrastructures. The article contributes a model of vulnerability, which integrates a number of system levels of technological change as they bear on critical infrastructures. The framework is exemplified by a case description and analysis of cyber attacks on vital public functions. Finally a number of key principles are proposed for addressing systemic vulnerability in critical infrastructures across sectors of society.

Keywords: Infrastructure; Critical; Vulnerability; Systemic; Technology; Change

1. Introduction

In 1997 the President's Commission on Critical Infrastructure Protection established that greater cooperation was needed between the public and private sectors, as well as

* Tel.: +46 317739697.
E-mail address: tomashellstrom@linuxmail.org

0925-7535/$ - see front matter © 2006 Elsevier Ltd. All rights reserved.
doi:10.1016/j.ssci.2006.07.007

between agencies, in order to protect the critical functions of society (PCCIP, 1997). This was mainly due to the fact that while government is responsible for protecting the public and guaranteeing a certain level of societal functionality and safety, many of these functions, or at least the technologies upon which these functions critically depend, are owned and operated by private interests. In addition, many infrastructural threats are directed towards functionally and physically distributed and interlocked systems, whose ownership reside with many different public and private organizations.[1] In terms of risk analysis and risk management, this type of 'hybridization' of infrastructural systems has implied a broadening of focus from single to interconnected technologies, from individuals to social systems, from impact risk/probability of impact to structural vulnerability, and from frequency thinking to scenario thinking, where 'safety imagination' and mechanisms for (inter)organizational learning become necessary (Pidgeon and O'Leary, 2000; Kirwan, 2001; OECD, 2003). However, while these shifts in perspective have been convincingly argued for with regard to specific areas of the risk cycle (e.g. risk analysis needs to become more interdisciplinary, or risk management needs to become more cross-institutional), a comprehensive, integrative approach to these issues is still in the making. The present article seeks to contribute to such an approach by (1) introducing a new notion of technological and social change to risk analysis, and (2) by utilizing a systemically sensitive view of vulnerability, in order to (3) suggest an integrative tool for realizing the ambition of cross-sectoral planning. The argument is that a systemic or comprehensive understanding of vulnerability of critical infrastructure is necessary for an equally systemic policy coordination effort aimed at increasing the resilience of such structures. If system understanding and system intervention are not on par within the ambit of one flexibly yet coherent framework for describing and negotiating vulnerabilities, robust solutions will not emerge. While both the PCCIP and the more recent OECD report Emerging Risks in the 21st Century (OECD, 2003) indeed contain many of the premises for a solution, neither provides the theoretical building blocks for generating it as such far less to adapt it to changing circumstances. The present contribution will make an attempt towards those ends.

The article is structured as follows: Firstly, a notion of innovation will be elaborated which explains the potentially systemic and disruptive nature of technological change; secondly the concept of critical infrastructures will be discussed with an eye to some tricky methodological implications for assessing 'criticality'; thirdly a framework for vulnerability will be proposed which emphasizes interconnectedness and 'layerdness' of social and technological systems. Following this will be introduced a case description of critical infrastructure risk and vulnerability resulting in cyber terrorism, particularly here the interactive technological and social elements of rogue computer/network use. Finally, the aspects discussed above will be integrated within an analytical planning framework for critical infrastructures, and a number of key principles for their functioning will be proposed.

[1] A case in point is the 1998 US incident where the PanAmSat's Galaxy IV satellite malfunctioned due to an on-board controller failure, the immediate result of which was a disruption of 80–90% of the country's pager services. This disruption caused problems for hospitals (which were dependent on pagers to reach doctors), emergency workers, the functioning of credit card machines, as well as several more critical functions (Ziad, 1998). The key characteristics of this event, as well as the ones discussed by the PCCIP, can be seen as extensions of traditional risk analysis typical of our time.

2. Innovation, infrastructure and vulnerability

In what follows, three areas of importance for assessing and reducing systemic vulnerability to critical infrastructures will be reviewed: (1) the modalities of technological change, particularly the sources and effects of creeping and disruptive innovation, (2) the notion of critical infrastructures, whose consideration it is argued must include structural and locational as well as methodological and definitional aspects, and (3) an understanding of vulnerability which emphasizes dynamic and nested pressures on critical systems.

2.1. Disruptive technological change

One may say that innovation or technological change becomes a risk when as a result of creation or improvement of technology, one or several system components increasingly threaten to come into adverse contact with other system components so as to negatively impact on human values. From a quantitative vulnerability assessment (QVA) standpoint vulnerability is generated by the emergent complexity and connectivity of multi-component systems, which is also referred to as 'complexity induced vulnerability' (Gheorghe and Vamanu, 2004). This phenomenon has also been addressed under the rubric of 'negative technological synergy' (Hellström, 2003), where the emphasis is on the combinatory effects of planned, chance or physically latent interference between components of one or several technological systems. The likelihood of such disruptions may in some instances be hypothesized already in advance, but they may also be completely new to all involved actors. The risk of the latter increases when innovation becomes geared towards the 'technological system', that is, when one innovation affects the workings or relevance of many seemingly unrelated technologies through a profound change in disparate social practices as well as in what is perceived to be technologically possible (Freeman and Perez, 1988; Christensen, 1997).[2]

