Critical Infrastructures under Threat: Learning from the Anthrax Scare

Arjen Boin*, Patrick Lagadec**, Erwann Michel-Kerjan*** and Werner Overdijk****

Conventional thinking in emergency and crisis management focuses on the application of codified procedures to unforeseen contingencies. Modern society's increased dependence on critical infrastructures and the emerging vulnerabilities of these large-scale networks create challenges that are hard to meet with conventional tools of crisis management. This article discusses the inherent vulnerabilities and explores the requirements of effective preparation for escalatory network breakdowns.

Introduction

From time to time, modern society is confronted with the inherent vulnerability of its critical infrastructures (Rochlin, 1997; Guilhou and Lagadec, 2002). Well known examples include the New York City blackout (1977), the Hindsale Telecommunication Center Fire in Chicago (1988), the Auckland power outage (1998), the Canadian ice storm (1998), the 'Millennium bug' (1999), and the California energy crisis (2001). The events of 11 September 2001 – soon thereafter followed by the Anthrax attacks in the U.S. and Anthrax threats in Europe – graphically illustrated the abstract writing of crisis academics, warning of emerging vulnerabilities and future contingencies.

Students of crisis describe the state of our society in terms of complex networks intertwined at the international level, marked by globalisation and mediatisation (Rosenthal, Boin and Comfort, 2001; Godard et al., 2002). The meaning of these concepts have now almost become self evident. The vulnerabilities of modern society are taken very seriously, increasingly disrupting patterns of daily life in ways that were unthinkable before those fateful 9/11 events. The security organisations routinely deal with entirely new threats, such as biological attacks (smallpox), cyber attacks and possible breaches of tunnels and metro systems. Today it is much easier understood than in the pre-9/11 world that new crises come with 'domino effects' dynamics, which cause shock waves in all directions.

It is not so clear how these modern crises should be managed. Apodictic characterisations of modern threats, future crises and inherent vulnerabilities suggest that little can be done – that is, if we do not wish to address the sources of our troubles (cf. Perrow, 1984). These challenges are hard to meet, but, we argue, they are not insurmountable.

Crisis management in the context of complex systems has never been easy (cf. LaPorte, 1975). Consider the parliamentary report following the massive oil spill that landed on the French coast line after the 1978 sinking of the *Amoco Cadiz.* The report documents patterns of structural failure in collective responses to the spill. The analysis has lost little of its relevance as we learned after the *Prestige* caused a huge environmental and social disaster in Spain last year:

> What is at issue here is a complicated system in which information is shared amongst various agents who are more or less unaware of each other, and in which any bit of information is chopped up and circulates badly. Paradoxically, the information received finally results in the ignorance of the authority with competence to act. This is a system in which one administration has powers but no material means and must request the latter from another administration, which decides whether it would be advantageous to grant them and, or inversely, an administration having material means does not receive the information that would stimulate it to use them, or does not have the power to use them. In short, this is a fractured system, deprived of any synthetic function(Colin, 1978: 223).

Two decades after the French report was published, President Clinton's Commission on Critical Infrastructure Protection (1998: ix)

*Arjen Boin, Department of Public Administration, Leiden University, P.O. Box 9555, 2300 RB Leiden, The Netherlands. E-mail: boin@fsw.leidenuniv.nl.
**Patrick Lagadec, l'École Polytechnique, Laboratoire d'Econométrie, 1 Rue Decartes, 75005 Paris, France. http://ceco.polytechnique.fr/CHERCHEURS/LAGADEC/; http://www.patricklagadec.net/.
***Erwann Michel-Kerjan, Center for Risk Management, The Wharton School, Jon Huntsman Hall, Suite 500, 3730 Walnut Street, Philadelphia, PA-19104, USA. E-mail: erwannmk@Wharton.upenn.edu.
****Werner Overdijk, Crisisplan, Frambozenweg 123, 2321 KA Leiden, The Netherlands. E-mail: crisisplan@crisisplan.nl

described the vulnerability of critical infrastructures in the following terms:

> Our national defence, economic prosperity, and quality of life have long depended on the essential services that underpin our society. These critical infrastructures – energy, banking and finance, transportation, vital human service, and telecommunications – must be viewed in the Information Age. The rapid proliferation and integration of telecommunications and computer systems have connected infrastructures to one another in a complex network of interdependence. The interlinkage has created a new dimension of vulnerability, which, when combined with an emerging constellation of threats, poses unprecedented national risk.

