Ten Uncertainties of Risk-Management Approaches to Security

Richard V. Ericson
Centre of Criminology
University of Toronto

L'auteur analyse 10 sources d'incertitude pouvant compromettre tout système de gestion du risque et les illustre par des exemples de mesures antiterroristes. (1) Toute évaluation du risque est une affirmation incertaine de savoir concernant des événements futurs dont on ne pourra saisir pleinement la nature. (2) On ne peut porter son attention que sur un nombre restreint de risques, et les autres risques non traités sont des sources d'incertitude. (3) Certaines décisions en matière de gestion du risque véhiculent l'incertitude de faux positifs ou de faux négatifs. (4) Les technologies de gestion du risque engendrent de nouvelles incertitudes, dont certaines présentent des risques plus graves que ceux visés par ces mêmes technologies. (5) Les risques se multiplient par un phénomène de réaction : en agissant en fonction des risques identifiés, on modifie l'environnement du risque et on fait naître de nouvelles incertitudes. (6) En raison de leur complexité, les systèmes de gestion du risque peuvent aboutir à des défaillances multiples et imprévues qui surviennent simultanément; ces « accidents normaux » représentent une source d'incertitude qui échappe au contrôle direct de l'humain. (7) À la suite de défaillances catastrophiques, la tentation est forte d'imposer la gestion du risque à toutes les activités; or, l'accroissement des mesures de surveillance, de vérification ou de réglementation augmente la complexité des systèmes ainsi que le niveau d'incertitude. (8) Les responsables de la gestion du risque, qui doivent évoluer dans un contexte où les défaillances font de plus en plus l'objet d'actions en justice, adoptent une posture défensive en prenant davantage en compte les risques opérationnels pouvant compromettre la réputation de leur organisation que sur les risques véritables qu'il leur appartient, en principe, de gérer. (9) Un excès de prudence augmente l'incertitude, suscite la peur, et engendre par conséquent des mesures de gestion du risque qui sont mal adaptées quand elles ne provoquent pas de nouveaux risques de catastrophes. (10) Les systèmes de gestion du risque peuvent restreindre les libertés, envahir la vie privée et faire en sorte que certaines populations soient victimes de discrimination ou d'exclusion. Enfin, la seule façon de minimiser ces tendances coûteuses et destructives et les incertitudes qu'ils engendrent consiste à modifier les *systèmes de gestion du risque en posant aux acteurs des questions de valeur portant sur les droits de la personne, le bien-être, la prospérité et la solidarité.*

This paper examines 10 sources of uncertainty in any risk-management system and illustrates them in security measures against terrorism. First, any risk assessment is an uncertain knowledge claim about contingent future events that cannot be fully known. Second, only some risks can be selected for attention, and those left unattended are sources of uncertainty. Third, specific decisions in risk management bear the uncertainty of false positives and false negatives. Fourth, risk-management technologies manufacture new uncertainties, some of which pose risks greater than those they were designed to control. Fifth, risk is reactive: as people act on knowledge of risk, they simultaneously change the risk environment and create new uncertainties. Sixth, the complexity of risk-management systems can result in multiple and unexpected failures occurring simultaneously; such "normal accidents" are a source of uncertainty beyond any direct human capacity for control. Seventh, catastrophic failures result in the urge to risk manage everything: intensified surveillance, audit, and regulation increase system complexity and yield more uncertainty. Eighth, risk managers facing an increasingly litigious environment for failures become defensive, focusing more on operational risks that might affect the reputation of their organization than on the real risks they are supposed to manage. Ninth, excessive precaution escalates uncertainty and breeds fear, leading to risk-management measures that are at best misplaced and at worst incubate new risks with catastrophic potential. Tenth, risk-management systems can restrict freedom, invade privacy, discriminate, and exclude populations. Such self-defeating costs and the uncertainties they entail can be minimized only by infusing risk-management systems with value questions about human rights, well-being, prosperity, and solidarity.

Any risk-management approach to security must start from the premise that uncertainty is the basic condition of human knowledge. Risk-management systems are always surrounded by uncertainties that make security provision far from perfect. In this article I briefly sketch 10 uncertainties of any risk-management system, with application to the risk of terrorist activity.

I. Risk is a statement of uncertainty

Risk is the probability of contingent harm, assessed in terms of frequency of occurrence and severity of loss. While statements of risk are intended to provide more certainty, they also convey uncertainty. They are at once expressions of knowledge and expressions of ignorance: uncertain knowledge claims about contingent future events that cannot be fully known (Adams 1995, 2003).