Innovation trajectories within the technological system can cascade in unforeseen ways. This typically occurs when the technological 'action sphere' of a certain subsystem expands rapidly into many areas of life, as well as into other technological systems. However, the potential for truly disruptive technological change and associated risk stems from the combination of radical innovation with another more mundane form of innovation. Incremental innovation is the gradual refinement of systems to achieve small improvements in performance. Disruption does not come about through expansion of a system, but rather because incremental change may embed design flaws gradually deeper into a system, where ad hoc solutions to improve workability hide problems under increasingly thick layers of technological 'improvements', yet do not eliminate them. Such systems rather build up an internal pressure, which a sudden change in system environments (such as that brought about by an innovation in the technological system) may unleash. Notions of long-term incubation of industrial disaster, for example such as those reported by Turner and Pidgeon (1997) and by Shaluf et al. (2002) are examples of risk from incrementalism. It is important to note that in these cases, and this is also the present understanding of innovation and technological change, technologies are seen as physical systems in conjunction with the routines for their

[2] The Internet and the proliferation of the personal computer perhaps best exemplify this type of 'interactive' innovation. The steam engine was an early example of such a technology, which reformed production systems, communication, transportations systems and international relations alike (Rosenberg, 1994).

operation and the social practices that underpin development and use of technology (cf. MacKenzie and Wajcman, 1999; Guston and Sarewitz, 2001).

One way of capturing the complexity and embeddedness of technological transitions is to carry out a description on three simultaneous levels: macro, i.e. the evolving socio-technical landscape that drives and enables the technological system, meso, i.e. the 'patchwork of regimes', standards, regulations, etc., and micro, i.e. the novel configurations which an technology undergoes through the actions of individuals and firms who seek new forms of utility (Rip and Kemp, 1998). Authors in the quantitative risk analysis tradition have also pointed out that frameworks for risk criteria for critical infrastructures must find useful correspondences between those criteria employed to analyse vulnerability on the macro (societal) level, and those used for specific infrastructures (micro or technological level) (Vrijling et al., 2004). This multidimensionality is compounded by the fact that many technologies are 'multiform', with newer technologies embedding older ones, so that one technology, in one end of its lifecycle, may contain pockets of significantly older or newer technological components at another end of their life cycles. This is true for large infrastructural systems as well as for consumer products, which increasingly comes to embed digital technology of various forms.[3] This type of embeddedness also encourages the development of 'pockets of expertise' (Petrick and Echols, 2004) relating to the same system but radically different forms of technology. Where the expertise set for single technologies becomes harder to distinguish, the overall system becomes increasingly vulnerable.

One important insight that follows is that disruptive technological change must not necessarily be connected to single radical innovations. In fact, Foster (1988) among others has noted that firms rarely leap from one technological platform to another. This is mainly due to previous investments and the need to regain sunk costs, but also to the interconnectedness of the innovation process, where firms often use customers to determine product needs. That is a mutual dependence develops in the value chain, which locks firms into technological trajectories. Networks of public and private organizations tend to continue to invest in known technological solutions until the marginal cost for incremental improvements to the system as a whole has increased beyond what is acceptable. In other cases the everyday compensation and rescue of a continuously failing system may accrue costs quite outside of any reasonable cost-benefit consideration. An unacceptability limit usually comes about as a result of challenges posed by scale (when technology has to meet impossibly small or large applications) as well as by systems complexity (Sahal, 1981). At this stage, the viability of a radical systems redefinition exists. Two conclusions may be drawn from the above reasoning: firstly, new radical replacement technologies are not likely to be adopted blindly due to among other things costs, and secondly, new technologies have to be scale adapted, i.e. they cannot spread unrestrictedly. Again, this interpretation of technological change seems to support a system perspective on technological risk in the sense that it lends credence to the view that threats are likely to come from unexpected interaction effects between new and old technologies, and between new and new technology, mainly due to the difficulty in assessing the scope of one technology as it is combined with another. As we will see further down, when technology is expanded to also include various social technologies (such as the education system), this holds particularly true.

[3] An example is the dependence of mobile communication on earth bound carrier and networks, e.g. switching stations, which offer points of relative vulnerability to intentional breaches (see the example of 'phreaking' in Section 3.2).

2.2. Critical infrastructures

Critical infrastructures have recently sailed up on the international and national agendas due to among other things the threat from terrorism. The concept has been gradually broadened from its original meaning, that is "those structures whose prolonged disruption could cause significant military and economic dislocation" (Moteff et al., 2003, p. i). The German authority Bundesamt für Sicherheit in der Informationstechnik for example now defines it as "organizations or facilities of key importance to public interest whose failure or impairment could result in detrimental supply shortages, substantial disturbance to public order or similar dramatic impact." (BSI, 2004). Both of these definitions are broad and are at the same time of a 'counterfactual' nature. They are broad because they cover sectors such as transportation and traffic, energy, hazardous materials, telecommunications, finance/insurance, and of course services such as waste management, water and food, civil protection and health. They are also broad because it is typically assumed that "if individual such infrastructures are affected by deliberate disruption (Information Warfare, cyberterror, etc.) or failures of information technology, this could have the effect of triggering a chain reaction of disruption in other areas as well." (BSI, 2004). The notion of critical infrastructure is counterfactual, because we do not know in advance, due to systems evolution, complexity and shifting intentions and actions of relevant actors, where failure will occur and what impact this will have. Critical infrastructure then risks becoming everything that we think is important to the functioning of society and yet nothing really specific enough to focus vulnerability reducing measures on. The fact is that in these vast socio-technological systems failure is indeed a normal condition (Perrow, 1984).