The core message flowing from this analysis – 'our modern societies have become increasingly vulnerable' – was echoed world wide in the face of the Millennium transition. The expected disaster never materialised and was forgotten before New Year's Day 2000 was over. The effects of the global Millennium crisis management program were neither studied or evaluated; no lessons were learned. This cannot be said of the 9/11 disaster, which has been studied from every conceivable angle.

This contribution to the JCCM special issue on the management of the Anthrax threat aims to place a very special event into a wider context. This special issue reports on the unique debriefing project conducted by La Poste and Post Europ for European and U.S. postal services in the wake of the Anthrax attacks in the United States. This contribution places this project in the context of critical infrastructures, future crises, crisis management and inventive learning methods. We begin by summarising developments in the nature of critical infrastructures and the crises that threaten to disrupt these networks. After briefly discussing the challenges of modern crisis management, we focus on what we think is an essential tool: network debriefing in the wake of critical events. We conclude with a few pointers from the Anthrax conference in Paris.

Critical Infrastructures, Classic Vulnerabilities and Future Crises

Modern society has come to depend on so-called critical infrastructures, the networks that facilitate traffic, financial transactions, communication and the delivery of water, electricity, gas and food. We depend on more networks than we probably realise. Waste disposal and sewer systems may not be classified as critical, but a two-week strike of garbage men will plunge a big city into chaos. Daily life and regular operations have become so dependent on all these infrastructures that even a slight disruption has significant consequences. The Millennium crisis is instructive in this regard. The dominant scenarios in the months leading up to the Millennium predicted, in essence, nothing more than a temporary and easy to repair breakdown of these networks. But the very threat of a few days or weeks without these networks is apparently sufficient to mobilise tremendous resources.

The networks in question have increased in size as a result of privatisation and economies of scale. They have become more complex, in order to enhance speedy delivery and improved efficiency. As more and more clients began to wear out network capacity, new technologies had to be introduced. Increased capacity nurtures dependence, which, in turn, demands more capacity. The price is a widespread loss of patience with glitches and breakdowns that interrupt service delivery. Thirty minutes without power causes problems that were unimaginable not so long ago – and are still inconceivable today in most of the world.

Critical networks, in turn, are increasingly becoming dependent on each other. The operation of any given industry may thus be thoroughly upset by a breakdown in a network that is only indirectly related to the industry in question. Small glitches in one network may cascade into large-scale breakdowns in other networks. Our livelihood is becoming a function of well operating networks.

This increased dependence on interconnected networks, and the networks' dependence on interdependent networks, have implications for the way we assess vulnerabilities in our society. It suggests that we should monitor the evolution from the traditional preoccupation with local security issues to a slowly awakening realisation that our vulnerabilities are globalising along with our modern economies. Whereas our traditional worries pertained to technological failures in localised parts of the network, we are now experiencing local disoperation as a result of natural hazards that have occurred halfway across the globe.

Normal, routine forms of adversity can rapidly develop into compound disasters, as these events 'ride' from one network to the other leaving a trail of destruction behind. A number of recent disasters show that this is more than a restatement of the 'Brazilian butterfly causes Japanese landslides' thesis, which was often heard when chaos theory was still popular. The Kobe earthquake in 1995 destroyed most of the infrastructures of the city, including its harbour (Comfort, 1999). The dependence of regional economies on the Kobe harbour (and all the Japanese trade networks connected to that harbour) contributed to the Asian monetary crisis of 1997. The January

1998 ice storm in Canada destroyed the largest part of the electrical network (over several thousand miles), deprived more than 3 million people of electricity for weeks, and caused water and gasoline shortages, communication breakdowns and traffic problems (Scanlon, 1999).