The capacity to assess and manage risk varies by the type of harm involved (Hood, Rothstein, and Baldwin 2001; Ericson and Doyle 2004a). Terrorist activity is especially difficult to assess in terms of frequency and severity (Ericson and Doyle 2004b). Terrorism is intentional catastrophe that can occur anywhere, at any time, repeatedly (Reuter 2004). Indeed, terrorists are in the business of uncertainty, playing on randomness to keep whole populations in fear, anticipation, and disestablishment. They precipitate an urge in the population for more certainty – expressed through escalating security measures – but are adept at grasping the rationality of each new security measure in order to subvert it and induce more uncertainty. The terrorist power of uncertainty is especially strong precisely because we live in a society dominated by the desire to tame chance and by institutions increasingly organized around risk management. Terrorism strikes at the foundation of this culture because it is a stark reminder of the limits of risk management. It brings home the potential ungovernability of modern societies, and how those with little power can work cheaply and effectively to destroy.

2. Risk selection

There are countless sources of harm in the world, only some of which can be subject to attention and risk management. Risk selection is in part a question of knowledge: Is the risk directly perceptible, subject to mediation by experts, or virtual in the sense of being easy to imagine but impossible to observe (Adams 1995, 2003)? Risk selection is also a social, cultural, political, and economic process. A few potential sources of harm are brought to the centre of a risk-management portfolio because they are believed to have the greatest potential for adversely affecting the interests of portfolio stakeholders. Risk portfolios are often constituted in politically charged contexts where the risks selected are used to define values, interests, and ways of life beyond probabilistic reasoning (Douglas 1990; Hacking 2003).

Prior to 9/11 there were repeated attacks on American targets by al-Qaeda, including one on the World Trade Center (WTC). However, it was the catastrophic events of 9/11 that precipitated the move of terrorism to the centre of the risk portfolio of Western societies. An executive of a reinsurance company that paid out several billion dollars in claims following 9/11, articulating his views on catastrophic risk selection, has said his company was aware of various assessments of the new terrorism prior to 9/11, including the possibility of a second al-Qaeda attack on the WTC aimed at total destruction. However, only a few possible sources of catastrophic loss are brought to the centre of the company's risk portfolio at a given time, and prior to 9/11 terrorism was not one of them:

> An international reinsurer is supposed to have a certain experience with catastrophes. But the question is... given the diversity of liability scenarios, how can we meaningfully process such experience? This is scarcely possible using actuarial methods alone. It calls for professional methods that are probably more akin to those of a social historian than those of an actuarial scientist or legal expert... So the problem is not know or not to know, the problem is... what you should consider... This is a sophisticated game, obviously, but this sophisticated game is based on four, five, six catastrophes out of twenty, forty, fifty. And this selection is absolutely based on, I don't know what, casual developments. And so the whole basis of this sophisticated game is not so sophisticated. (Ericson and Doyle 2004b: 144)

3. False positives and false negatives

All case-specific decisions in risk management bear the uncertainty of false positives (wrongly identifying a source of harm and acting upon that source unnecessarily) and false negatives (failing to identify a source of actual harm and therefore failing to act in ways that might reduce that harm). This uncertainty is rooted in the two previous points: that risk is a statement of uncertainty and involves selection. A risk-management system is based on prior conventions for recognition, selection, assessment, and evaluation, which, in turn, are grounded in institutions, values, interests, and ways of life. Aggregate data of population risks can never be used precisely to indicate whether the case under scrutiny is an actual source of harm: Probabilities offer only possibilities. Decisions are also taken on the basis of knowledge that is intuitive, emotional, aesthetic, moral, and speculative.

Criminologists have long grappled with the problems of false negatives and false positives in their efforts to identify and risk-manage dangerous offenders. The same conundrums and issues are salient in efforts to identify and deal with potential terrorists. It is now painfully evident that the vast majority of those detained as possible terrorists post-9/11 are false positives (Stafford Smith 2005;

Greenberg and Dratel 2005). Countless others have been discriminated against, but were fortunate enough to have the problems of the risk-assessment system identified at an early stage to avoid prolonged exclusion. At the same time there have been instances of false negatives, beginning with those who succeeded on 9/11 and continuing with repeated instances worldwide, such as the attacks in Bali in October 2002 and Madrid in March 2004.

4. Technological failure

Technological failure always looms in risk-management approaches to security. