Patrick Lagadec, Erwann O. Michel-Kerjan, and Ryan N. Ellis

innovations
TECHNOLOGY | GOVERNANCE | GLOBALIZATION
mitpress.mit.edu/innovations

Disaster via Airmail

The Launching of a Global Reaction Capacity After the 2001 Anthrax Attacks

> In 1914, we were caught totally unprepared.
> In 1940, we were fully prepared—for the First World War.
>
> —*A member of the Civil Contingencies Secretariat, Cabinet Office, London.*[1]
>
> If 9/11 was a failure of imagination, then Katrina was a failure of initiative. It was a failure of leadership. If this is what happens when we have advance warning, we shudder to imagine the consequences when we do not.
> Four and a half years after 9/11, America is still not ready for prime time.
> —*A Failure of Initiative*, U.S. House of Representatives, 2006.[2]

In this new century, increasing interdependence among people and organizations is creating a new web of challenges. "Unconventional" events—large-scale disasters and disruptions—that evidence the effect of interdependency are becoming the norm. In the past five years alone, the United States has experienced an array of events in this category resulting in dramatic losses and revealing profound vulnerabilities: the September 11, 2001 attacks, the Anthrax attacks, the Enron collapse,

Patrick Lagadec is a founding member of the European Crisis Management Academy, member of the French Academy of Engineering, and director of research at the Ecole Polytechnique in Paris. Author of ten books, among them Preventing Chaos in a Crisis (McGraw Hill, 1993), he has been acting as a strategic advisor and trainer in the field of major risks, unconventional crises and global "ruptures" for the past 25 years. Dr. Lagadec received the Engelberg Forum Prize in 1999.

Erwann O. Michel-Kerjan is Managing Director of the Wharton Risk Management and Decision Processes Center at the University of Pennsylvania's Wharton School. His work focuses on managing and financing extreme events. A member of the Global Risk Network of the World Economic Forum, he is the co-author most recently of Seeds of Disaster, Roots of Response: How Private Action Can Reduce Public Vulnerability (Cambridge University Press, 2006).

Ryan N. Ellis is a doctoral student in the Department of Communication at the University of California, San Diego. He received his MA in Communication in 2004 also at the University of California, San Diego. His current research focuses on the history of competition within the U.S. postal industry and the contemporary politics of postal service.

the explosion of the Columbia shuttle, the 2003 blackout, and the 2004 and 2005 hurricanes seasons. Will 2007 be even worse?

How well are we prepared, individually and collectively, for this new world of global turbulences and large-scale dislocations that result when a series of local events creates impacts at a large scale? Most crisis management tools developed over the past 20 years are based on the outdated assumption that risks are always calculable, that it is possible to list all adverse events, to determine the probability of each one based on past experience, and to measure the costs and benefits of specific mitigation measures. But in today's world, we increasingly experience events of a type and scale never seen before, in rapidly changing contexts, and requiring ever more rapid response.[3]

When traditional risk assessment tools are of limited use, creativity is imperative. The first step is recognizing that, as the ratio of "crisis time" to "normal time" increases, leaders of both business and public policy must not only address large-scale risks, they must also prepare for management during times of crisis as a central element of their operating strategy. The second step is realizing that, since local actions can have global impacts, managers of even moderately-sized organizations face, to some extent, similar challenges as global leaders. We can innovate if we can imagine new avenues of action and new approaches to collaboration, as both the official inquiry into "mad cow" disease in Britain[4] and the report of the 9/11 Commission in the United States made very clear.

In this paper, we focus on the new landscape of risks we all face today and on *how* strategic partnerships can be developed at the senior-executive level, domestically and internationally, to better prepare organizations to face such risks. Specifically, we describe an initiative, "Anthrax and Beyond," two of us (Lagadec and Michel-Kerjan) organized in the wake of the Anthrax crisis of 2001. The initiative brought together top-level decision makers from postal operators, international postal organizations, and crisis management experts with one main goal: create trusted relationship, share experience and develop a global reaction capacity. In doing so, we attempt to create a framework for addressing the new challenges posed by just-in-time operations within an interdependent world.

This crisis started on September 18, 2001, just one week after the attacks of 9/11, when four anthrax-contaminated envelopes, along with thousands of hoaxes, paralyzed the U.S. postal service and destabilized the international postal system as a whole. We describe how postal organizations responded to the crisis and demonstrated a lack of coordination capacity, which motivated this initiative. We then suggest some lessons involving leadership and collective action. The lessons are relevant to those managing risks in other interdependent networks: for example, pandemics spread through commercial airlines, or terrorist attacks employing the food distribution system, to name a few.

THE CHALLENGES THAT NEW FORMS OF RISK PRESENT

Before turning on this initiative and its key features as well as measurable outputs, we discuss the Anthrax crisis per see. A lot has been said and written about it, so it is not our goal here to summarize all these contributions. Rather we would like to offer a somewhat different perspective on what happened, and why it happened that way. Occurring over a 10-week period between mid-September and mid-November of 2001, the anthrax attacks were a paradigmatic event acutely illustrating the challenges that new forms of risk present. They illustrate three key phenomena: the role of surprise and the limits of scientific understanding in new forms of large-scale risks, the rising level of global interdependence, and the economic challenges that unknown probability / high-consequence events present in the context of increasing market liberalization and competition. Each of these phenomena teaches us a different lesson.

Surprise and Scientific Ignorance

The use of anthrax for hostile purposes is not new. The hazards of anthrax have been known for centuries,[5] and governments have been experimenting with deploying it as a weapon since at least World War II.[6] During the 1990s, U.S. officials became concerned about a biological attack, which could use anthrax,[7] and between 1998 and early 2001, several letters arrived at in the U.S. and Canada, falsely claiming to contain anthrax.[8] Yet, the actual anthrax attacks of 2001 confounded the expectations of scientists and planners, revealing how inadequate and inapplicable the current state of knowledge was. The pre-attack planning scenarios were nothing like the actual events, and it was very difficult to simulate the consequences of an attack under laboratory conditions.