We have come to realise that terrorists may abuse our dependency on networks. Terrorism is, of course, nothing new. A major change in our sense of vulnerability comes with our understanding that terrorists may not even try to destroy a network, but rather seek ways to use the network itself as a weapon and turn it against us. The 9/11 terrorists did not seek to destroy an aircraft or the airport. They used the commercial aviation network to attack civil targets outside the system. In similar vein, the anthrax attacks were (apparently) not directed against the U.S. Postal Service. Attackers took advantage of the trusted capacity to effectively deliver *their* letters.

Crisis Management Challenges

It is easy to see how the contamination – rather than all out destruction – of our trusted life-sustaining networks may have catastrophic impacts. When we can no longer trust our mail man or incoming e-mail messages from friends, the functioning of our society comes under threat. We are facing a new dimension of potential destabilisations within industries that operate and use those networks. The social, political and economic continuity of a country may be at stake.

This observation underlines the importance of effective crisis management structures. It also begs the question whether public and private organisations are ready for the challenge. Revisiting the basic lessons derived from twenty years of crisis research suggest that there is much to be desired in this respect (Rosenthal, Charles and 't Hart, 1989; Lagadec, 2000; Rosenthal, Boin and Comfort, 2001). We see four patterns in contemporary crisis management practices that may be particularly prohibitive in protecting critical networks from disruption.

First, the very characteristics of infrastructural networks discussed above create challenges for crisis management preparedness. The Millennium operation has shown how difficult it is to distinguish between critical and non-critical networks. The interdependence between networks suggests the futility of such a distinction. The Millennium operation also displayed a fascination with hardware (technology, production lines, pipes etc.). Crisis managers tend to focus on potential violations of the hardware (fire, explosions, sabotage etc.) and very little attention to the 'human software', which is captured in the organisations running these hardwired networks. They are preoccupied with prevention and tend to forget that resilience is the key to adequate responses.

The increased scale of the networks has organisational consequences that undermine crisis management capacity. Network management in many cases has become global management. The subsequent tensions between centralised and decentralised managerial functions – headquarters in one region, the incidents tracking system in another, the crisis center in a third – breed unforeseen and ultimately unmanageable contingencies (Lagadec, 1993).

Secondly, crisis management is still predominantly a local affair. For instance, the trend in designing emergency management structures is to build them from the bottom up: local authorities begin to deal with a disaster, regional and national authorities offer assistance. Only when a disaster outpaces local capacity will regional or national authorities take over. This way of organising rests on the idea that a disaster is almost by definition local in nature. This way of organising corresponds nicely with modern management practices in the public sector – generally known under the New Public Management label – which prescribe autonomy for street-level bureaucracies.

The situation in the private sector may be better than in the public sector, but the level of preparation is generally low. In many large corporations, executives still do not take crisis management seriously and leave that to lower ranked technicians (Lagadec, 2000). Crisis management plans concentrate on prerequisites for business continuity management and prepare for the occasional fraud and recall procedure. Very few corporations can explain what crisis management philosophy they have, because they do not have one.

These are worrying observations, as crisis challenges are shifting to the systemic level. Local disturbances have immediate consequences for the system in which they occur, but also in connected systems. Where usual crisis management procedures used to be effective in isolating difficulties within a system, the very concept of isolation has become obsolete. Once the system is infected, all borders are crossed at unbelievable speed. Local governments are used to deal with the usual actors in a relatively well-known theatre of operations; systemic crises force local authorities into unknown (foreign) theatres with different actors. It is not clear what the trend is among private corporations. The recent system crises have exposed many corporations as conservative, blindsided and overall rather powerless in their dealings with 'external' shocks.

A third characteristic of contemporary crisis management patterns is the long-time reliance on rational planning procedures. Crisis manage-

ment has long been approached in terms of finding or generating certainties for emerging uncertainty. If a crisis meant that the basic references did no longer suffice to deal with a situation, crisis management aimed to bring in new solutions. Crisis management is akin to urgent trouble shooting – 'Houston, we have a problem' – and effective crisis managers are particularly adroit at co-ordinating that process. During a crisis, crisis managers routinely rely on the advice of experts. But in systemic disruptions of critical infrastructures, basic references of experts are frequently shattered. When BSE (Mad Cow Disease) emerged in the UK, the experts of the European Union could not even agree on the nature of the problem (Gronvall, 2001).