In the US National Strategy for the Physical Protection of Critical Infrastructures and Key Assets (2003), a systemic 'effect-vulnerability' notion of critical infrastructure is proposed, namely that three types of effects may confer vulnerability on a system:

- *Direct infrastructure effects.* Cascading disruption or arrest of the functions of critical infrastructures or key assets through direct attacks on a critical node, system, or function.
- *Indirect infrastructure effects.* Cascading disruption and financial consequences for government, society, and economy through public- and private-sector reactions to an attack.
- *Exploitation of infrastructure.* Exploitation of elements of a particular infrastructure to disrupt or destroy another target (p. 20).

What this explication adds is a clear understanding of critical infrastructures as grounded in 'critical nodes', 'cascading effects' or multiplicator effects, and the possibilities of 'acting at a distance' which the interlinked nature of such systems offer. The result of these qualities is that an assessment of what is a critical infrastructure cannot proceed solely on assessing what structures are important to society. Instead such an analysis must elaborate some systemic 'maximum reference point' for criticality of specific technological and social systems in conjunction, that is where in fact a technological system is most vulnerable, combined with an assessment of where a socio-economic system is most vulnerable, and how the medium between these systems presents a differentiated propensity to propagate harm or energy between their respective points of vulnerability. This reasoning is consistent with both the notion of internal connectivity of multi-component systems

(Gheorghe and Vamanu, 2004) and the idea of a unified framework for societal and infrastructural vulnerability criteria developed in QVA (Vrijling et al., 2004). In addition, risk analysis is necessary to assess the quantity and quality of outside triggering forces on a given system. Such a view would offer a more contextual and comprehensive account of technological innovation and change, in that it emphasizes the social embeddedness and the critical vulnerability conferring qualities of this embeddedness on technology and society. Before a case is presented to further illustrate this dynamic, I will present a model of vulnerability that seems particularly useful for addressing these systemic qualities of infrastructure and change.

2.3. Dynamics of vulnerability

The notion of vulnerability emphasizes the exposure of a system to hazard from the point of view of the nature of that system itself. Ideally such an account should include some of the systemic properties that have been described above, particularly from the perspective of the resilience of the technology–society interfaces of the system at hand. Because vulnerability has often been regarded as a property, and not as an outcome of social relations and technological systems (Hilhorst and Bankoff, 2004), the concept is easier to deal with than that of risk, as it does not exclusively emphasize a future, or counterfactual state of affairs, but also, and perhaps most obviously, certain qualities of a system in the here and now. Vulnerability assessments cannot take place without attention to hazard and thereby also to risk, however, the concept puts the emphasis on what an actor can directly affect rather than a threat from the outside, or a possible development in the future. One may say that the vulnerability, or opposite, the resilience, of a system is a more 'ontologically robust' and 'epistemologically accessible' dimension than that of its exposure to risk.

The notions of technological change and critical infrastructures elaborated above necessitate a dynamic understanding of vulnerability. Such an understanding can be found in Blaikie et al.'s (2001) 'pressure and release' (PAR) model. The PAR model was originally developed to account for socio-economic vulnerability to natural disasters in developing countries, and has the household as a main reference point. Because of its comprehensiveness, it is well suited for analyzing vulnerability in larger socio-technical systems. The model depicts how underlying factors or root causes, which are deeply embedded in social and technological conditions give rise to dynamic pressures affecting specific areas of activity, and ultimately resulting in unsafe conditions at different localities. When unsafe conditions generated by underlying factors and root cause are confronted with a hazard or trigger event, which in the present understanding could be a planned attack on a system as well as a intersystem conflict brought to the surface by an environmental fluctuation, the result of which is an adverse event. Triggering events are synonymous to hazards and the combination of these events and vulnerability is the same as risk (i.e. risk = hazard + vulnerability).

Fig. 1 is a version of Blaikie et al.'s original PAR model adapted to better take account of infrastructural issues such as the one discussed in the case below.

The factors to the left and the right of the adverse event can be seen as pressures, and actions taken to alleviate these from the system are called releases. It is important to note that the two sides of the model are not isolated, but bear heavily on each other, as well as are transformed by the progression of the adverse event itself, should it realize. It is also important to note that unlike the original PAR model, where vulnerability progresses from

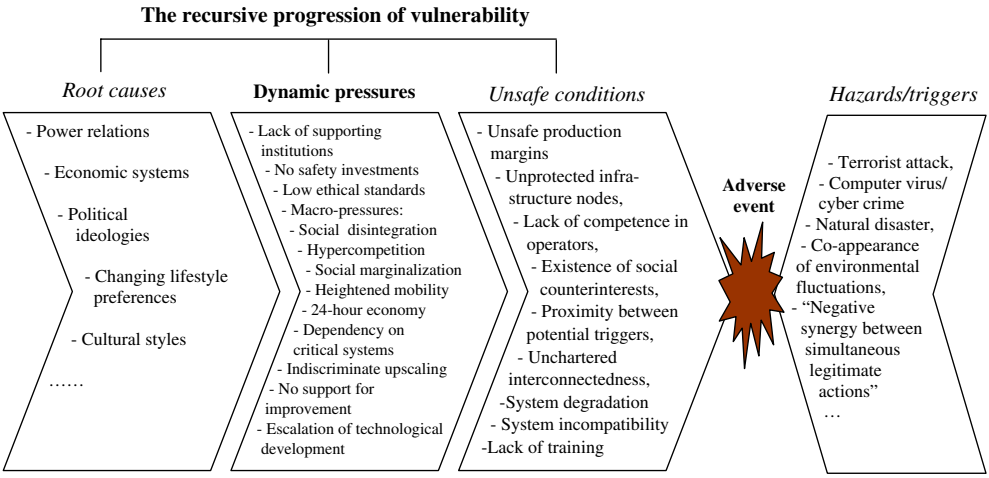

Fig. 1. The multilayered and recursive progression of vulnerability in critical infrastructures (adapted from Blaikie et al., 2001).

root causes to unsafe conditions, this version of the model can be seen as recursive in the sense that unsafe conditions can create dynamic pressures, which may eventually turn into root causes and generate a number of new unsafe conditions. From a governance perspective it seems then especially pertinent to identify these recursive movements, and pinpoint which unsafe conditions may be in risk of becoming dynamic pressures or worse. Furthermore, the model can be used as a means to avoid 'unnecessary' release interventions in the wrong parts of the system, i.e. by viewing vulnerability as a progression from root causes to unsafe conditions and vice versa, one is better able to analyse which interventions will sustain safety under fluctuating conditions, which conditions are dependent on which root causes and in extension which social actors must cooperate in order to remedy these conditions. A cross-sectoral planning tool for infrastructural vulnerability reduction must be able to motivate empirically and analytically the necessary points of inter-agency cooperation, as well as to find efficient public–private and national–international interfaces. The modified PAR model contributes a framework for structuring such arguments.

3. Cyber attacks and systemic vulnerability

This section describes how certain aspects of the intersection of information systems, people and critical infrastructures create complexities and unforeseen vulnerability. In the President's Commission on Critical Infrastructure Protection, PCCIP (1997), Chairman Robert T. Marsh announced that all US infrastructures are increasingly dependent on information and communication systems that criss–cross the globe, and that this dependence is the main source of society's increasing vulnerability. The commission reported on the debilitating effects on the general infrastructure of cyber attacks, and that there is a wide spread and growing capability to do serious harm to these information systems and in extension to infrastructure at large, (1) because of advances in rogue 'computer virology', i.e. data virus development, and (2) because of the complex interconnectedness of vulnerable systems.

3.1. Systemic pressures: cyber terrorism and computer 'virology'

In the case of cyber terrorism, social and technological innovation go hand in hand. On the human side, increasing computer literacy on a global level has meant that potential threats are spread geographically wider, as are motives to do harm more diversified. The US National Security Agency (NSA) has estimated the number of people computer literate enough to launch a cyber attack against a system to be about 21 million worldwide in 2002. To the author's knowledge, this estimate is yet to be confirmed, however given what is now known about the diffusion of home computers and Internet technologies, the figure seems low. On the technology side, the wide adoption of common protocols for system interconnection, embedded (and hidden) functionalities in software, and the availability of hacker tool libraries on the Internet are other key pressures. We will not delve into the psychosocial root causes for cyber terrorism in this article (a few possibilities are suggested in Fig. 2), but rather what aspects of the technostructure these threats emerge from, and are increasingly directed against. We will start by looking at a number of 'innovations' in computer virology that may serve to further enhance these threats.

Specifically, it is often stated that the emergence of tools for attacking computer systems in order to shut them down poses a larger infrastructural threat than those that aim to steal, corrupt, destroy or manipulate specific data, e.g. in industrial espionage. The former can be shown to be on the rise recently, and have proven to have severe consequences for critical infrastructures on a global scale. Some aspects of technological development in this area, e.g. its utilization of informal distributed work and open source models for organizing development, while certainly constructive in other domains of innovation, make it difficult for authorities and corporations to successfully keep abreast with developments. In order to give a brief contextualization of these vulnerabilities, a history of developments so far will be presented, as well as a couple of pointers to possible future developments.

Network Associates estimated that the number of known viruses and worms had reached more than 54,000 by January 2001 (Vibert, 2001). Worm viruses such as Kak, Loveletter and Prolin were designed to spread themselves through e-mail by exploiting

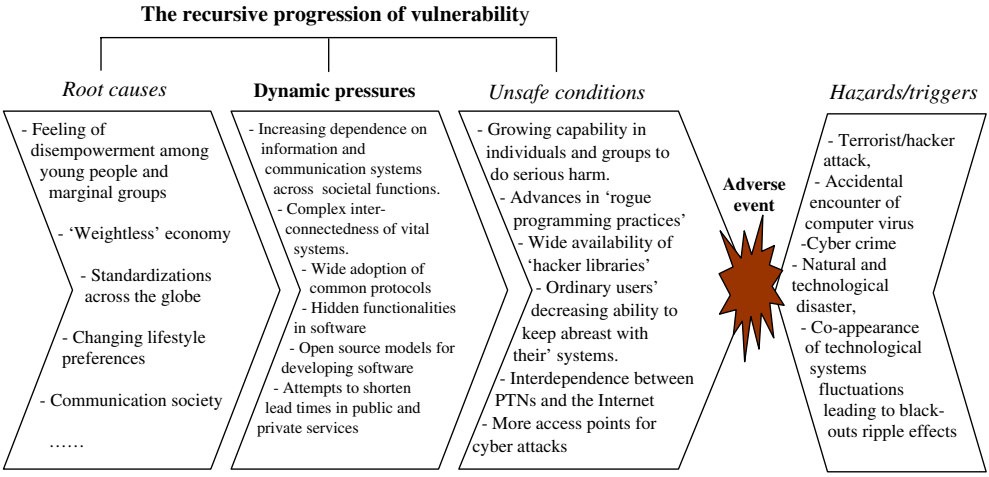

Fig. 2. Vulnerability and triggers in the cyber attack case.

vulnerabilities in common applications, e.g. MS Outlook and Outlook Express. Active infection by any of these so-called 'worms' can result in thousands of infected messages being broadcast within a few hours, thereby infecting other users. The first of this type of virus, Melissa, emerged in 1999 and quickly brought down numerous corporate and public servers by overwhelming them with messages. LoveLetter surfaced a year later and had similar but worse effects on the ICT-structure, causing severe disturbance to peripheral infrastructural utilities as well. Cost estimates to organizations worldwide are in the billions of dollars.

Viruses of this kind are increasingly delivered through direct use of the functionality and interactivity of the computer system itself. For instance, several use the fact that many e-mail programs allow the use of HTML-code in the body of the message. The Kak worm works in this fashion, and infects the system when the user merely previews the infected e-mail message. Again others enter as file attachments and take advantage of Windows' rarely changed display settings, which show the name of the file but not its extension. Thereby users may unwittingly open an executable file with a .vbs (Visual Basic) extension – as in the LoveLetter case – by viewing the file name "LOVE-LETTER-FOR-YOU.TXT".vbs. Macroviruses utilizing functionalities in the Word program are hidden in ordinary .doc files and carry malicious macros inside. These, as well as the self-mail worms described above account for the largest number of incidents now, and are expected to continue to do so in the future.

This is a problem that should not be underestimated, because it resides partly in the cognitive abilities or bounded rationality of users in relation to the pace in which they work their computers, and partly in a sort of auto-immune reaction, where the interactivity of desktop applications and the user friendliness of programming tools such as Visual Basic and Word Macros, have turned the systems' functionality against themselves. Viruses set off in this fashion, by the user/system interface 'itself', continue to grow, causing infrastructural disturbances at great costs.

'Hybris', which was discovered in November 2000, gives an indication of where virus attacks have been heading in the past few years, and what to expect in the future. This type of virus can continually enhance and modify itself by downloading new version of its code from websites on-line. The virus may, for instance, access Usenet groups such as *alt.comp.virus* to obtain plug-ins that alter its behavior and enhances its capabilities. In this way it can become extremely difficult to stop, as it can enter as harmless code and later become damaging to the system in a variety of ways.

Virus attacks may also be directed against a particular object. Examples include cyber attacks against a specific operator or database for the purpose of gaining access and information and/or control. A subset of this type of attack is the 'electronic reconnaissance' where networks with low security standards are used to gain access to more secure and critical networks through utilization of their interconnectivity. Cyber attacks for the purpose of shutting down services are becoming more and more common. This usually takes place by flooding communication lines, or in the case of vital services by short-circuiting 911 switches. Critical infrastructures are also increasingly attacked through introduction of harmful instructions, such as Trojan horses devised to destroy software at a preselected time, or simply to feed passwords and other information to an outsider.[4]

[4] For more information on these types of cyber attacks, access the RiskINFO homepage at www.riskinfo.com/cyberisk.htm (accessed 08.07.06).

3.2. Key vulnerabilities

The ICT-system, i.e. Public Telecommunications Networks (PTNs), the Internet and an increasing number of Extranets, connects emergency services, financial networks, military command-control systems, gas and oil pipeline systems, transport and educational systems. Growing complexity and interdependence in particular in the energy and communication infrastructure imply that even minor disturbances can cascade into, for example, regional outages. Technical complexity may also permit major disturbances to go unrecognised, and cumulate, until failure occurs. The most important vulnerability lies in the interdependency between PTNs and the Internet, in the sense that the Internet depends heavily on PTNs, and the PTNs in turn depend on electrical power operations, satellite and optical cables. Continuing deregulation of the telecommunication industry means that the number of access points will increase, as will opportunities for attack.

The ICT-systems and the Internet connect in various ways to physical infrastructural systems, at which points these physical systems may be directly attacked through virtual means or damaged by dint of a more wide spread cyber attack. As previously stated, the PTNs are increasingly managed and maintained through computer networks, which in turn are subject to remote operation through AXE-phones. Incidents of so-called 'phreaking', or manipulation of distant digital switches through the telephone may disrupt large PTNs, and pose a threat to emergency systems, as was the case when two Florida 911-switches were completely short circuited by a teenager sitting in Gothenburg, Sweden using nothing but his parents' phone. In the case of electrical power, the widespread and increasing use of Supervisory Control and Data Acquisition (SCADA) systems for external control provides a possible access point for cyber attacks, which targets substations, generation facilities and transmission lines.

In the case of banking and finance many back-up systems and parallel arrangements create a high level of security. However, functions such as payment systems, securities and commodity exchanges with their clearing and settlement organizations are heavily dependent on telecommunications services and electrical power and their breakdown, even if improbable, would put the economy at large at risk.

The sector of physical distribution is increasingly relying on ICTs to shorten lead times, route and schedule traffic, tracking, etc. This means that vulnerabilities in the ICT-structure can potentially affect every aspect of the transportation industry and its dependent downstream systems. Future challenges may be found in the modernization of Air Traffic Control functions (e.g. the National Airspace System in the US) and in Global Positioning Systems (GPS), which are soon to become the sole basis for radio navigation. On the firm level, emerging organizational technologies such as Enterprise Resource Planning (ERP) and Electronic Data Exchange (EDI) allow customers to access inventories, prices and other data in the company. Because of the interconnectedness of back-office systems and order-entry and customer service departments, even a small attack may resonate with the customer. As online business-to-business and business-to-consumer relations grow, this trend is likely to continue and show increasingly adverse effects.

With publicly held companies, market valuations may be affected by only the hint of a cyber attack. For example, when 'denial-of-service' attacks shut down several large e-commerce sites in 2000 share prices fell sharply as investors reacted to a threat that they had not seen before (SANS Institute, 2000). However effective, these new technologies also allow for new forms of security breaches, and pose new economic/infrastructural threats to

the economic sector. This situation may be represented in terms of the above notion of systemic vulnerability (Fig. 2).

Only a limited number of factors can be accommodated within the model due to lack of space, however the principle of attempting to assess root causes, dynamic pressures and unsafe conditions, and then ascertain what type of triggers may act upon the system, still stands. What is further important to note is that the difference between opportunity and risk becomes hard to differentiate from a public perspective, for instance, the increased call for participatory democratic mechanisms is an opportunity for a reformed political society in line with general post-cold war transformations, however it also risks giving rise to renegade expressions of associate interests, such as radical political groups which ultimately resort to violence when the supporting democratic structures are not perceived to function in their favour (cf. the notion of 'anomie' and the notion of 'rebellion adaptation' developed by Merton, 1938). The dynamic pressure of 'increased computer literacy' is another case in point, where it is hard to practically separate knowledge to create from knowledge to destroy. Several such dialectic contradictions may be found or constructed from the vulnerability model, and such constructions should indeed become a part of systemic risk analysis and vulnerability reduction.

4. A systemic framework for vulnerability reduction

In what follows, the above theoretical exposition of technological dynamics and critical infrastructures, together with the insights drawn from the area of cyber attacks and PTNs will be used to draw some implications for a planning framework for vulnerability reduction.

4.1. Lessons from the ICT case

Since many of the causes of the vulnerabilities and risks outlined above originate in the social sphere, with increased computer literacy and a diversification of motives, vulnerability reduction must go beyond simple virus protection, fire-walls, etc., and address for instance educational issues, i.e. creating awareness of risk, but also infusing a sense of ethics into the computing activity on an early stage. On the policy side a number of additional issues need to be resolved. Since information and communication systems are now mainly privately operated and infrastructures are largely public domain, a systemic management of these risks should be conducted in partnerships between public and private interests, e.g. between local and regional infrastructure owners, companies, operators and government.

The strategy outlined by the PCCIP (1997) in relation to these kinds of vulnerabilities includes a comprehensive cooperation and communication strategy between the above actors, involving cross-sector clearing houses with industry CEOs/systems owners, state representatives and local governments to provide policy advice, implementation commitment and real time capability for attack warning. Such clearing houses could function to promote industry development and implementation of common incident reporting processes, initiate and coordinate exercises and simulations (pressure testing ICT systems) to assist government and industry in vulnerability reduction decisions, as well as to define security metrics for ICT-networks and their infrastructural interfaces. Clearing houses of this kind should function both as centres for knowledge transfer, and promoters of the deployment of new security measures among participants, and thereby increase the systemic resilience of critical

systems. Such clearing houses may also be utilized by governments to mainstream and clarify elements of the legal structure that have not kept pace with the developments in market and technology, both with respect to information security and deregulation as well as to the responsibility of, and legitimate oversight over Internet Service Providers (ISPs). Some laws may be too ambiguous for application to future situations envisaged by industry, and again some may be directly security unfriendly. This is a task that must be effective on the local, regional and international level.

Governments need to identify critical ICT-network dependent nodes of the critical infrastructure and create buffers together with operators to insulate these nodes from system disturbances. Such nodes would typically be found by 'backtracking' from the critical infrastructure and into the publicly accessible ICT-network. Interfaces of particular importance are those that connect to high reliability systems, like nuclear and process industries, airspace systems, and certain physical distribution systems such as railroads, pipelines and bridges. Critical ICT nodes may also be identified in emerging IT-dependent systems, like Intelligent Transportation Systems (ITSs) which rely on GPS, and emerging industry production networks (cf. Hellström, 2003). Critical nodes of this kind may be mitigated through 'buffering', e.g. as airspace radio navigation becomes GPS based, a possible buffer may be to have back-up navigation and landing capabilities for air vessels, by retaining functions from the old system.

In order to organize these efforts it is necessary to find a 'systemically sensitive' framework for analyzing risks and vulnerabilities as well as to organize their mitigation.

4.2. Principles for a vulnerability reduction framework

Obviously there is a great need to reduce the complexity inherent in deciding how administrative resources should be put to use for vulnerability reduction in critical infrastructures. In this article it has been assumed that critical infrastructures are essentially technological systems filling social functions, which are dependent for their creation, utility and maintenance on human actors. To add complexity, such systems are commissioned at different times (a temporal dimension) and different places, (a spatial dimension), during and at which there are different interests and capabilities at play. Across sectors there will be a spectrum of judgements as to what are the cost-benefit trade-offs, and finally, if one takes enough of a birds-eye view it becomes apparent that all technological components of a critical infrastructure are added and removed incrementally, and have differently paced cycles of adoption, maturation and death. These qualities of system components generate a number of key 'interfoliations' between technologies, social systems and interests, which together form an analytical framework for planning of vulnerability reducing interventions (cf. Figs. 1 and 2). This framework refers back to the previous discussion on innovation, critical infrastructures and the dynamics of vulnerability, and derives a number of analytical principles for vulnerability planning. In the following usage a critical infrastructure will be addressed in terms of a socio-technical system, which comprises the technological and the social components of the critical infrastructure as well as the context of relevance to its functioning.

Principle 1: Functional interlocking.

A socio-technological system has a functional interlocking, i.e. its functionality is dependent on the functionalities of other systems according to the principle 'get one get them all'. This quality means that cascading effects through a number of systems may occur even

when these systems are not physically connected. A system may be functionally dependent on another only on certain occasions, and when used for certain ends. Successfully reducing critical points of interlocking does not only depend on 'architectural analysis' of the interrelatedness of parts, but also on the dimensions of functionality, which in turn relate to level of functional embeddedness and place of the interrelated technologies in their respective life-cycles. In effect such an analysis must also deal with the social life of the technology. A critical question for this type of analysis is how hard will it be to 'challenge' a technology which is part of normal life for many people in the sense that it is integrated into more complex technological and social practices.

Principle 2: Temporal embeddedness.

It is important to take account of how piecemeal additions and improvements (incremental innovation), relate to radical innovations or innovations in the technological system as a whole. For example, if a critical system is about to undergo a radical innovation, it makes sense to carefully identify the 'depth' of this system in terms of how it depends on technologies and social practices that have been deeply embedded throughout a longer period of time. Hidden faults may emerge as a result of a radical change in the superstructure of a system. How, for instance is new aviation-navigation technology dependent on more sticky operating procedures for air communication? Commissioning and decommissioning new technologies on top of old ones, may be a play of dice. Insofar as this is an embedded technology, are there competences available for its successful decommissioning? Here it becomes important to critically assess what is a technology. Is an education system a technology?

Principle 3: Critical socio-technical tipping-points.

Critical infrastructures are 'critical', not because they are important in general, but because they are strategically connected in such a way that they focus society's total vulnerability to a few particular points in the system. While from the perspective of risk analysis critical infrastructures must be conceived broadly enough to allow for an open minded assessment of the possible interaction effects between social and technological systems, from the perspective of vulnerability reduction and cost-effective interventions, these critical points must take the centre stage. It is through eliminating pre-emptively (by for example pro-active technology assessment) and by protecting such critical points that we can effectively engage with the critical infrastructure without disrupting the wider functioning of society (cf. the fact that dynamic pressures are also often sources of benefit for society). The fact that these critical points are of a socio-technical nature, means that their management is not a technical question but a rather an question of finding an optimal 'tipping-point' where intervention in technology does not disrupt social functionality, i.e. the question of when the medicine will kill the patient.

Principle 4: Dynamic and reversive effects

It is important to note that critical points of large socio-technical systems are dynamic and fluid. The analysis of the ICT case in terms of root causes, dynamic pressures and unsafe conditions shows that one unsafe condition can become a dynamic pressure, which is harder to remedy, and further that a few root causes and dynamic pressures can affect several unsafe conditions at once. Also, the model makes it clear that triggers of adverse events are not necessarily taking shape outside of the system itself, but are critically dependent on factors already present as vulnerabilities in the system. It is rather the combination of vulnerabilities/pressures focused at some point of the system, that ultimately realize the potential for an adverse outcome.

5. Conclusion

5.1. Some organizational implications

Petrick and Echols (2004) point to two important effects of cross-sectoral and hierarchical sharing of technological knowledge regarding subcomponents of critical systems: synergy and leveragability. Here synergy would imply that actors jointly seeking understanding of an area of vulnerability through deliberation and cooperation, may improve each partner's understanding of this area through a form of triangulation. This is the traditional way of conceptualizing the 'knowledge benefits' of cooperation. Leveragability would imply that one system owner can extend its reach and understanding within one existing area on the basis of information received from other parts of the system. This is a more systemic way of conceiving of what is relevant knowledge for improving the resilience of a system, in that some speculative thought would have to go into the way that actors can find leveragability in each others' knowledge. Among other things such speculation would require a planner to consider how surface vulnerabilities (e.g. unsafe conditions) are tied to dynamic pressures according to the principle 'one actors unsafe condition is another's dynamic pressure'. The principle of 'leveraging' in cooperation speaks directly to the understanding of a system as a set of interactive layers, the way it has been outlined above. The PAR model, the way it has been elaborated above, together with the four principles for vulnerability reduction, presents a methodology for coordinating cross-sectoral planning alliances with respect to critical structures.

It is worth noting that selection and mode of inclusion of actors in a comprehensive vulnerability assessment requires great sensitivity, since experience has shown that many involvement procedures with respect to actors further down the organizational hierarchies risks disenfranchising these even more, only in new ways. Practically, vulnerability assessment in this mode may be conducted, for example, through scenario development or technological road-mapping exercises focused on one particular infrastructural domain, and involving several different institutional actors from outside of this domain. In addition, Stoop (2003) has pointed to the need to include at least three different levels of policy actors in assessing critical infrastructures: (a) the commissioner or initiator of a new component of the system, whose interest lies primarily in the quality and cost-effectiveness of future operations, (b) the administrators involved in supervision and inspection including regulative policy making, whose interest is primarily in safety related procedural verification, and (c) the public and the rescue and emergency services, whose interest is primarily in safe operations and evidence that an emergency can be managed. This division includes a public–private, as well as a public–public relationship.

It is also clear that actors within these categories will deal with different aspects of an infrastructure. For example, assessment of standards will relate to both industrial and public sector activities, assessment of architectures will be a concern for maintenance personnel of the system owner (commissioner) as well as the rescue services: the former being involved with the integration (maintenance) and the latter with the disintegration (destruction) of these architectures. Linkages between various infrastructural elements will have to involve the assessments of public users of the systems, who operate with various levels and forms of expertise, while substitutions of elements are a concern for industry and public standard setters (cf. Vojak and Chambers, 2004). What the above presented framework offers, is a particular ontology for considering critical infrastructures and their elements/

subsystems in novel yet disciplined ways. Seeing such systems laid out qua socio-technical dynamic interactions, validates and gives a legitimate voice to a diversity of problem owners, and creates a framework for disciplined imagination with regard to critical infrastructures.

