

Meeting the Challenge of Interdependent Critical Networks under Threat : The Paris Initiative

Erwann Michel-Kerjan, Patrick Lagadec

▶ **To cite this version:**

Erwann Michel-Kerjan, Patrick Lagadec. Meeting the Challenge of Interdependent Critical Networks under Threat : The Paris Initiative. 2004. ⟨hal-00242926⟩

HAL Id: hal-00242926

https://hal.science/hal-00242926v1

Preprint submitted on 6 Feb 2008

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



HAL Authorization

ECOLE POLYTECHNIQUE

CENTRE NATIONAL DE LA RECHERCHE SCIENTIFIQUE

Meeting the Challenge of Interdependent Critical Networks under Threat : The Paris Initiative, "Anthrax and Beyond"

Patrick LAGADEC
Erwann MICHEL-KERJAN

June 2004

Cahier n° 2004-014

LABORATOIRE D'ECONOMETRIE
1rue Descartes F-75005 Paris
(33) 1 55558215
http://ceco.polytechnique.fr/
mailto:labecox@poly.polytechnique.fr

Meeting the Challenge of Interdependent Critical Networks under Threat : The Paris Initiative, "Anthrax and Beyond"[1]

Patrick LAGADEC[2]
Erwann MICHEL-KERJAN[3]

June 2004

Cahier n° 2004-014

Abstract: The growing globalization of activities translates into large-scale area of operation, just-in-time processes and increasing interdependencies among national and international networks. Combined with the emergence of a wide spectrum of threats - sabotage, terrorism, disease, natural disasters- one faces a whole new arena of large-scale emerging risks and crises involving critical networks in which failure to operate can have debilitating impacts on an entire country and even abroad.

Strategic and operational answers have to be developed to deal with such events and improve collective preparation through the creation of specific partnerships.

In the aftermath of 2001 Anthrax crisis we suggested launching an ambitious debriefing process on the Anthrax episode: a large pilot study, with a clear strategic view consisting on bringing some hallmarks to help postal operators at the highest executive level.

This led to the "Paris Initiative", with senior executives of postal sectors from 30 countries meeting in Paris one year after the international crisis to share their experience gained throughout this "out of the box" episode and suggest new avenues of international partnerships. An innovative international platform for immediate cross-organizational response capacity resulted from that initiative too; a partnership enabling the necessary common learning process. To date postal operators have been among the very few to launch such an innovative process to understand and meet the collective challenge of an increasingly interdependent world.

After discussing some key challenges associated with the operation of critical networks today as well as some behavioral barriers and financial issues associated with the development of an adequate set of possible actions by top decision-makers, this paper presents the Paris Initiative in more detail (challenges, preparation, choice of a strategic team within and outside organizations, success through measurable outputs).

Beyond this specific pilot initiative, some strategic clues are suggested for successfully applying the developed framework to other critical sectors.

Appendix 1: Strategic Check-List for Senior Executives

Mots clés : Risques à grande échelle - Gestion de Crise internationale - Interdépendances - Infrastructures critiques - Anthrax - Initiative collective - Stratégie - Préparation des états-majors -

Key Words : Large-scale Risks - International Crisis Management - Interdependencies - Critical Infrastructures Anthrax - Senior Executives Preparedness - Board's Strategy - Collective Initiative

Classification JEL: D78; D81; L21; L9; L87; M13; M14

---

[1] We thank participants at the Foundation for Strategic Research's workshop on «Hyperterrorism and Europe: Threats, Vulnerabilities and Responses » in Paris, the Lawrence Livermore National Laboratory «Leaving with Risk» workshop in Boston, the 12th Conference on Postal and Delivery Economics in Cork, Ireland and at the GMU-Harvard «Private efficiency, Public vulnerability» workshop in Boston, Harvard University's Kennedy School, for helpful discussions on related issues and comments on the paper.

This cahier will appear during the Summer of 2004 also as a Wharton Risk Center working paper, WP # 04-28.

[2] Ecole polytechnique, Laboratoire d'économétrie, 1 rue Descartes, 75005 Paris, France. and European Crisis Management Academy. Email: plagadec@club-internet.fr ; Web site: www.patricklagadec.net

[3] The Wharton School, Center for Risk Management and Decision Processes, Jon Huntsman Hall, Suite 500, 3730 Walnut Street, Philadelphia, PA 19104, United States and Ecole polytechnique, Laboratoire d'économétrie, 1 rue Descartes, 75005 Paris, France. Emails: erwannmk@Wharton.upenn.edu / erwannmk@poly.polytechnique.fr ; Web site: http://grace.wharton.upenn.edu/risk/ (Wharton Risk Center).

1. Introductory Overview

September 11, 2001, and the global rules are torn apart. This is the most dramatic, but not the only facet of the risk arena. One jet-propelled SARS contamination and public health paradigms have to be revisited all over the world. One technical incident in the power grid in August, 2003 – "a 9-10 second event" and a quarter of North America is plunged into the dark, the same in Italy a few weeks later. One mad cow and the US meat market teeters within 24 hours. March 11, 2004, and the whole European vision of homeland security has to be changed. Not a month goes by without a very unforeseeable crisis hitting the headlines. A few Anthrax-contaminated envelopes in the United States during the autumn of 2001, and the international postal system is under threat.

The new web of challenges organizations now face is made of "unconventional" events, reflecting more than mere specific and local incidents, but rather global turbulences, real-time large-scale risks, and out-of-scale domino effects in an increasingly interdependent world where the actions of one organization can have a direct impact on others thousands of miles away.

This paper focuses on how strategic partnerships within a specific industry can be developed at the senior-executive level and internationally so as to better prepare organizations in managing and financing these types of emerging risks. While concentrating on postal security in the aftermath of the Anthrax crisis, the arguments and the spirit of the Paris Initiative itself go far beyond and could be applied with benefit to other critical sectors.

In the aftermath of the Anthrax crisis during the autumn of 2001 that raised fundamental questions on postal security world wide, we suggested launching an international debriefing process on the Anthrax episode. Our strategic goal was clear: (a) to bring some hallmarks to help postal operators at the highest executive level meet a double-challenge; (b) to understand the new arena of emerging vulnerabilities and (c) to prepare creative operational breakthroughs that are seen as crucial for the global sustainability and development of postal operations in the future.