Good crisis managers are trained to communicate with key audiences. Their training tells them to communicate the facts and to lessen anxiety among citizens and customers. But communication becomes potentially self-defeating in the absence of hard facts and a clear understanding of cascading dynamics. These processes have no clear beginning, no chief cause (the proverbial individual error), no manageable consequences. Hence it becomes impossible to prove that nothing is wrong or that a risk does not exist, which boosts anxiety and fuels pre-emptive reactions. Soon the vicious cycle feeds on the ill-fated interventions of well-trained crisis managers.

The combination of inherent vulnerabilities in critical infrastructures and outdated crisis modes does not bode well for the large organisations that typically 'run' the infrastructures. During a breakdown, the very products of rational management – beautifully engineered and tightly connected networks; lean and mean organisations; long-term crisis planning – become the modifiers of cascading crises (Turner and Pidgeon, 1997). What we see is perplexed crisis managers: everything seems too complex, too novel, too rapid; it's snowballing out of control. Text-book crisis techniques do not work anymore. As a result, the public is shocked and feels betrayed when discovering that people in charge do not have the capacity to act. Infrastructural breakdowns can thus easily trigger an institutional crisis, separating society from its leaders (Boin and 't Hart, 2003). The lines between crisis management and strategic management begin to blur, as the requisites for strategic management closely resemble those of effective crisis management:

> At least 90% of textbooks on strategic management are devoted to that part of the management task which is relatively easy: the running of the organisational machine in as surprise-free a way as possible. On the contrary, the real management task is that of handling the exceptions, coping with and even using unpredictability, clashing counter-cultures. The task has to do with instability, irregularity, difference and disorder(Stacey, 1996: xix-xx).

Fourth, crisis management preparation is in too many organisations still only a paper reality. Elaborate plans nicely describe procedures, exercises, scenarios, organisational structures, competences and responsibilities. Such plans contribute to the pervasive but false belief that the network organisations are well prepared for crisis (Clarke, 1999). But they have never been tested and the question is whether they will hold up in the actual event of network disruption.

Meeting the Challenge

There is, obviously, no clear-cut framework to deal with these new threats to modern society. Unless we rid our societies of critical networks (cf. Perrow, 1984), we must try to develop a crisis management paradigm that fits modern management practice and helps to mediate the unintended consequences of this modernity. In the past years – particularly in the upswing toward the Millennium threat – much work has been done in this regard. In this section, we outline three basic requirements for new managerial responses to these new crises dynamics (cf. Boin and Lagadec, 2000).

Towards Understanding Evolving Crisis Dynamics

There are crisis managers who still cling to the irresponsible idea that crises are rare occurrences without any real consequences for the long-term operation of the networks. This type of blissful ignorance is unlikely to persist within large corporations, if only because crises in infrastructural networks bring organisations down. But it is important to understand that traditional crisis preparations are becoming dysfunctional as well: crisis managers can no longer pretend that they are capable of rational crisis management, which would consist of recognising and defining a crisis, selecting the corresponding crisis scenario and applying the programmed response to the situation at hand. This amounts to dangerous wishful thinking (Clarke, 1999).

It is crucial, therefore, that the administrative elites of public and private companies begin to understand that crises tend to be rapidly emerging and evolving processes that can turn into vicious and unmanageable circles. Top executives must be prepared to deal with emerging vulnerabilities in the networks they manage and in those networks their home organisation is

(in)directly connected to. Crises cannot simply be delegated to technical teams, but must involve the responsibility of the highest officials. The stakes have become so high and the need for strategic, crucial decision making is so intense that crisis management response should no longer be a question for specialists, scientific experts and communication officers only.

Preparing for the Unpleasant and Unexpected Unknowns

The vulnerabilities discussed in this article and special issue may appear new, but that is more a function of interest than a true picture. The rise of modern and dangerous technologies has been accompanied by warnings of destructive side effects (Perrow, 1984). The reliance on rational management practices to deal with these modern technologies has been shown to be rather optimistic (Turner and Pidgeon, 1997). Yet, the predicted chaos and mayhem has never quite materialised. The Millennium syndrome seemed to prove that technological progress could be managed and controlled. Perhaps we should march ahead and accept a crisis here and there as the price to pay for progress in safety (Wildavsky, 1988).