This is a key point: pre-attack scenarios assumed that attacks would be geographically and temporally fixed, and that their parameters would be visible and known. Pre-2001 discussions mainly focused on mass-casualty scenarios involving a large-scale attack in which anthrax particles would be dispersed in the air—in a densely populated area.[9] Other scenarios considered limited exposure through the mail.[10] Both kinds of scenarios assumed temporal and geographical fixity: one dispersal of a large quantity of anthrax would target one densely populated area. Or, letters treated with anthrax would pose a threat only to individuals who were right where the letter was opened, and the presence of anthrax would be obvious.[11]

Assuming away questions of scope, in these scenarios the key challenge of a large-scale attack was the many casualties. So the key challenges appeared to be triage—separating the sick from the worried—and treating a contained, bounded, exposed population. Medical discussions focused on Lethal Dose (LD), the amount of exposure that could kill a person. By determining LD, planners could determine the potential magnitude of a large attack in a densely populated area. LD_{50}, the amount of anthrax spores that would kill 50 percent of a population, was the figure used to project the consequences of an attack.[12]

But in the fall of 2001, the actual attacks could not be reduced to a single location or single point in time; suddenly the challenge was to define the limits of meaningful exposure and track the spread of anthrax cross-contamination through the entire postal system. Indeed, much of the knowledge about a hypothetical anthrax attack was structured around the exigencies of a fixed event and did not apply in this real situation where there was ignorance both on the nature of the threat and its scale.

It is worth noting that the string of hoaxes, the so-called "fake anthrax letters," of the late 1990s and early 2001, led the U.S. Center for Disease Control (CDC) and Canadian Defense researchers to consider the scenario of an anthrax attack that used the postal system. Only one publicly available laboratory study of such a hazard was conducted before the actual attacks; it focused on the danger of opening, or being near the person opening, an anthrax letter.[13] Likewise, CDC guidelines established in response to the hoaxes focused on this moment of letter-opening as the critical point of exposure.[14] Importantly, no one considered cross-contamination in much detail.

But little of this knowledge applied to the actual attacks in the fall of 2001. In fact no one knew for several weeks how many letters containing Anthrax had been introduced into the network. Moreover, two other factors created additional geographic and temporal uncertainty: cross-contamination (as anthrax spores spread throughout the postal system, leaving spores on other letters, equipment, and surfaces), and re-aerosolization (as spores traveled through the mail stream and continued to re-disperse). Now the key challenges were largely definitional: Where are there anthrax spores? What are the limits of cross-contamination? How dangerous is exposure? When do spores become aerosolized? Measures of LD_{50} were suddenly of little use; the public was demanding a much higher level of safety. Similarly, the moment of letter-opening was no longer the single moment of exposure, now that cross-contamination was assumed to be widespread, but ill-defined, and re-aerosolization was occurring repeatedly. Now the key challenges were mapping the scope of the attacks in space and time, and defining where and when meaningful exposure was occurring.

Scientists and public officials could not answer questions of definition; testing methodologies could not map the spread of cross-contamination throughout the mail stream. Nor could anyone establish a minimum threshold to define what quantity of anthrax represented a risk to humans.[15] As a later government report observed: "Anthrax test results … cannot be interpreted as a health risk based on current scientific knowledge" and the "CDC did not know how to extrapolate … test results to an individual's risk."[176] The U.S. Postal Service (USPS), using downstream modeling, attempted to define the scope of exposure through cross-contamination in its facilities, but this was plainly inadequate. Initially, 280 facilities were tested and 23 returned positive results. Later, however, anthrax was found in facilities previously found to be anthrax-free, casting doubt on the tests' reliability. Then, an elderly Connecticut woman died and a facility that had been stated as outside of the USPS's defined scope of possible exposure was indeed found to be cross-contaminated. This made it clear that the USPS could not correctly model cross-contamination.[17]

Thus, scientists and public officials faced three challenges during the attacks: charting cross-contamination, identifying exposure, and interpreting exposure; what amount of anthrax represents a risk? People in authority could not use pre-attack planning and knowledge to answer these questions with confidence, or tailor their responses effectively. And this was despite a long history of study into and preoccupation with the possibility of an anthrax attack.

Furthermore, as mentioned above, the ignorance was not only about the science per se; simple counting was impossible. Authorities felt they were driving in the fog, unable to determine how many envelopes were contaminated: 4, 4,000, 40,000, or far more? That is, how badly contaminated was the U.S. postal system that carries nearly 700,000,000 pieces of mail every day?

What lesson do we learn from understanding surprise and facing ignorance?

> LESSON 1: "Science deals with regularities in our experience. Art deals with singularities."[18] If singularities become the normal feature of emerging crises, we confront a radical gap. And if our usual practice is to document and model risks in "pure" conditions (LD_{50}), our expertise is in great difficulty when we must respond to in-situ problems. Ignorance and surprise were the hallmarks of the anthrax attacks.

Interdependence

Historically, and as this has been the case of many critical infrastructures,[19] postal service integrated people into the national and global community as communication expanded across great distances. But the anthrax attacks transformed the very closeness and intimacy that integration promises into something alarmingly sinister. As public health and postal officials struggled to answer the most basic of questions—"Is the mail safe? Is this area dangerous?"—the interconnection provided by the postal service became a source of uncertain danger that no one could easily contain or calculate.

The global postal network integrates a set of interconnected national and regional networks, each of them its own amalgam of local routes and hubs. This network of networks is made up of public national carriers (like the USPS) and, increasingly, privately-operated firms (e.g., UPS, FedEx), including competitive private delivery services, transportation companies that offer long-haul contract service, and third parties that handle and sort mail. Ignorance about cross-contamination made it exceedingly difficult to segregate the infected channels of the national and global postal network from other, "clean," pathways. In such an interconnected network, cascading failures quickly become acute: failures of one component of a larger system lead to failures throughout or across systems. One way to address this problem is to intentionally allow "islanding": when problems arise, formerly interconnected systems separate into autonomous units, to prevent further problems. This type of intentional system-failure can work very well if it isolates problem areas and lets other systems continue functioning (one can see that isolating feature in some electrical systems).

But no one could start "islanding" the postal network unless they could first map the cross-contamination. And, as discussed in the previous section, ambiguity was everywhere: anthrax was found in facilities that tests had previously been declared clean, and in facilities formerly thought to be outside the range of possible contamination. Nationally, it was impossible to provide a reliable map of contamination by charting exposed nodes (postal boxes, post offices, processing plants, transportation lines, and other facilities vital to transmission of the mail). This also made it impossible to separate the distinct nodes, so public officials had to concede that they could not establish the scope of cross-contamination and exposure.[20]

The same was true on a global level. Over the past few centuries, national systems have become increasingly interconnected, and in the last few decades international service has become increasingly lucrative and prominent. Short of stopping all international shipments by mail, officials had no way to assure that anthrax did not expose formerly unexposed segments of the global network.[21] Once again problems of definition were key: ignorance surrounding the hazards presented by cross-contamination and re-aerosolization allowed the attacks to move from a purely local problem, confined to a discrete subsection of the postal network, to a system-wide, and hence global, problem.

As a plethora of international hoaxes and false alarms occurred in the next few months, we saw another important dimension of interdependence. Once anthrax was in the mail, unverified cases around the world took on a new urgency. Investigating these unverified reports is costly, both economically (human labor) and emotionally (anxiety). The perception that mail was unsafe spread faster than authority figures could determine safety limits—and markedly expanded the scope of the attacks.

Thus hoaxes and false alarms are not external to such an attack, but simply another dimension of it. Moreover, if the attackers wanted to psychologically destabilize a nation already under stress, then "playing" with true and false alarms was certainly an effective part of their strategy. In that sense it was in many occasions meaningless to distinguish between "false" and "true" alarms.

In this regard, the anthrax attacks were explicitly global. Local disruptions were globally significant, potentially impacting health and continuity of operations worldwide. The security of any one of the networked players depended on the actions of the others. The failure of one link in the networked chain threatened all the other links, making coordination indispensable yet frustratingly elusive.

Indeed, crisis management among European postal operators, and between USPS and these operators, took on a different cast in the wake of the first confirmed anthrax letters in 2001. On November 2, 2001, in the middle of this two-month crisis period, Martin Vial, chairman of the French postal operator La Poste, was in New York when he heard the news that two persons had been infected with anthrax in Germany. He immediately tried to contact his German counterpart at

Deutsche Post, to no avail. Nor could he contact the head of Britain's Royal Mail. Unfortunately, November 2 was part of a long weekend holiday in much of Europe. Mr. Vial had to settle for a conference call with a few staff members at La Poste who were working that day. Tension remained high until late that evening, when media finally announced that the earlier report had proved false. A case of actual contamination in Europe would have made the crisis far more complex. Since no institutions had developed mechanisms for sharing real-time information across the global postal network, coordination was nearly impossible, even if actors saw it as necessary.

This kind of interdependence is visible far beyond the global postal network. Risks to the postal infrastructure affect other essential everyday services. Consider the closing of the Hart Senate Office Building, and the limited relocation of the Supreme Court during the attacks; here the disruption in postal communication led to a disruption of government operations. Interdependent effects originating in the postal system could shut down not only government offices, but also hospitals, police stations, and essential services like the distribution of welfare checks. The postal network also provides material links across the globe. The anthrax crisis had the potential to disrupt many sectors of services that keep societies operating around the world.

Thus the anthrax attacks show how novel forms of risk take on global dimensions, moving disruptively across and between different systems. The problems of cross-contamination and definition transformed the interconnection of postal networks (national, regional, and global) into a dangerous series of couplings that could not be undone or reliably assayed. Meanwhile, the ubiquity of the postal network jeopardized many different forms of activity, as they spilled across the boundaries of postal operations. A huge and interdependent operation came face to face with its own ignorance, and decision makers had neither well-defined tools nor well-defined responsibility and accountability to take collective action; the elements combined to create unprecedented destabilization. Five years later, the public still does not know what really happened. Who did send those letters? And what lesson do we learn from understanding interdependence?

> LESSON 2: In the 1980s, we learned that isolating a crisis was key to managing it. "Clearly, the successes of Johnson & Johnson in handling its Tylenol crisis [1982] and Procter & Gamble in handling its Rely tampon crisis [1980], were largely due to the ability of those two companies to isolate both the crisis and the people dealing with it."[22] Today's emerging crises are likely to become global, instantly. Crisis intelligence and management must mutate accordingly.

Economic Challenges

The anthrax attacks illustrate a third important dimension of novel risks: economic considerations. Postal markets have changed drastically in the last four decades. Formerly closed national markets, served by state-run operators, are being exposed to competition as nations liberalize their laws governing postal service and newly introduced technologies provide customers with alternative avenues, both material and electronic, for sharing and delivering information.[23]

The process of preparing for large-scale risks of immeasurable likelihood and consequence is often at odds with the reality of competitive infrastructure services. In a competitive environment, it can seem like an impossible luxury to provide increased protection against an event with an incalculable (or extremely low) probability and unknown consequences.[24] Defining the probability of an attack is an uncertain gambit; unlike other type of disasters for which there are historical data available (e.g., natural disasters), intentionally caused disruptions are adaptive and render the past an uncertain guide to the future. In a competitive environment, markets and organizations attempt to maximize efficiency and minimize expenses; they have often little tolerance for setting aside resources to address risks that cannot be quantified, unless a similar untoward event has happened to them recently.

After the anthrax attacks, as leaders discussed new sets of practices that could prevent or respond to a similar attack, they necessarily tried to marry business and security concerns. The costs of security are invariably passed on to users through rate increases; no one ever seriously considered federal appropriations as a way to cover all of the costs associated with the attacks and their aftermath. To maintain the economic health of the industry, the needs and interests of users must be considered, especially in the face of uncertain risks of indeterminate consequence. Those qualities that make the postal network useful and valuable—openness, speed of delivery, geographic reach, low cost—also make it vulnerable. New practices designed to address the possibility of large-scale risks must seek a middle path that can both speak to the vulnerabilities and continue to provide value.[25]

The new risks we now confront are of a different sort: unformatted, geographically and temporally unmoored, irreducible to the specific boundaries of industries or nations, and incompatible with trends towards greater competition to provide services. All these challenges are unique and crucial. They are not the burden of any nation alone, nor are they the exclusive responsibility or concern of the public sector. Creative global collaboration between public and private actors may offer the only way to succeed with these daunting tasks.[26]

On a positive note, more and more top decision makers within service organizations realize that these emerging risks are an integral part of an even more competitive environment. No longer is it enough to compete during "normal time"; competition puts even more at stake during "disaster time." Indeed, customers certainly see leadership as a gauge of quality; many can turn to another operator who has looked much more prepared during a recent crisis. As disasters occur more and more often, top leaders who are well prepared see the window of opportunity growing; visibly good preparation can give them a measurable return on investment. The other face of the coin is probably more crucial: any organization that shows impotence or paralysis will lose credibility, consideration, and even dignity—making any recovery process very difficult. What is the lesson from considering these economic issues?

> LESSON 3: As soon as we leave the boundary and protection of a relatively isolated, stable, and "reasonable" world, the economic dimension becomes even more critical. When we leave the tiny calm harbors where we used to think and practice business, to navigate turbulent and unknown oceans, we must reconsider our most basic references. And the very nature of the market in which we operate is one of them.

MAKING DECISIONS AT THE TOP: GETTING OVER MYTHS

As the anthrax attacks of 2001 illustrate, this new era has direct implications for the way crises must be addressed in the future. As we saw with SARS and the avian flu, people in charge during a crisis are instantly confronted by a maze of various issues: scientific, technical, organizational, economic, diplomatic, cultural, and ethical. The business world is spread over several locations, with headquarters in one region, the incident-tracking system in another, and the crisis center in a third— and very different actors and frameworks of decision-making in each. This limits the use of simple global decision rules during a crisis unless they are already collectively in place beforehand. To make key decisions in this difficult context, decision makers must acknowledge and deal with three crucial lines of challenge: in intellect, in training and behavior, and in finance.

Intellectual Challenge: From Linearity to Discontinuity

Decision-makers confront situations that are global in scale, of uncertain importance or consequence, influenced by several different players, and temporally unstable. Postal planners could not readily assess the limits of the anthrax attacks, nor could they establish the significance of exposure. They also had to balance the interests of a skittish public, sometimes disbelieving unions, and indeterminate scientific findings, without the benefit of probabilistic analysis to guide their response. Operating on these different fronts under situations of immense pressure offers new intellectual challenges.

Underlying these new challenges is discontinuity: a fault line, splitting one situation into radically different worlds. People are trained to expect stability and rely on institutions (patterned ways of thinking and doing) to confront a familiar range of scenarios. Yet, these emerging critical contexts, most of them unstable, may lie far beyond society's capacity to understand quickly, at the moment when decisions must be made. Here, research can fill an urgent need. As Hegel said, "If you are confronted with unthinkable challenges, you have to invent unthinkable paradigms."

A Training and Behavioral Challenge

Decision-makers must begin thinking about surprises, and learn to adapt to them better. Oddly, almost all textbooks on strategic management focus on the easiest part of the management task: running the organization in as surprise-free a way as possible. But, as Ralph Stacey pointed out 10 years ago, "On the contrary, the real management task is ... handling the exceptions, coping with and even using unpredictability, clashing counter-cultures; the task has to do with instability, irregularity, difference and disorder."[27]

Behavior matters too. We must understand behavioral biases because they can present important obstacles as we launch the collective initiatives we need to tackle large-scale risks and crises. First, many people do not see anticipated catastrophes as credible events. Most corporations think "it won't happen to us."[28] Or they think that if something happens, they can deal with it, though their organization has never supported any preparation for it. We must dispel these perceptions. Consider how mad cow disease spread in the United Kingdom, and a line from the later national inquiry: "In their heart of hearts they felt that it would never happen."[29]

The second behavioral bias has been well documented by experimental studies. First, those in charge immediately over-estimate the chances of a new event similar to one that just happened. Then, with time, public attention fades and people tend to under-estimate the probability of another catastrophe. This is often the case if nothing similar has happened in months or years.[30]

Indeed, the lesson to be learned from the anthrax case is not simply that the postal system must be better prepared to confront the threat of anthrax (although it should). It is that postal managers, as those in other critical sectors, must prepare for a crisis not yet understood. Preparing only to confront yesterday's crisis can creates new vulnerabilities today and tomorrow. A paradigm shift is in order, so that managers of organizations can have the resources to confront the undreamed.

A Financial Challenge Because of Security Externalities

Several key financial challenges are also associated with these large-scale risks and the crises related to operating 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 most efficient? How can we measure such effectiveness?

In situations with global interdependencies, the public sector—or a coalition of private firms—may need to take the leading role in providing protective measures, because private firms will have few economic incentives to do so separately. The concept of "security externalities" is relevant here. [31] Businesses may not always realize how their failure to operate could affect many agents, often rippling far beyond their direct influence. After all, it is hard to hold a business entity accountable for negligence when it is responsible for initiating a cascading failure across multiple economic sectors. This causes the divergence between what economists call the "private costs" and "social costs" of the firms' actions. Private costs are privately borne; social costs are borne by the community. When both the costs and benefits of an action are privately borne, then there is every reason to believe that investment decisions to mitigate such costs will be privately optimal. However, when a private decision has social impacts—either costs or benefits that are not taken into account by the private sector —then it is more likely that the outcome will not be optimal from a societal standpoint. In the case of a security externality, a private firm undertakes an action that creates a vulnerability, or possibly an uncompensated benefit, elsewhere in the economy.

Let us consider a specific case. Kunreuther and Heal recently introduced the idea of interdependent security; they used game-theory models to address some of the challenges associated with deciding on investments in security for large-scale interdependent networks.[32] The interdependent security paradigm raises the question of what economic or other competitive incentives may influence firms or governments to undertake protection in a given sector when they are connected to other organizations or groups and where failures anywhere in the sector may create losses for some or all of the others. The framework recognizes that any firm's risk strongly depends on the operational behaviors, priorities, and actions of others via interconnected networks and supply chains.

In particular, by developing partnerships organizations could share the costs (and benefits) of implementing collective preparation and risk mitigation to improve global security. These are costs a single organization often cannot afford alone.

ANTHRAX AND BEYOND

Like other recent large-scale events, the anthrax crisis during the autumn of 2001 provides an opportunity to discuss a concrete initiative in the context of the framework we described above. Ultimately, only four anthrax-contaminated letters were found in the U.S. postal network, but the great uncertainty about the degree of contamination lasted for weeks. That the elements of the network could be used as a weapon surprised everyone—and turned the U.S. infrastructure into a global threat. Indeed, during the crisis hundreds of false alerts occurred daily in the United States and in many postal services worldwide. The decision to shut down the whole U.S. Postal Service had been seriously considered at the very top of the country. But the service treats about 700 million pieces of mail every day. Even shutting it down for just a week, to better measure the scale of the contamination, would have implied trying to eventually turn in a system with billion pieces unchecked. Eventually, it was decided against a shutdown; even that drastic step would not have let them determine which of nearly 5 billion of pieces of mail were contaminated.

The anthrax crisis raised fundamental questions about postal security worldwide. The "Anthrax and Beyond" initiative that two of us designed and implemented, began only a few months later. As a response, we suggested an international debriefing process. Our strategic goal was to help postal operators at the highest executive level meet a double challenge: 1) understand the new arena of emerging vulnerabilities, and 2) prepare creative operational breakthroughs that will keep worldwide postal operations sustainable and growing in the future.[33]

Launching an International Debriefing

After the anthrax attacks top managers were determined: “never again.” They were amazed that among top leaders of postal services they could not speak and share questions and perspectives during a global crisis. Notably, this behavior is the opposite of the usual denials (“let’s just forget what just happened, and go back to business as usual as soon as possible”—no lessons learned).

In April 2002, France’s La Poste launched a national debriefing process to learn the key lessons from the anthrax attacks (the French network had been challenged by thousands of alerts, but not a single real case). During this debriefing, Patrick Lagadec strongly advised them to go beyond their national process: as the crisis had been transnational, the debriefing should be too. La Poste quickly decided to launch an international debriefing process, which would soon lead to a conference in Paris.

La Poste wanted to bring together the crisis management and security experts from postal operators worldwide so they could exchange their internal lessons from the anthrax crisis and plans to cope better with future large-scale risks and threats. The anthrax crisis was viewed as the catalyst for discussions, but the conference (and its preparation) would go much further, to address the emergence of a whole new profile of crises. The old dictum “never fight the last war,” was to remain in every participant’s mind.

The conference was intended to gather ideas and then launch concrete initiatives that would let postal operators better handle future contingencies, rather than standing in the middle of the uncompleted bridge we’d seen during the Anthrax crisis (ordering a the shutdown of the whole network or letting the system operating under strong ignorance of what could happen next). This initiative had three objectives: 1) learn about others’ experiences and lessons from the anthrax crisis; 2) share ideas and proposals to improve the collective reaction to emerging threats; and 3) establish a platform for crisis management that would link Europe and the United States, so postal operators could connect immediately with their counterparts and with other international organizations.

In-depth Preparation

In order to achieve this goal, it was important to adopt a different posture than the one consisting in simply organizing “another” conference. We knew the conference we envisioned would be just the tip of the iceberg. In-depth preparation and the quality of people this process would bring together was a key to the success of this initiative. The initiative involved people at the highest level, both in their organizations and across organizations within a specific sector; it also, crucially, involved external people. Actually, in many occasions we have seen an idea or plan of action dying internally after several unfruitful meetings. These external stakeholders included a few relevant experts who clearly understood not only the emerging risks and crises but also possible conflicts of interest of launching the partnership. We wanted consensus on what to do and how to do it, and sufficient funding for the operation to let us avoid internal rivalry and competitiveness.

External actors bring another key advantage: they can act as catalysts to launch and sustain the process. This combination of actors—internal and external, and across organizations—is fundamental for collective thinking, leadership, and innovation. In a competitive world, these neutral catalysts will play a key role in linking the stakeholders.

We then created a core team who traveled with us to various European countries, and around the U.S., to meet in advance with speakers and experts. We visited people in charge inside postal organizations, listened to them, and suggested that they join the initiative. We also visited outside organizations and other international experts in the field to persuade them to join. These advance meetings generated trust with prospective participants and set up a framework for approaching the issues that would be central to the conference. Indeed, we all know that trust is fragile. Crisis episodes—perhaps more than any other situations—can destroy it easily. Like preparedness in crisis management, we saw that networking and trust were vital to the conference, and integrated them into our planning. This was hardly a natural behavior: when a storm is approaching, the instinct is to build partition walls.

We should say here that initially the initiative envisioned bringing together only a few postal operators, including those of France, Germany, the Netherlands, and the United Kingdom. But as the word was spreading that a core team had taken the initiative, we saw top managers of another postal operation joining in, then another… with the commitment of the first few we had rapidly met a critical mass and we saw a tipping effect.

Eventually the Anthrax and Beyond initiative involved postal operators and external stakeholders from nearly 30 countries across Europe and the United States. The two-day conference "Anthrax and Beyond," six months in preparation, took place in Paris in November 2002, one year after the height of the international postal crisis. Postal sector executives came to share their experiences, suggested new avenues for management, and launched a debate on new operational capabilities. Because emerging crises in interdependent networks would require high-level involvement, international organizations such as the Universal Postal Union and the Comité Européen de Régulation Postale (European Committee for Postal Regulation) also sent representatives.

But the key to the whole process has to be stressed. The first reason for success was the mere modest move: go and listen to other people; listen and share; suggest a common move, and share again. Such an attitude should be quite natural, it is far from being the case. But the result is crystal-clear: if you go beyond your bunker, if you inject trust and positive thinking, then the reward will be great. There is nothing of the kind in our distinguished decision theory, but the bottom line is there: if you trust, you will be trusted, and you will be able to invent, creatively beyond ordinary frontiers and silos.

Immediate Measurable Output: Strategic Partnership

The "Anthrax and Beyond" initiative produced more than the sharing of experience and lessons. It constituted the first steps in creating a network to improve the overall reaction among postal networks in case of a new transnational threat. It also launched an international partnership among postal operators to create a global crisis-management network. This network will allow executives of all the European and U.S. operators to connect instantly. Using this tool, they can exchange information about the solutions each country is implementing and 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 about a possible anthrax contamination around Washington, D.C.[34] The network provided postal services across Europe with accurate and timely information on this potential incident, enabling them to assess the scope of the risk. This was a large step beyond the situation in November 2001, described above, when the chairman of a large postal operator could not talk on the phone with two of his counterparts. The 2003 threat eventually proved to be a false alert, but it was a dramatic kick-off for the network; this global reaction capacity is still operating today.

MOVING FORWARD: NEW LEADERS WANTED

The Guns of August crushed Europe in 1914.[35] What we might call the *Planes and Letters of 2001*, and other waves of catastrophes on a totally new scale, are setting the scene today, with stakes of similar historical importance. The vision is clear: fiasco is not an option. Society has a collective responsibility: to transform emerging global ruptures into emerging global opportunities, and ensure that collective answers are reactive and scaled to the new scene. As the growing globalization of social and economic activities leads to increasing cross-industry and cross-country interdependencies, and large-scale risks are associated with great scientific uncertainty (if not ignorance), global actors are no longer playing conventional chess.

Events around the world over the past five years have shown that today a single event (or threat) can destabilize a whole set of firms or industries, or even several countries, and quickly inflict losses of billions of dollars. In that spirit, boards in both industry and government have begun to consider these issues urgently, but budget allocation—prioritizing limited resources—remains a crucial strategic decision.

Along with preparing executives in charge, it is crucial to train top leaders, as they have the hardest task in this new environment. Any crisis targets the leaders first. If they fail to act adequately, then the whole organization, or country, can sink into crisis, bringing others with it. Therefore, as our involvement in the "Anthrax and Beyond" initiative illustrates, it is essential to introduce and develop strategic and trusted catalyst teams. Composed of individuals from both inside and outside the organization, these teams can advise top leaders on emerging questions, formulate challenging questions, suggest bold innovations, and engage with multiple bodies outside the organization. As we have demonstrated above, these are not just consulting firms brought in to improve the company's image. Above all, catalyst teams are capable of and allowed to take bold initiatives with pilot projects involving unusual circles of people and organizations.

The Anthrax and Beyond initiative illustrates successful collective actions, partly because it was a pragmatic way to produce concrete outputs, and thus measurable benefits for all stakeholders, whether in terms of better preparation or financial return on investment. But conferences are no longer enough. We must go beyond the usual borders to develop high-level collective actions across industries and across countries.

The beginning of a crisis is not a good time to start exchanging business cards. Responses improvised during a crisis will be incomplete: *ex ante* collaboration must buttress responses by making institutions durable and flexible enough to allow interdependent actors to coordinate quickly. Before the unthinkable confronts us again, we must forge patterns and institutions that allow a disjointed, but interdependent, set of actors to respond effectively. As one very concrete approach, we advocate the proactive establishment of what we call "Rapid Reflection Forces" (see box).

Partnerships are necessary not only during a crisis as tools of response; they also have crucial *ex ante* functions. To facilitate crisis response, partners must share information, pool the costs of research and development, and establish relationships that can later function as key strategic resources, before a disturbing event begins. We are not talking about rote global plans—which would fail in the face of the unpredictable and novel— but rather about recognizing the interdependent nature of security and forging institutions that respect the unique challenges that emerge between players who are both mutually dependent and in competition.

Recently we have observed an encouraging and important trend. Rather than leaving risk managers to tackle these issues alone, several companies have recognized the strategic aspect of these questions and have now put them on the agendas of their boards. International organizations, such as the Organization for Economic Co-operation and Development (OECD) and the World Economic Forum in Switzerland, have now also made these large-scale risk issues a priority in their future action plans. These new initiatives could lead others to act too, and eventually move toward a new way of managing international crises. These issues were discussed in Davos earlier this year[36] and will get even more attention from world leaders at the January 2007 forum.

Each critical sector has its own set of key processes, activities, institutional and legal arrangements, and cultures. While "Anthrax and Beyond" used postal security as a large-scale pilot initiative, the framework we have introduced here would apply to similar international initiatives in other industries, where growing threats challenge the continuity of interdependent networks. These industries include

The Concept of "Rapid Reflection Forces"

Like the military's "Fast Action Forces" that apply strategy on the ground, we suggest creating "Rapid Reflection Forces" in every large corporation and institution, to clarify strategy and to define where to go, from where, with whom, and why, during crisis episodes.

The first priority is to empower a special team that can ask fresh questions, find fresh approaches, and work on them very hard and creatively. Team members are from the company and from outside, and they need special training:;they need not have all the answers to predetermined scenarios, but must know how to succeed in a crisis by being level-headed, creative, and able to work with others under pressure.

The team then needs a methodology for exploring the unknown and for clarifying a way out of crisis. Experience shows that the team must work on four seminal questions.

1. What is the essence of the problem? Generally people rush into a problem without really understanding its complexities. For example, a Class-5 hurricane is not just another hurricane; it is an "outside the box" disaster. The challenge is to clarify what the situation is really about, beyond the initial perception. Actors must repeatedly ask this question, throughout the crisis.

2. What are the key traps? Generally, fear and stress generate instant collapses and lead to terrible choices and devastating media communication. This is easy to understand but must be avoided. To avoid an instant quagmire, actors must continually ask, "What are the key mistakes to avoid?" during the crisis and right until the very end.

3. Who are the stakeholders? Unconventional crises cannot be solved solely by and with conventional actors. Commonly, crisis managers tend to work with the very few people they know. During an inconceivable event decision-makers must redefine their networks.

4. Which strategic initiatives are vital? During a severe and disturbing event, it is essential to restore sense, to re-establish balance, and to initiate powerful new dynamics. The way to do this is to launch some very specific initiatives, with some very specific people, at the right moment. This may be the most difficult challenge: to identify and define two or three specific actions that the team can implement to inject confidence, positive dynamics, and movement.

"Rapid Reflection Forces" must be able to link and interact extremely well with the very top management strata of the organization, which calls for a specific and crucial preparation effort. This process has just been launched in several leading organizations.

transportation, telecommunication, defense, energy, banking and finance, insurance, water supply, and hospitals and health systems. In each area collaboration must occur at many levels, and cannot include only public organizations. As risks become global and service provision mixes public and private action, international public and private participants must collaborate to survive. For example, it would have been of prime importance to launch a similar initiative with top-executives of the commercial airline industry and trade associations in the aftermath of the SARS episode, or after the summer 2005 terrorist attempt in the UK. To our knowledge, this has not been done yet.

Fortunately, some leading companies now see the need to visit, learn from, and share with teams that have confronted unusual events. This year, for instance, *Electricité de France* (EDF), one of the world's larger nuclear electricity providers, undertook to document the lessons that Toronto officials learned from the SARS episode, to prepare for a possible flu pandemic;[37] EDF, as other key companies and organizations, also considered the lessons of Hurricane Katrina by sending a core team made of EDF top managers and external experts in Louisiana and Washington, DC.[38] While these events do not relate directly to their core activities, all large organizations must learn from others about destabilizing events in other industries and countries.

As the saying goes, *When you see a venomous snake, kill it. Do not create a Snake Commission*. As we will face more and more chaotic environments, we must move from words to work, from visions to actions. Although much remains to be clarified, we cannot "wait and see." We need new answers to new problems and they will not simply fall "as a gentle rain from heaven." This paper provides some guidance as to how to do it. Eventually, proactive cooperation may be the only proven way to re-establish faith in our critical infrastructure services. And then the United States and other countries will be ready for prime time.

We invite reader comments. Email <editors@innovationsjournal.net>.

[1] Personal communication, 2004.

[2] U.S. House of Representatives. 2006. *A Failure of Initiative: Final Report of the Select Bipartisan Committee to Investigate the Preparation for and Response to Hurricane Katrina*, U.S. Government Printing Office, 15 February 2006, Washington, DC, p. xi.

[3] Risk management theory distinguishes *risk* (both the distribution of probability and consequences are well known), from *uncertainty/ambiguity* (the probability or consequences are not certain) and *ignorance* (neither the probability nor the potential consequences are known).

[4] Lord Philips of Worth Matravers, J. Bridgeman and M. Ferguson-Smith. 2000. *The BSE Inquiry, vol 1: Findings and Conclusions*. London: Stationery Office.

[5] Pile, J., J. Malone, E. Eitzen, A. Friedlander. 1998. "Anthrax as a Potential Biological Warfare Agent," *Archives of Internal Medicine,* March 9, Vol. 158, p. 429.

[6] Inglesby, T. et al. 1999. "Anthrax as a Biological Weapon," *Journal of American Medical Association,* May 12, 281(18), p. 1736.

[7] Inglesby, T. et al. 1998. "Anthrax as a Biological Weapon"; "Bioterrorism Alleging Use of Anthrax and Interim Guidelines for Management—United States, 1998," *Morbidity and Mortality Weekly*

Report, Feb. 5, 48(4), p.69-74; Center for Disease Control and Prevention, *Preventing Emerging Infectious Diseases: A Strategy for the 21st Century.* Atlanta, GA: CDCP, p.47.

8. After the hoaxes, a report written by the Defense Research Establishment Suffield, a Canadian government laboratory, stated with prescience: "It is only a matter of time until a real 'anthrax letter' arrives in some mail room." That did happen less than a year later. Defense Research Establishment Suffield (DRES) 2001. *Risk Assessment of Anthrax Threat Letters*, Technical Report, DRES TR-2001-048, p. 13.

9. For example, in the 1960s U.S. Department of Defense studies simulated an attack in a subway car; in the 1970s the WHO considered the likely impact of releasing a large amount of anthrax from an airplane over a densely packed area (such as a city block). J. Pile. et al., "Anthrax as a Potential Biological Warfare Agent," p. 433. In the 1990s Aum Shinrikyo used sarin gas in the Tokyo subway, providing a contemporary (false) analogue that some saw as a possible model for a successful anthrax attack, and by 1999 at least 17 nations were thought to have offensive biological weapons programs potentially including stocks or experiments relating to anthrax. Thomas V. Inglesby, et al., "Anthrax as a Biological Weapon," p. 1736. Note that such a scenario is not to be excluded either. More generally, terrorist attacks using weapons of mass destruction (chemical, biological, radiological or nuclear) are certainly seen today as worst case scenarios, but still quite plausible.

10. DRES, *Risk Assessment of Anthrax*; "Bioterrorism Alleging Use of Anthrax."

11. Ibid.

12. An uncertain LD_{50} of between 2,500 and 55,000 spores was posited based on older animal tests as well as one known deadly case of widespread aerosolized anthrax that occurred during an accident at a military microbiology facility in the city of Sverdlovsk, then in the USSR, in 1979. M. Meselson, et. al. 1994. "The Sverdlovsk Anthrax Outbreak of 1979," *Science*, Vol. 266, p. 1202-1208; Inglesby, et al., "Anthrax as a Biological Weapon," p. 1737.

13. DRES, *Risk Assessment of Anthrax.*

14. Ibid.

15. Several factors combined to create this situation. The risk posed by the presence of anthrax is a function of quantity, individual health, and mode of exposure. One spore, under the right conditions, could be deadly. Also, the available testing and sampling methods could not establish the absence of anthrax (negative tests were unreliable). For a full discussion of the problems of testing and tracking, see U.S. Government Accounting Office. 2003. *Better Guidance is Needed to Improve Communication Should Anthrax contamination occur in the Future, Report to the Ranking Minority Member Committee on Governmental Affairs, U.S. Senate,* GAO-03-316, Washington, DC; K. Rhodes and B. Unger. 2003. *Issues Associated with Anthrax Testing at the Wallingford Facility, Testimony Before the Subcommittee on National Security, Emerging Threats, and International Relations, Committee on Government Reform*, GAO-03-787T, Washington, DC. 03-787T, pp.9-10.

16. Rhodes and Unger, 2003.

17. Ibid.

18. Weinberg, A. 1985. "Science and its Limits: The Regulator's Dilemma," *Issues in Science and Technology* 2 (1), pp. 59-72. Quoted in J. Kandra and T. Wachtendorf. 2003. "Elements of Resilience After the World Trade Center Disaster: Reconstituting New York City's Emergency Operations Center," *Disaster*, 27 (1), pp. 37-53.

19. See chapter 1 in P. Auerswald, L. Branscomb, T. LaPorte and E. Michel-Kerjan, eds. 2006. *Seeds of Disaster, Roots of Response. How Private Action Can Reduce Public Vulnerability*, Cambridge University Press, pp. 534.

20. The presence and belated detection of anthrax at the Wallingford, CT. facility in early December of 2001 points specifically toward this problem and illustrates that adequate downstream modeling techniques were not available. This facility, later tied to the death of one elderly postal customer, was considered an unlikely site for exposure and was tested three times without any anthrax being detected. However, a fourth test, after the customer died, did establish the presence of anthrax at the facility. GAO-03-316; GAO-03-787T.

[21] It would not work to exclude shipments from networks identified as having been exposed, because exposure could come from a third party that had not yet or not quickly enough cut ties with an exposed network. Here, security is clearly interdependent.

[22] Fink, S. 1986. *Crisis Management: Planning for the Inevitable.* New York City: Amacom, American Management Association, p. 81.

[23] See United States Postal Service (USPS). 2002. *United States Postal Service Transformation Plan.* Washington, DC. Appendices C, E, H, I. See also R. Reisner. 2002. "Homeland Security Brings Rate-payers vs. Taxpayers to Center Stage," in M. Crew and P. Kleindorfer, eds., *Postal and Delivery Services. Delivering on Competition*. Amsterdam: Kluwer, pp. 223-242.

[24] For a discussion of security externalities and the inability of competitive markets to account for catastrophes and disasters that are difficult or impossible to predict, see P. Auerswald, et. al. 2006, pp. 534.

[25] After the attacks, U.S. officials were very intent on courting customers (particularly large-volume mailers). See Government Accounting Office. 2001. "Highlights of GAO's Conference on Options to Enhance Mail Security and Postal Operations," GAO-02-315SP, Washington, DC: GAO.

[26] Insurance can play an important role here. It is the world's largest industry in terms of revenues generated: three times the size of the oil industry as of December 2004. While the anthrax attacks did not severely affect the industry, three of the past five years have set records as the most costly ever in the history of insurance worldwide. What caused these records? Three extreme events in the U.S.: the 9/11 attacks, and the 2004 and 2005 hurricane seasons. Insurers are now redefining their business model; some have decided to stop covering certain risks in areas with high concentrations of value at risk. See E. Michel-Kerjan. 2006. "When Insurance Meets National Security: The Unnoticed Paradox of Critical Infrastructure Protection," Unpublished working paper, The Wharton School, Center for Risk Management and Decision Processes, Philadelphia, PA.

[27] Stacey, R. 1996. *Strategic Management and Organizational Dynamics*. London: Pitman, pp. 19-20.

[28] Mitroff, I. and T. Pauchant. 1990. *We're So Big And Powerful Nothing Bad Can Happen To Us: An Investigation of America's Crisis-Prone Corporations.* New York: Birch Lane Press.

[29] Phillips, Bridgeman, and Ferguson-Smith, *BSE Inquiry,* section 1176; op. cit. 2000

[30] Loch, S. and H. Kunreuther, eds. 2001. *Wharton on Making Decisions*. New York: John Wiley & Sons.

[31] The concept is introduced, defined and illustrated by Auerswald, et al., *Seeds of Disaster, Roots of Response*, Chapter 1.

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

[33] For a detailed analysis of this initiative, see P. Lagadec and U. Rosenthal, eds. September 2003. "Anthrax and Beyond: New Challenges, New Responsibilities," *Journal of Contingencies and Crisis Management*, Special Issue, Volume 11, Number 3.

[34] This happened after a positive test result: a piece of mail addressed to the U.S. Federal Reserve passed through a postal facility in the District of Columbia.

[35] Tuchman, B. 1962. *The Guns of August*. Toronto: Bantam.

[36] World Economic Forum. 2006. *Global Risks 2006* ; in collaboration with Marsh & McLennan, Merrill Lunch and Swiss Re, and in association with the Risk Management and Decision Processes Center at the Wharton School of the University of Pennsylvania; Geneva: World Economic Forum,

[37] Lagadec, P. and W. Dab. 2005. *Managing Vital Activities in an Unpredictable World: The large network operators and pandemic risks.* Paris: Electricité de France, Risk Management Division, November.

[38] Guilhou, X., P. Lagadec, and E. Lagadec 2006. "Non-Conventional crises and critical infrastructures. Katrina: Report-back Mission", New Orleans, Gulfport, February 19-25, 2006; Washington, DC, March 13-15, 2006, EDF, Risk Management Division, July 2006.