Initially this project was supposed to be undertaken for a few postal operators (France, Germany, the Netherlands, the United Kingdom, among others). Eventually we ended with the preparation and implementation of an international initiative involving nearly 30 countries across Europe and the United States as well as international organizations within the postal sector. The *Paris Conference "Anthrax and Beyond",* prepared over the course of eight months, took place in France in November 2002, one year after the international postal crisis.

This two-day meeting was set also to constitute the take-off step of an international partnership among postal operators, with the creation of a global crisis management network (among other outputs). This new network had its first test on January 15, 2003, the day it became operational, when the U.S. Postal Service was concerned by a possible anthrax contamination in the Washington, D.C. area.

This paper focuses on how this initiative came to be organized, starting with a small team and building on a positive tipping effect among postal operators and international organizations. It also illustrates the crucial importance for the success of the whole operation of having a core team made of people **both** from inside the partner organizations (CEO-like level) **as well as** outside these organizations who can bring a broader perspective on strategic elements and act as catalysts of the operation.

Let us be very clear in this introduction. Partnership is a brilliant concept. The practice of partnership is another matter. In the case of postal sector after the Anthrax attacks, our strategic line was, inside postal organizations, to visit people in charge in various postal services, to listen to them, and to suggest to them the initiative; outside postal organizations, to visit other international experts in the field, to suggest that initiative and constitute a core team. It was also important to involve international postal organizations, such as PostEurop, from the outset.

The proposed line of action was ambitious: a breakthrough in practice, an international debriefing, followed by concrete outputs that could be meaningful for postal industry. Moreover, from the beginning we suggested a high level goal: the publication of key features of the process and best results by a leading journal in the field. Not publicity, but rather a real step forward in the debriefing experience among operators of a critical network such as the postal service. As the success of this project was largely due to the commitment of several key decision-makers within postal organizations, it was crucial to diffuse the knowledge and insights gathered in that effort. This was the ambition of a special issue of the *Journal of Contingencies and Crisis Management*, published in autumn 2003, just one year after the Paris Conference[1]. All of that was done successfully[2].

Postal operators have been among the very few to launch an innovative process to understand and meet the collective challenge of an increasingly interdependent world confronted by the emergence of a new spectrum of threats. Hence, there is a large benefit in analyzing this breakthrough, and in suggesting a decisive move beyond the postal sector.

---

[1] Lagadec, Patrick and Rosenthal, Uriel (eds.) (2003). "Anthrax and Beyond: New Challenges, New Responsibilities", *Journal of Contingencies and Crisis Management*, Special Issue, Volume 11, Number 3, September 2003.

[2] That is not so common. For example, we approached the airline-airport industry after the SARS epidemics to launch a similar initiative. The project, however, never emerged from "great interest but no decisive move".

This paper is organized as follows. **Section 2** discusses some key challenges associated with the operation of critical networks today[3]: high level of surprise (even inconceivability) and scientific uncertainty (even ignorance), increasing interdependencies among networks worldwide and large-scale events capable of inflicting severe long-term economic and social consequences. **Section 3** discusses some intellectual, training, and behavioral barriers as well as financial issues associated with these extreme events. These barriers need to be considered in order to develop an adequate set of actions for top decision-makers.

Section 4 presents the Paris Initiative in more detail. Contributors to the aforementioned special issue are senior executives from postal operators and academic experts in the field of catastrophic risks and crisis management who played a key role in that project. In that spirit, we quote them voluntarily in this section to plunge the reader into the hot waters of the real world of crises. This aims to provide a broader view on this initiative and to reckon a collective action. This section suggests also some key lessons that could be taken away from this initiative and be applied to other industries. **Section 5** concludes and indicates some new avenues.

2. A Whole New Ball Game of Large-scale Risks and Crises

The first and crucial step is to understand that governments, industry leaders and citizenry are now confronted with a new world of risks. Most are of large magnitude, high speed, non-linearity, discontinuity. Just a few recent references are enough to have the new radar screen well in mind:

- Ice Storm, South Quebec, January 1998: " We were prepared for a technical breakdown. We were confronted by a network collapse." (Hydro Québec senior executives).
- BSE, UK, 1986-1996: " By the time that BSE was identified as a new disease, as many as 50,000 cattle are likely to have been infected. Given the practice of pooling and recycling cattle remains in animal feed, this sequence of events flowed inevitably from the first case of BSE " [4];
- SARS crisis, 2003: "a worldwide threat "; "The possibility of undetectable ill people." (WHO);
- Heat Wave, France, August 2003; 15,000 people died: " We did not know anything " (Minister of Health);
- U.S. power blackout, 14th August 2003: " This whole event was essentially a 9-second event, maybe 10 " (Michel R. Gent, president and CEO, North American Electric Reliability Council[5]).

[3] By "critical networks" we mean networks that support the economic and social continuity of a country: vital human services (supply of water, food; public health), energy (electricity, oil and natural gas), information and telecommunications, physical transportation (airports, ports, train; postal services) and banking and finance, among others.

[4] Lord Phillips, J. Bridgeman and M. Ferguson-Smith. (2001). *The BSE Inquiry, vol 1. Findings and Conclusions*, London, Stationary Office, October 2000, § 110.

[5] *The New York Times,* Saturday, August 16, 2003, p. 1.

Risks and crises became much more complex over the past years on at least three levels:

- (1) from well studied risks to a *high level of surprise and scientific ignorance*;
- (2) within an *increasing interdependent world*, globalization of social and economic activities leading to a globalization of risks among critical networks;
- (3) from more local accidents within a single firm or industry to *large-scale events or threats* that go more systematically beyond traditional frontiers, across firms, across industries, and cross countries, mixing interests from public and private sectors as well as civil society, with potential losses exceeding the capacities of insurance frameworks[6].

High level of surprise and scientific ignorance

"We must be constantly aware of the likelihood of malfunctions and errors. Without a command of probability theory and other instruments of risk management, engineers could never have designed the great bridges that span our widest rivers, homes would still be heated by fireplaces or parlor stoves, electric power utilities would not exist, polio would still be maiming children, no airplanes would fly, and space travel would just be a dream".[7]

These lines from a bestseller in this field tell the positive vision of the evolution of risks and risk management. From time to time, however, some errors and malfunctions create real breakdowns as stated by Bernstein quoting Leibniz (1703): "Nature has established patterns originating in the return of events, but only for the most part". And Bernstein goes on: "Despite the many ingenious tools created […], much remains unsolved. Discontinuities, irregularities and volatilities seem to be proliferating, rather than diminishing." [8]. Those changes raise some key questions. One was used to anticipate and handle "normal breakdowns"; the society is confronted now more regularly with extreme phenomena. People in charge used to rely on judgments of experts. Unfortunately, those extreme events appear mostly over a short period – not enough time for experts in the scientific community to provide decision makers with precise and well-established knowledge; i.e. scientific uncertainty and even ignorance– which increases the capacity of these events to destabilize the social, economic and political continuity of countries. Accordingly, surprise becomes "normal factor".