Both the optimistic (nothing really bad will happen) and pessimistic (there is nothing we can do when it happens) perspectives leave crisis managers grossly unprepared. As a result, crisis managers are left with only extreme alternatives. In the event of a system breakdown, network managers can either shut down the network (limiting the diffusion effect, but with heavy consequences for many people) or continue to operate with the possibility that the network capacity will be redirected against the users of the network.

Crisis management will have to be based on the premise of resilience: learning to organise for the unknown. Scenarios and decision support systems will not do. Organisations will have to rely on the expertise of their operators who know the networks and understand the cascading dynamics of breakdowns. In their search for effective organisational cultures, crisis managers may learn from so-called high reliability organisations in which resilience has been embedded into the finest veins of the organisation, thus limiting both the potential impact and chances of network breakdowns.

Learning from Each Other's Critical Experiences

Once crisis managers realise that crises cannot be viewed as 'local' events, the next step is to look to other organisations and networks to learn from their experience. Such collective efforts can take three forms. First, there is post-event learning. Crisis managers share their experiences in managing a particular breakdown episode. They present best practices and explain errors with unexpected consequences. A second form is prevention learning: they seek to gain better understanding of initiatives launched in other sectors or countries, which may possibly serve as a framework of action for their own organisation (if only to begin with). A third form is a mixture of the other two. It relates to collective initiatives to work on identified issues through the elaboration of networks of people susceptible to share *ex ante* and work quickly together when safety breaches occur. These ostensibly simple learning forms require changes that amount to cultural revolutions in many public and private organisations. Organisational leaders must try to:

- involve and engage with new stakeholders from within but in particular from the wider environment in order to improve its information position, to develop relationships and fast connections, to learn about organisational cultures in connected networks.
- adapt communication cultures within the organisation: opening up to questions rather than trying to provide definite answers; nurturing collective sensemaking processes without demanding immediate positive results (which may emerge after severe delays).
- introduce and develop strategic intelligence teams that advise top leaders, formulate contra-fashionable questions, suggest bold innovations, engage with multiple bodies outside.
- organise structural debriefings: each and every difficult experience must be exploited as an opportunity to improve collective know-how. Debriefing must be required for directors and surpass mere technical feedback.
- run simulation exercises: non-trained organisations have the greatest difficulties in taking charge of abnormal situations. Continuous practise is required to deal with surprises. Simulations can take many forms and are becoming increasingly creative and smart. Simulations must be followed by rigorous debriefings ('t Hart, 1997).
- introduce training programs aimed at 'specific perfection'. In addition to creating a generic crisis culture, it is crucial to train certain officials to carry out their crisis functions in very specific ways. The most delicate roles include leaders, crisis team facilitators, 'strategic observers' (whose role it is to reflect on the crisis during the crisis, reporting to the strategic level), spokespersons, the experts (who will suddenly be expected to provide elements of judgement in the face of glaring television cameras).

'Anthrax and Beyond': Hallmark in International Crisis Learning

In the fall of 2001, the U.S. Postal Service was confronted with deadly Anthrax attacks. The postal services in nearly all European countries were confronted with thousands of alarms; false alarms, as it turned out, but with instant disruptive effects. Each postal operator has organised its own debriefing and evaluation operation. At the Paris conference in November 2002, representatives of most postal services joined in Paris and launched an inter-organisational learning process to share experience and lessons, to share ideas to improve the collective capacity in handling crisis events, and to launch a structural network that may facilitate joined reaction capability within Europe and across the Atlantic.

These are timely efforts. The severe crises that emerge on the horizon of our complex societies require entirely new logics of preparation, response and repair. Leadership on both the organisational and political level is an essential factor in driving the development, adopting and overseeing the implementation of such new crisis logics. Lack of leadership translates into unpreparedness, which fuels the type of escalatory network breakdowns discussed in this article.