Acknowledgement

The author would like to acknowledge the financial and intellectual support of the Swedish Rescue Services Agency in preparing this article.

References

Blaikie, P., Cannon, T., Davies, I., Wisner, B., 2001. At Risk: Natural Hazards, People's Vulnerability and Disasters, second ed. Routledge, London.

Bundesamt für Sicherheit in der Informationstechnik (BSI), 2004. Kritische Infrastrukturen in Staat und Gesellschaft. Available from: <http://www.bsi.bund.de/fachthem/kritis/index.htm> (accessed 08.07.06.).

Christensen, C.M., 1997. The Innovator's Dilemma: When New Technologies Cause Great Firms to Fail. Harvard Business School Press, Harvard, Mass.

Foster, R.N., 1988. Timing technological transitions. In: Tushman, M.L., Moore, W.L. (Eds.), Readings in the Management of Innovation. Ballinger, Cambridge, Mass, pp. 215–228.

Freeman, C., Perez, C., 1988. Structural crises of adjustment, business cycles and investment behaviour. In: Dosi, G., Freeman, C., Nelson, R., Silverberg, G., Soete, L. (Eds.), Technical Change and Economic Theory. Pinter, London (Chapter 3).

Gheorghe, A.V., Vamanu, D.V., 2004. Complexity induced vulnerability. International Journal of Critical Infrastructures 1, 76–84.

Guston, D.H., Sarewitz, D., 2001. Real-time technology assessment. Technology in Society 23, 93–109.

Hellström, T., 2003. Systemic innovation and risk: technology assessment and the challenge of responsible innovation. Technology in Society 25, 369–384.

Hilhorst, D., Bankoff, G., 2004. Introduction: mapping vulnerabilities. In: Bankoff, G., Frerks, G., Hilhorst, D. (Eds.), Mapping Vulnerability: Disasters, Development and People. Earthscan, London, pp. 1–9.

Kirwan, B., 2001. Coping with accelerating socio-technical systems. Safety Science 35, 77–107.

MacKenzie, D., Wajcman, J. (Eds.), 1999. The Social Shaping of Technology, second ed. Open University Press, Berkshire.

Merton, R.K., 1938. Social structure and anomie. American Sociological Review 3, 672–682.

Moteff, J., Copeland, C., Fischer, J., 2003. Critical infrastructures: what makes infrastructures critical? In: Report for Congress. Congressional Research Service, Library of Congress, Washington, DC.

National Strategy for the Physical Protection of Critical Infrastructures and Key Assets, 2003. Government's Printing Office, Washington, DC.

Organization for Economic Cooperation and Development (OECD), 2003. Emerging Risks in the 21st Century: An Agenda for Action. OECD, Paris.

President's Commission on Critical Infrastructure Protection (PCCIP), 1997. Critical foundations: protecting America's infrastructures. In: The Report of the President's Commission on Critical Infrastructure Protection, October 1997. Government's Printing Office, Washington, DC.

Perrow, C., 1984. Normal Accidents: Living with High-Risk Technologies. Basic Books, Harper Collins Publishers, New York.

Petrick, I.J., Echols, A.E., 2004. Technology roadmapping in review: a tool for making sustainable new product development decisions. Technological Forecasting and Social Change 71, 81–100.

Pidgeon, N., O'Leary, M., 2000. Man-made disasters: why technology and organizations (sometimes) fail. Safety Science 34, 15–30.

Rip, A., Kemp, R., 1998. Technological change. In: Rayner, S., Malone, E.L. (Eds.), Human Choice and Climate Change, vol. 2. Batelle Press, Columbus, OH, pp. 327–399.

Rosenberg, N., 1994. Exploring the Black Box: Technology, Economics and History. Cambridge University Press, Cambridge, Mass.

Sahal, D., 1981. Patterns of Technological Innovation. Addison-Wesley, London.

SANS Institute, 2000. Consensus Roadmap for Defeating Distributed Denial of Service Attacks – A Project of the Partnership for Critical Infrastructure Security Version 1.10, February 23, 2000. Available at the Global Incidence Analysis Center: <http://www.sans.org/dosstep/roadmap.php> (accessed 08.07.06.).

Shaluf, I.M., Ahmadun, F.-R., Said, A.M., Sharif, R., Mustapha, S., 2002. Technological man-made disaster pre-condition phase model for major accidents. Disaster Prevention and Management 11, 380–388.

Stoop, J.A., 2003. Critical size events: a new tool for crisis management resource allocation? Safety Science 41, 465–480.

Turner, B.A., Pidgeon, N., 1997. Man-Made Disasters. Butterworth-Heinemann, Guildford.

Vibert, R., 2001. Emerging technology: Snaring rogue code. In: Networkmagazine, 4 May 2001, p. 1–4.

Vojak, B.A., Chambers, F.A., 2004. Roadmapping disruptive technological threats and opportunities in complex technology-based subsystems: the SAILS methodology. Technological Forecasting and Social Change 71, 121–139.

Vrijling, K.J., van Gelder, H.A.J.M., Goossens, L.H.J., Voortman, H.G., Pandey, M.D., 2004. A framework for risk criteria for critical infrastructures: fundamentals and case studies in the Netherlands. Journal of Risk Research 6, 569–579.

Ziad, I.A., 1998. Space security: possible issues and potentially solutions. Online Journal of Space Communication 6. Available from: <http://satjournal.tcom.ohiou.edu/pdf/issue6/ziad.pdf> (accessed 08.07.06.).