---

[6] Among recent analyses of catastrophe risk coverage, see Godard, Olivier, Henry, Claude, Lagadec, Patrick and Michel-Kerjan, Erwann. (2002). *Treatise on New Risks. Precaution, Crisis, and Insurance.* Paris: Gallimard, Folio-Actuel; Grace, Martin, Klein, Robert, Kleindorfer, Paul and Murray, Michael. (2003). *Catastrophe Insurance.* Boston: Kluwer. On terrorism risk coverage, see Kunreuther, Howard and Michel-Kerjan, Erwann. (2004). *Insurability of (Mega)-Terrorism: Challenges and Perspectives.* Report for the OECD Task force on Terrorism Insurance. Paris: OECD.

[7] Bernstein, Peter L. (1996). *Against The Gods. The Remarkable Story of Risk.* New York: John Wiley & Sons, p. 2.

[8] Berstein, ibid. p. 329.

Moreover, when dealing with terrorism or malevolent threats, the nature of the uncertainty also reflects an important difference from other sources of risks (e.g., natural hazards, technological failure). Since attackers will adapt their strategy as a function of their resources and their knowledge of the vulnerability of the entity they are attacking, the risk is thus the equilibrium resulting from a complex mix of strategies and counterstrategies developed by a range of stakeholders. The nature of the risk changes over time and it is continuously evolving, which leads to *dynamic uncertainty.*[9]

This dynamic uncertainty also makes efforts to quantitatively model the risk more challenging. One deals with a short of dynamic game where the actions of the terrorist groups in period *t* is dependent on the actions taken by those threatened by the terrorists (i.e. the defenders) period *t-1*. For example, terrorism risk will change depending on the protective measures adopted by others (including firms potentially at risk) as well as actions taken by governments. In that regard, strategy to deal with these risks is a mixed public-private good, which poses real challenges in coordinating actions by the private and public sectors and in doing so in several countries at the same time.

An Increasing Interdependent World: The Network Factor

Increasingly, the dominant features of these risks and crises are the set of vulnerabilities associated with the *network factor* in a global world. By "network factor" we mean an *increasing dependence of social and economic activities on the operation of networks, combined with increasing interdependencies among theses networks.*

Indeed, there is a paradox. From a technological perspective, important progress has been made in engineering and operation management so as to obtain better quality and robustness of large infrastructures as well as just-in-time delivery. In parallel to these improvements, the use of large-size network and their interconnections allowed a reduction in operating cost thanks to economies of scale. On the other hand, when these large-scale networks fail, the consequences immediately affect a large number of people and firms, as well as, by cascading effect, other networks. So is it important to consider not only direct risks susceptible to limit networks' operation (e.g., natural disasters or internal technological failure) but also increasing interdependencies among several networks, i.e. indirect risks. In other words, large networks induce large risks associated with their potential failure to operate; large interdependent networks can have even worse consequences associated with them.

[9] Michel-Kerjan, Erwann. (2003). "Large-scale Terrorism: Risk Sharing and Public Policy." *Revue d'Economie Politique.* 113: 5, pp. 625-648.

As remarkably diagnosed as early as 1998 by a U.S. Presidential commission, " 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 telecommunication and computer systems have connected infrastructures to one another in a complex network of interdependence. This interlinkage has created a new dimension of vulnerability, which, when combined with an emerging constellation of threats, poses unprecedented national risk ".[10]

Modern society has come to depend more and more on critical infrastructures.[11] Networks have become more complex and hence more susceptible to several sources of interdependent risks.[12] Privatisation also could have an impact in some cases on the vulnerability of a whole system as security investments might be reduced continuously to meet competitiveness challenges.[13]

Large-scale Risks: Reversing Network Capacity against Populations

These large systems of networks are now embedded in a new violent and torn context. Terrorist or malevolent groups seeking to inflict large-scale attacks by *reversing the network capacity* against populations can use the large networks with high capacity of distribution. The dynamics have to be rightly understood. Terrorists may not even try to destroy physically some elements of a network infrastructure, but rather seek ways *to use the huge diffusion capacity of our own networks as a weapon.*[14]

In that regard, the 9/11 events and the anthrax attacks during the fall of 2001 demonstrated this new kind of vulnerability. In these two cases, attackers used the diffusion capacity of a critical network and turned it against the U.S. population so that each element of the network (e.g. every aircraft, every piece of mail) then became a potential weapon.

---

[10] President's Commission on Critical Infrastructure Protection. (1998). *Critical Foundations, Protecting America's Infrastructures*, Washington D.C., p. ix. The US Presidential initiative launched by President Clinton in 1996 was the first initiative world wide to put the issues of protection of critical infrastructures on the top-level agenda of the public and private sectors.

[11] Boin, Arjen, Lagadec, Patrick, Michel-Kerjan, Erwann and Overdijk, Werner. (2003). "Critical Infrastructures under Threat: Learning from the Anthrax Scare », *Journal of Contingencies and Crisis Management*, Volume 11, Number 3, p. 99-104.

[12] And in fact 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; and the BSE has shown that garbage could be the key way for global contamination.

[13] For example, that was the main cause of severe difficulties that occurred because of cold weather in Paris Airport Hub on January 4-5, 2003, each airline having its own contracting parties for de-icing, each of those sub-companies being unprepared to act alone in unconventional situations; some airlines have nobody or very few people able to take charge in case of such a chaotic situation.

[14] Michel-Kerjan, Erwann. (2003). "New Challenges in Critical Infrastructures: A U.S. Perspective". *Journal of Contingencies and Crisis Management*. Volume 11, Number 3, September 2003, p. 132-141.

The 9/11 terrorists did not seek to destroy an aircraft or a specific airport. They used the commercial aviation network to attack civil targets outside the system (every aircraft becoming potentially at risk). As the number of hijacked planes on 9/11 was not known and each flying aircraft was a potential danger, the U.S. Federal Aviation Administration (FAA) ordered all private and commercial flights grounded less than one hour after the first aircraft crashed against the North WTC Tower. It was on September 12th 2001 that they were authorized to resume their flights. It was the first time that the FAA has ever shut down the airline system[15].

During the anthrax episode in autumn 2001, the attacks were not turned against a specific postal office either. Rather, the attackers took advantage of the whole United States Postal Service network to spread threats throughout the country and abroad by taking advantage of the trusted capacity of the mail to effectively deliver *their* letters. Any envelope could have been considered contaminated by anthrax, so the whole postal service was potentially at risk. The question as to whether the postal service itself was contaminated and whether it should be down entirely was considered seriously[16]. Shutting down a large-scale network such as the U.S. Postal Service, the officials knew, would inflict debilitating impacts on the economic and social continuity of the country as well as increase stress on the already sensitive psyche of the nation under siege. As stopping the postal service would not have prevented future contamination if the whole system were already contaminated[17] –one day, it would have been necessary to reopen it– the network was not closed.[18]

These events raised fundamental questions for the security of national infrastructures not only in the U.S. but also at the international level. As warned as early as 1978, " It has been rather misleading and unfortunate that the academic study of crisis management was initiated chiefly by the Cuba missile crisis in 1962 […] It appeared to approximate to the form of a 'two-person game'. […] The episode really did look rather like a diplomatic chess game […]. If there is a 'game' model for crisis, it [is] certainly not chess, but poker for five or six hands in the traditional Wild West saloon, with the participants all wearing guns, and quickness on the draw rather than the fall of the diplomatic cards tending to determine who eventually acquire the jackpot ".[19]

---

[15] Recently, the 3/11 terrorists in Madrid followed the same configuration of attack –reversing network capacity against populations– as they probably tried to use the rail network to destroy not some scattered trains but a key station of Madrid grid.

[16] Lipton, E. and Johnson, K. (2001). "Tracking Bioterrorism's Tangled Course". *New York Times Magazine*, December 26.

[17] The USPS delivers nearly 700 million pieces of mail every day; stopping the whole service for one week, so as to better understand the situation, would have implied 4 billion delayed pieces.

[18] For an analysis of the impact of anthrax crisis on long-term strategic aspects of the USPS's operation, see Reisner, Robert. (2002). "Homeland Security Brings Ratepayers vs. Taxpayers To Center Stage", in Crew and Kleindorfer (eds.), *Postal and Delivery Services. Delivering on Competition.* Kluwer Academic Publishers: Boston, pp.223-242.

[19] Bell, Coral M. (1978). "Decision-making by governments in crisis situations", in D. Frei (ed.) *International Crises and Crisis Management. An East-West Symposium.* Praeger Publishers, New York, p.50-58.

The warning takes its full meaning just now. A simple but crucial question is to know how collective preparedness for top-decision making can be improved for dealing with these emerging risks.

3. Making Top Decisions: Getting over Myths

All this has direct implication on the way crises have to be addressed. Two related points need to be considered as well. First, there is increasing fuzziness. For example, the city of Toulouse in France was severely damaged by a colossal industrial explosion, ten days exactly after 9/11. Two and a half years after this tragedy it is still unclear if this event falls into the "industrial disaster" or a "terrorist attack" category[20]. In the same vein, it took a long time to clarify the origin and causes of the 2003 US-Canadian power blackout, referred to in the introduction.

Second, the business world is spread over several locations: headquarters in one region, the incident tracking system in another, the crisis centre in a third – with very different frameworks of decision-making in each and every other actor involved. This limits simple decision rules if not implemented collectively before something happens. As witnessed with SARS, people in charge are instantly confronted by a maze of various dimensions of combined scientific, technical, organizational, economic, diplomatic, and cultural issues.

In that regard, three crucial lines of challenges are to be acknowledged and dealt with to make top decision in the difficult context: intellectual challenges, training and behavioural challenges, and financial challenges.

An Intellectual Challenge: **From Linearity to Discontinuity.**

Decision-makers have to appreciate how far these situations are from the usual references:

- *Out-of-scale gravity*: the usual scales suddenly appear outdated; one needs to think global.
- *Indeterminate gravity*: the mere impossibility of clarifying the potential seriousness of a suspected threat. One already had to face, as in the BSE case, situations when it is even impossible to determine whether you are confronted with a "non-event", a medium range problem compared to others, by a real potential disaster, or a new Great Plague or other catastrophe to Mankind; What level of decision could be made then?
- *Meaningless probability*: the notion of probability, in a statistical sense, loses sense for emerging risks (no data available). What is the probability of a terrorist attack using

[20] The distinction does not only affect national security issues but also on insurance aspects.

weapons of mass destruction next week in London, Rome, Philadelphia or Tokyo? [21] ; of a class 3 hurricane in New York?; of an original heat wave for a whole month over Europe, a long-lasting polar weather episode in a so-called temperate zone?

- *Real time*: many people are trained to react swiftly to a well-specified situation (in space and time), but how can they successfully respond independently to dramatic speedy events, at international scale, with no scientific consensus available (impossible to know where, when, who, why, for sure)?
- *Unknown maps*: potential actors are numerous, immense voids in organisational systems, key conventional actors become marginal, unknown actors become central.[22]
- *Shattering references*: in a period of crisis, the visions, the frameworks, the measurements one thought stable and that allowed thinking and operating do not work anymore, to a large extent.

Each dimension justifies new intellectual approaches and research. As discussed, there is a common point to all of these: *discontinuity, meaning a fault line, splitting radically different worlds.* Our intellectual tradition poorly incorporates these non-linear jumps, mutations, snowballing effects, etc. We are so wonderfully trained to the world of stability, linearity, limited uncertainty at the margin, partitioned theatres of operation and optimisation under a few well shared and accepted constraints. Those emerging critical contexts, most of which are unstable by nature, may be far beyond our understanding capacities. Research has an urgent mission to fulfil in that essential respect. As Hegel said: "If you are confronted by unthinkable challenges, you have to invent unthinkable paradigms".

A Training and Behavioral Challenge

Thinking and training out of the box. As the point was clearly stated, "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 organizational 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

[21] The recent development of terrorism models assists in the risk assessment process but it is difficult to estimate the likelihood of future terrorist attacks given our current state of knowledge. Although none of the terrorist models currently provides well-specified distributions of expected loss in the statistical sense, they can be helpful in enabling insurers to understand the degree of their exposure under specific attack scenarios; see Kunreuther, Howard, Michel-Kerjan, Erwann and Porter, Beverly. (in press). "Extending Catastrophe Modeling to Terrorism and Other Extreme Events" in Grossi and Kunreuther (eds) with Patel. *Catastrophe Modeling: A New Approach to Managing Risk*. Kluwer Academic Publisher: Boston.

[22] After Pan Am 103 flight crashed on Lockerbie, Scotland in December 1988, that small city saw in a couple hours its "population" doubled in number to included journalists for all over the world, emergency teams, politics, citizens for other cities coming to see or help, etc.

using unpredictability, clashing counter-cultures; the task has to do with instability, irregularity, difference and disorder." [23]. The lesson of experience is that very few people receive any training to manage severe loss of references.

In that spirit, understanding some behavioral biases can be useful with regard to important limitations on such initiatives. First, ex ante. Above all, catastrophes that may happen are not seen as credible events. Most people think "it will not happen to me", "this is not possible", "don't be pessimistic". Or "if something happens we will be able to deal with it although our organization has never supported any preparation for it" –a myth we need to dispell. As in the case of BSE, brilliantly analysed by the Phillips Report, these key lines explain the whole dynamics: " In their heart of hearts they felt that it would never happen ". (Phillips Report [24]).

Second, ex post. Another behavioral bias is well illustrated by experimental studies and consists of over-estimation of the likelihood of a new event similar in nature to one that just happened, and under-estimation, even if nothing similar has happened in months or years. [25] Indeed the whole scenery of decision-making when something goes wrong is now in the shadow of difficult managerial challenges.[26]

Third, there are still deep threats among top-level executives to launch something new on these topics, whether ex ante or even ex post. Ex ante, emerging risks are not welcomed. It is much common to treat them as "unrealistic", "too rare", "beyond our responsibility", etc. Lack of historical data and the difficulty in measuring these emerging threats with metrics executives are familiar with could make it difficult for them to report to the board of directors on these issues. Ex post it remains rare to see CEOs taking the lead in ordering collective debriefing on a subject that was, by chance or on purpose, ignored until a recent crisis. Even if the crisis directly affected the organization, the first reflex is mostly "we don't want to talk about it anymore" or "let's try to forget that episode".

While a few CEOs and people in charge of governments recently have demonstrated a clear understanding of the importance of launching a collective healing initiative, most of them remain afraid, thinking that there is a hypothetical risk of doing something afterwards that could affect their career. The short-term incentives facing some managers differ from the long-term

---

[23] Stacey, Ralph. (1996). *Strategic Management & Organizational Dynamics*. Pitman: London, p. 19-20).

[24] Lord Phillips, J. Bridgeman and M. Ferguson-Smith, The BSE Inquiry, vol 1. Findings and Conclusions, London, Stationary Office, October 2000, § 1176.

[25] A survey realized in the U.S. by the Council of Competitiveness –a Washington, DC-based group of CEOs, university presidents and labor unions leaders– in autumn 2002 (just one year after 9/11) found that only 70% of senior executives said they were concerned about a terrorist attack to their business. Half of those had done anything about it. Wharton School. (2003). "How Far Should Business Go to Protect Itself Against Terrorism?". *Knowledge at Wharton, Strategic management*. February.

[26] See Lagadec, Patrick. (1993). *Preventing Chaos in Crisis*. McGraw Hill; Loch, Stephen and Kunreuther, Howard (eds). (2001). *Wharton on Making Decisions*. John Wiley & Sons: New York.

incentives facing the firm, industry or even country. Only a few consider that the major risk today vis-à-vis extreme events is to do nothing about them.

A Financial Challenge

There are also several key financial challenges associated with these large-scale risks and crises related to operation of interdependent networks: Who should pay for the consequences of such events? Who should pay for preventing them? What type of strategy for security investment and collective preparation is more efficient than another? How could one measure such effectiveness?

In these situations with global interdependencies, there may be a need for the public sector – or a coalition of private firms– to take the leading role with respect to providing protective measures because private firms individually may have few economic incentives to take these steps on their own. Kunreuther and Heal recently introduced the concept of *interdependent security* (IDS) using game-theoretic models as a way of addressing some part of the challenges associated with decisions of investment in security for large-scale interdependent networks.[27] The IDS paradigm raises the following question: What economic or other competitive incentives do firms or governments have for undertaking protection in a given sector when they are connected to other organizations or groups and where failures anywhere in the sector may create losses to some or all of the other parties?

Specifically, this framework has been applied to evaluating investments by firms in operational and systems security related to infrastructure operations, while recognizing that any firm's risk is strongly dependent on the operational behaviors, priorities, and actions of others via interconnected networks and supply chains. The interdependent risks across firms may lead all of them to decide not to invest. When the decision is made to invest large amounts of money in preparation of senior-executives and in new security measures, the question as to how prioritize budget allocation in organization operations worldwide is key. In these situations, there could be a need for a general framework for budget allocation as well as the development of new types of metrics to measure progress over time.

In particular developing partnerships could allow spreading the costs –and benefits– associated with the implementation of collective preparation and risk mitigation to improve global security over all partners, a cost a single organization often cannot afford alone.

Future work should address the appropriate strategies for dealing with situations where there are interdependencies between agents (persons, organizations, countries). An important feature of recent episodes is that there are potential out-of-scale consequences, as discussed: the ultimate

[27] Kunreuther, Howard and Heal, Geoffrey (2003). "Interdependent Security". *Journal of Risk and Uncertainty,* 26(2/3): 231-249.

frameworks are not overtaken at the margin, but appear radically inadequate. The anthrax attacks demonstrated the *asymmetric value* of destabilization of large-scale networks: a small scale but carefully targeted attack can cause large-scale reactions because of strong interdependencies and possible cascading fallout. For example introducing a pathogenic agent into a nationwide distribution network may require small financial investments from terrorists compared with the debilitating national impact of such an action on health and business continuity of the country. In order to prioritize budget allocation, scenario-based simulations, involving senior executives that would be effectively in charge if something happens, can be very helpful and worthy.

4. The Paris Initiative: "Anthrax and Beyond"

With this "whole new ball game" in mind, the anthrax episode during the autumn of 2001 is only one of numerous large-scale events that occurred over the past few years. To make a fair transition between this whole framework and a concrete initiative we launched in the spirit of what has just been described, let's focus on some of the key challenges of this network crisis that were systemic in nature, as discussed. To do so, and as we would like also to offer the reader the most factual description of the preparation and development of involved, we quote directly the officials that were part of this initiative from their contribution to the Journal of Contingency and Crisis Management (special issue on Anthrax and postal security; see introduction).

An unconventional episode

A global harm: Reversing the network factor "In late September through early October 2001, a series of bio-terror attacks took place on the east coast of the United States. The pathogen used was anthrax and the vector for the attack was the US Mail system. The anthrax attack in 2001 was one of the most serious crises ever faced by a postal administration. This event caused the American public to question the very safety and security of their mail. While the level of human tragedy, five deaths, was relatively small; the psychological impact on a large portion of the US population was significant. In the classic sense of a terrorist attack, there was an asymmetric relationship between perception and reality. It caused individual citizens to question a fundamental service provided by their government –the daily delivery of mail." (Thomas Day, Vice President, USPS).

"The anthrax crisis was one of the biggest threats to the worldwide postal service ever because it struck at the very heart of our activity. In other words, it affected the transportation and distribution of mail. It was also an unprecedented crisis since, for the first time in the history of the postal service, the future of our business was at risk." (Jean-Paul Bailly, President, La Poste).

Systemic dynamics: a disseminating capacity embedded in systems " Cross contamination" was further confirmed through extensive tests conducted by the US Postal Service, in conjunction with the Department of Defense. Simulated Anthrax-laden letters were prepared in a manner very similar to the letters used in the actual attack. When run through high-speed automated letter processing equipment in a lab environment they expelled contaminates in significant quantities. Further, letters that were processed on the same equipment became contaminated, or "Cross-contaminated" (Thomas Day, Vice President, USPS).

Ignorance, and multi-actor theatre "Lack of knowledge and understanding of this new threat were the key features of the first few days. We had to acquire some basic understanding of the science involved, rapidly provided by our medical team; assimilate the USPS experience, which inevitably did not become clear for some weeks; and build new relationships with the emergency services and the National Health Service. » (Chris Babbs and Brian O'Connor, Royal Mail).

From a top decision-maker's vantage point, a key experience was not to be forgotten: "La Poste's chairman, Mr. Vial at the time, was in New York when he heard the news: According to AFP, two persons had been infected with anthrax in Germany, Europe's first confirmed cases in the mail-borne terrorist scare of autumn 2001. He immediately tried to get in touch with his counterpart at Deutsche Post, to no avail. He was also unable to get a hold of the head of Royal Mail. Unfortunately, the news came on November 2, part of a long weekend holiday in much of Europe. Mr. Vial had to settle for a conference call with a few of the staff members at La Poste who were working that day. Tension remained high until 8:30 p.m. that evening, when AFP finally announced that its earlier report had proved false." (Martin Hagenbourger, Advisor to the President, La Poste).

Launching an International Debriefing

The determination was strong: "never again". It was seen unthinkable that the top leaders of postal services could be unable to speak together so as to share questions and perspectives during such a global crisis. It is worth noting that this behavior is far opposite to the traditional refusal of concern, as discussed in Section 3.

In April 2002, La Poste launched in France a national debriefing process after the Anthrax crisis to learn internally the key lessons of this unconventional episode: the French network had been challenged by thousands of alerts, but not a single real case. During this debriefing, Lagadec strongly advised to go beyond that usual process: the crisis had been trans-national, and accordingly the debriefing had to be trans-national. Martin Hagenbourger, advisor to the President, immediately approved the concept. One needed to think about global preparation, not

at local or national levels only. The decision was rapidly made to launch an international debriefing process, leading to a conference in Paris during the following months. The objective was to ensure that never again would Europe's posts be at a loss to respond readily to a new crisis, especially one that could paralyze the entire European postal network.

The international void Senior executives in charge were convinced that a swift move was necessary to avoid the discussed window of opportunity getting narrower and then disappearing before an adequate international initiative could be launched. It was decided to act with executives in other countries and PostEurop, whose membership at the time encompassed 42 public postal operators across Europe. Experts in public health issues would also be involved, as well as experts in managing emerging crises.

In June 2002, eight months after the Anthrax crisis, La Poste submitted a proposal to PostEurop's Management Board, suggesting holding a closed meeting on the theme of *European postal security*. A meeting bringing together crisis management and security experts from all these postal operators would offer an excellent occasion to exchange views on what different posts had learned internally from the anthrax crisis as well as what they needed to do to cope better with future large-scale risks and threats. While the anthrax crisis could be viewed as a starting point for discussions, the conference would go much further. The challenge was not anthrax per se, which would have been dangerously misleading, but the emergence of a whole new profile of crises. The objective was to grasp the overall lessons linked to the underlying challenge, not the self-evident tactical difficulties of the specific event. The old dictum "never be a crisis behind," had to remain in all minds as a key.

Accordingly, it was felt that participants should be encouraged to share their thoughts on improving the European postal industry's collective ability to respond to future crises. The ultimate goal of the conference was to gather such ideas and to serve as the launch-pad for concrete initiatives that would strengthen the ability of postal operators to better handle whatever contingencies may lie ahead and not to be in the situation of ordering a whole network shutting down again. Finally, the three objectives were clarified:

- 1) learning experiences and lessons on the anthrax crisis from others;
- 2) sharing ideas/proposals to improve the collective reaction to such emerging threats;
- 3) establishing a European-U.S. crisis management capacity enabling postal operators to connect with their counterparts and with other international organisations, using a common platform.

Putting together the Good Team

One clue to keep in mind: our objective was **not** to organise another conference providing some ready-made crisis management recipes. La Poste and PostEurop united their efforts to launch a collective move in order to stimulate common efforts in an area where there is no pre-specified answer.

As it is well known, but also rapidly put away when attempting to launch something "new", what does really matter is the process itself and the quality of people one can bring together. In other words, planning involves more than putting plans down on paper. Getting people involved who are in charge at the highest level of organizations (per organization and cross-organizations within a specific sector) is crucial but **not** enough. The risk here is in seeing an idea or plan of action dying internally after several unfruitful meetings. The lack of consensus on what to do, how to do it, and in allocating a sufficient budget for the operation (internal rivalry, competitiveness) could be the only output each organization is likely to end with.

Another complementary clue is to get **external** people involved, preferably experts on those issues with real capacity of understanding not only these emerging risks and crises but also possible conflicts of interest in the process of launching the partnership. One of the main advantages of having such external people is that they can act as *catalysts* for launching the process and sustaining it over its lifetime. Such an internal-external cross-organizations combination is fundamental for collective thinking, leadership and successful innovation.

This perspective led to a widespread effort:

- The **core team** was made of Lagadec (Ecole Polytechnique, who had a long experience of debriefing processes in many sectors) and Hagenbourger (La Poste). They had to construct the whole concept of the process and set up an international team.
- The **international team** included specialists in managing and financing large-scale risks (Michel-Kerjan, Wharton) and in crisis management (Arjen Boin and Werner Overdijk, affiliated with the *European Crisis Management Academy, ECMA*). Their task was to help incorporate what crisis management experts in the field have already learned elsewhere, providing conference participants with a current view of the issues at stake. Michel-Kerjan took also the lead in clarifying the most recent developments in the United States related to protection of critical infrastructures, emerging global crises and public-private partnerships. From Philadelphia he could also more easily bridge with the USPS.
- In addition, the core team travelled in different countries to meet in advance with European speakers and experts. This was necessary to set in motion a common approach and framework for dealing with the issues as well as to create trust. Trust was key to sustain the

launching process of this initiative. The objective here was definitely to build a common dynamic and a working relationship for the conference itself and more important for the outcome and follow-up afterwards. In crisis management's preparedness, **networking and trust are vital**, and this aspect was thoroughly integrated into the planning.

- In that spirit, several representatives from European public postal operators were invited to share their experiences during the anthrax crisis: TPG Post, The Netherlands (J.A. Rasink), Post Danmark (Ebbe Anderson); Deutsche Post AG, Germany (Edith Pfeifer), Royal Mail, United Kingdom (Chris Babbs); La Poste, France (Martin Hagenbourger). Our main goal here was to create a positive dynamic by first involving a few key postal operators, and we expected a tipping effect with others following the initiative.
- PostEurop, via its General Secretary (Marc Pouw), brought support in to reach members and to bring experts and official involvement.
- La Poste sent out a questionnaire to its European counterparts to find out more about their experiences and expectations.
- To link the initiative between Europe and the U.S., the U.S. Postal Service was represented by one of its vice president, Thomas Day, who joined to provide a first-hand account of what it was like, on the front lines, to deal with these deadly attacks and to be part of the international network we expected to develop in the meeting.

November 2002, Paris: Sharing Experience, and Lessons

That preparation phase lead to representatives from nearly 30 public postal operators coming to Paris in late November 2002 to share their experiences, suggest new avenues for research and to launch a debate on new operational capabilities. As emerging crisis situations in interdependent network would require high-level involvement, international organizations such as the Universal Postal Union (UPU) and the Comité Européen de Régulation Postale (CERP) attended the meeting too.

Many shared converging lessons. Again, let's choose here some of the fundamental lessons, beyond the anthrax episode itself, that can be taken away. The key here is not the " kit " as it often prevailed these last decades. The underlying, in-depth attitude, is a much more fundamental policy approach, shared and underpinned by entire organizations from the very top, internally and externally, through the development of innovating partnerships.

In other words, the ultimate message here would be "this is a challenge for the whole organization, and especially for top level decision-makers, not only for technical specialists, crisis officers and risk managers".

- Martin Hagenbourger, La Poste

1. *Firstly, we must count on ourselves: which means being proactive, the crisis always comes as a surprise for everyone. It is important to count first and foremost on our own capacity to react.*
2. *The crisis shows the need to be modest. We need to be totally transparent in our communication and in our decisions, but it would be a mistake to seek to master everything, and to claim to have all the answers right away.*
3. *Crisis management begins with the work of multidisciplinary teams. The first act of a crisis manager should be to gather around him all of the experts who can help him master the crisis.*
4. *In a crisis situation, sharing information is a must, as is obtaining and having access to the material resources to distribute this information speedily throughout the company.*
5. *Listen attentively to those who manage the crisis out in the field, and always be in a position to respond to their requests.*
6. *The capacity to face a crisis is largely dependent on networks of contacts, which should be set up before the crisis. In the complex world in which we live today, it is impossible to react adequately with the support of only your internal company network.*
7. *Last but not least, where crises are concerned we should always plan on a 'Factor X' which could be referred to as the 'unknown crisis scenario'. One day, we might need it!*

- Thomas Day, USPS

1. *Effective communication is essential.*
   - Reach out to ALL constituencies (employees, unions, customers, etc);
   - Use multiple forms of communication (direct talks, written correspondence, internet, telephone hotlines, TV, Radio, Newspapers, etc);
   - Tell what you know – don't speculate, don't overstate;
   - You can't communicate too much.
2. *Initial Response is critical*
   - Focus must be on the safety of employees and customers;
   - Employees and Customers need to see a visible demonstration of action;
   - Use technology or process/procedural changes that work;
   - Tie the response to the communication. Decide what to do, tell people why, and do it.
3. *Technology evaluation requires a rigorous process*
   - Find the experts;
   - Determine which technologies are proven and validated;
   - Understand your own operating environment;
   - Combine proven technology with operating environment -figure out what works.
4. *Once you have a plan understand it will change*
   - A well-written plan has a limited life, plans must be updated on a regular basis;
   - Technology changes at a rapid pace, incorporate improvements into updated plans;
   - Threat and vulnerability assessments must be continually updated;
   - Don't focus on the "last war"; constantly consider future threats;
   - Threat and vulnerability assessment must consider biological, chemical, radiological and explosive threats (and anything else that might be added in the future)."

- Chris Babbs and Brian O'Connor, Royal Mail:

1. *The next crisis will never be the same as the last and may well be something the organization has never contemplated. Consequently:*
   - Developing processes and relationships is more important than doing detailed planning;
   - The processes need to be practiced;
   - Limiting the detail of planning to the minimum consistent with achieving the objective;
   - Not doing over-plan, as all plans are out-of-date the moment they are finished and over-elaborate out-of-date plans can be positively dangerous!
   - Trying to develop plan 'granularity'- small-scale plans which can be fitted together in the framework required by the next crisis.
2. *Communications planning requires the same level of effort as operational planning.*
3. *Managing perceptions can be as important as managing the reality.*
4. *Concrete gestures, even if not strictly relevant, can have enormous psychological effects.*
5. *Make sure your crisis management model can accommodate additional specialist input, and make sure you know where to get each kind of expertise.*
6. *You need people standing back from day-to-day handling of the crisis and seeking to spot the longer-term strategic issues.*

Immediate measurable output: Launching an international partnership supporting rapid reaction capacity

The Paris Initiative produced more than the sharing of experience and lessons. It was decided to create a network to improve the overall reaction in case of a new transnational threat. The project was simple but essential: the creation of a permanent platform connecting all the European operators within the first 24 hours of a crisis. Such a tool would allow them to exchange information about the solutions being implemented by each country and to work out a concerted strategy.

That new network had its first test on January 15, 2003, the day it became operational. PostEurop had received an advisory from the U.S. Postal Service concerning a possible anthrax contamination in the Washington, D.C. area.[28] The network provided posts across Europe with accurate and timely information on this potential incident, enabling them to assess the proper scope of the risk involved. The network is still operating today.

5. Conclusion and New Avenues

Providing keys for dealing with postal security at an international level, we would like to quote executives from the U.S. and French postal services who were part of this project.

"The anthrax crisis was a unique event. This does not mean that anthrax is the only threat to consider, nor does it mean that the only target will be the US Postal Service. This attack should serve as a wake-up to all postal administrations to the possibility of a broad-range of threats. […] Don't focus on the 'last war'; constantly consider future threats" (Thomas Day, VP, USPS, 2003).

"The lessons learnt as a result of the anthrax crisis have taught us that, from now on, we need to work together to counteract these crises effectively. We must strive towards an optimal level of cooperation between postal operators. The aim of the Paris conference was definitely – and this objective was successfully achieved– to come up with a series of operational mechanisms that can be implemented on a European [and U.S.] scale as rapidly as possible, mechanisms that can be progressively transferred to encompass the entire world.

Already, during a recent (false) alarm, again related to the issue of anthrax in the United States, we were able to witness the positive results. But we must not allow ourselves to become complacent: from now on we all need to resolutely commit ourselves to making a significant and determined long-term effort to ensure that we are constantly capable of dealing with the complex and ever changing challenges in terms of risks, crises and breakdowns in relations." (Jean-Paul Bailly, President of La Poste, 2003).

[28] This was following a positive test result: a piece of mail addressed to the U.S. Federal Reserve and passed through the V Street's postal facility.

The Guns of August crushed Europe in 1914.[29] *The Planes of September* and other waves of emerging ruptures are setting the scene today. Stakes are of historical importance. The *vision* is clear: "fiasco is not an option". Our collective responsibility is to transform emerging global ruptures into emerging global opportunities, and collective answers have to be reactive and scaled to the new scene. With the growing globalization of social and economic activities that leads to increasing cross-industry/cross-country interdependencies and large-scale risks associated with high degree of scientific uncertainty, we do not play chess anymore. Events that occurred worldwide over the past 5 years have shown to all of us that today a single event (or threat) can be sufficiently extreme to destabilize a whole set of firms or even industries, or even several countries, as well as to inflict quasi-instantaneously irreversible losses of billions of dollars. In that spirit, while boards in industry and governments have begun to consider these issues with a real sense of urgency, the question of budget allocation –prioritization of limited resources– remains one of the most crucial strategic aspects to be decided on but goes beyond the scope of this paper.

Related to preparation of executives in charge, it is crucial to train top leaders, as they have the most difficult task in this new environment. This is not so natural. And let's remember that "crisis has no time to waste"; its first target is the key leader. If he or she adopts an inadequate line of actions, then the whole organization, as well as others that depend on it, will be in the hand of the crisis. As our involvement in the Paris Initiative illustrates, it is key today to introduce and develop strategic and trusted catalyst teams. Coming from both inside and outside the organizations partnered in the joint initiative, they can advise top leaders on these emerging questions, formulate contra-fashionable questions, and suggest bold innovations as well as to engage with multiple bodies outside. And, above all, they can take bold initiatives with pilot projects involving unusual circles of people and organizations. That is the only proven way to develop trust, capability, and empowerment.

The Paris Initiative is an illustration of successful collective actions, partly because it had been thought of as leading to concrete outputs, and thus to measurable benefits for all stakeholders, whether in terms of better preparation or financial return on investment. Numerous conferences are now organized on the subject of critical infrastructures and risks associated with globalization. However, conferences are not sufficient anymore. What is strongly needed are concrete and collective actions.

Each critical sector has obviously its own set of key processes, activities, institutional and legal arrangements, and cultures. While our initiative dealt mainly with postal security –on

[29] Barbara Tuchman. (1962). *The Guns of August*. Bantam: Toronto.

purpose, as a large-scale pilot–, the framework introduced in this paper could be meaningful for preparing and implementing similar international programs in other industries in which activities also are sustained by the continuity of interdependent networks challenged by growing threats. These industries include aviation, defence, energy, banking and finance as well as water supply, hospitals and health systems, among others. The Paris Initiative has been a watershed. Let it be the first of a long and lively list. The *immediate imperative* is clear: time to get to work.

Appendix 1.
CHECK-LIST FOR
SENIOR EXECUTIVES' QUICK TEST

"Do not abandon the field to the unthinkable"

This check-list is based on our personal experience
within a club of senior executives from various critical networks

You already have a crisis management capacity and good training for well-known events.
Now you can address today emerging risks.
Just to control your road-map, some guidelines:

When, if ever?

1. When did you *organize* the latest unconventional simulation exercise in your organization?
2. When did you *participate* in the latest unconventional simulation exercise in your organization?

If your answer is "never" or "a long time ago", please consider the following question:

Why is your organization still among the few ones convinced that "as long as it is unthinkable, there is nothing to think about and prepare?"

Who is in charge, and with whom? (for those who actually participated in an exercise)

3. Did you personally play your role in this exercise?
4. Did you involve partners outside of your organization?

What?

5. Was this simulation effectively anchored on unconventional "out of the box" threats or are you satisfied with old fire evacuation or last-century "media communication" exercises only?
6. Did you organize a debriefing, focused on the key surprises and reactions to them?

Strategic preparation

7. Are you systematically investigating emerging significant crises at national and international level? (*for example, what did you do after 9/11, after the Anthrax crisis, the SARS alert, or after the 14 August blackout in the US and the one in Italy?)*
8. Are you actively involved in a club of CEOs, Presidents, and top-level specialists within leading research institutions and think-tanks to share questions, ideas, answers, as well as face the unthinkable and turn emerging large-scale risks into real opportunities?
9. After reading about the Paris Initiative on Postal Security, don't you think other organizations in your sector (for example, your competitors, if any) are much better prepared than your organization? What kind of bold initiatives you would be prepared to consider and to launch?
10. In this context, what is *your* roadmap for the next two years?