Crisis management thus falls within the leadership domain, whether leaders like it or not (Boin and 't Hart, 2003). Today's role example of leadership involvement is Rudolph Giuliani, who intensely involved himself in crisis exercises as mayor of New York City (Giuliani, 2002). We may well ask how many mayors, ministers and other CEOs have actively participated in similar efforts. The Paris conference is remarkable in this sense, as it was built on the personal involvement of top-level postal executives.

The participants of this conference, which represents a real breakthrough in international preparation and partnerships' development to deal with emerging large-scale vulnerabilities, showed a clear desire to learn from each other's crisis management experiences. In the contributions to this special issue, they present their insights to a broader audience. The report of this conference should serve as a source of inspiration for key executives in charge of the infrastructural networks we depend on.

References

Boin, R.A. and 't Hart, P. (2003), 'Public Leadership in Times of Crisis: Mission Impossible', *Public Administration Review*, forthcoming.

Boin, R.A. and Lagadec, P. (2000), 'Preparing for the Future: Critical Challenges in Crisis Management', *Journal of Contingencies and Crisis Management*, Volume 8, number 4, December, pp. 185–191.

Clarke, L. (1999), *Mission Improbable: Using Fantasy Documents to Tame Disaster*, University of Chicago Press, Chicago.

Colin, A. (1978), *Rapport de la Commission d'enquête du Sénat*, seconde session ordinaire 1977–1978, no 486.

Comfort, L. (1999), *Shared Risk: Complex Systems in Seismic Response*, Pergamon Press, London.

Giuliani, R. (2002), *Leadership*, Miramax Books, New York.

Godard, O., Henry, C., Lagadec, P. and Michel-Kerjan, E. (2002), *Traité des nouveaux risques: Précaution, Crise, Assurance*, Gallimard, Foliot actuel, Paris.

Grönvall, J. (2001), 'Mad Cow Disease: The Role of Experts and European Crisis Management', in Rosenthal, U., Boin, R.A. and Comfort, L. (Eds), *Managing Crises: Threats, Dilemmas and Opportunities*, Charles C Thomas, Springfield, pp. 155–174.

Guilhou, X. and Lagadec, P. (2002), *La Fin du risque zéro*, Eyrolles, Paris.

't Hart, P. (1997), 'Preparing Policy Makers for Crisis Management: The Role of Simulations', *Journal of Contingencies and Crisis Management*, Volume 5, number 4, December, pp. 207–215.

Lagadec, P. (1993), *Preventing Chaos in a Crisis*, McGraw Hill, London.

Lagadec, P. (2000), *Ruptures créatrices*, Editions d'Organisation-Les Echos Editions.

LaPorte, T.R. (1975), *Organizational Social Complexity: Challenge to Politics and Policy*, Princeton University Press, Princeton.

Perrow, C. (1984), *Normal Accidents: Living with High-Risk Technologies*, Basic Books, New York.

President Clinton's Commission on Critical Infrastructure Protection (1998), *Critical Foundations, Protecting America's Infrastructures*, Washington D.C.

Rochlin, G.I. (1997), *Trapped in the Net: The Unanticipated Consequences of Computerization*, Princeton University Press, Princeton.

Rosenthal, U., Charles, M.T. and 't Hart, P. (Eds) (1989), *Coping with Crises: The Management of Disasters, Riots and Terrorism*, Charles C Thomas, Springfield.

Rosenthal, U., Boin, R.A. and Comfort, L. (Eds) (2001), *Managing Crises: Threats, Dilemmas and Opportunities*, Charles C Thomas, Springfield.

Scanlon, J. (1999), 'Emergent Groups in Established Frameworks: Ottawa Carleton's Response to the 1998 Ice Disaster', *Journal of Contingencies and Crisis Management*, Volume 7, Number 1, pp. 30–37.

Stacey, R. (1996), *Strategic Management & Organizational Dynamics*, Pitman, London.

Turner, B.A. and Pidgeon, N.F. (1997), *Man-made Disasters*, Butterworth-Heinemann, Oxford.

Wildavsky, A. (1988), *Searching for Safety*, Transaction Books, New Brunswick.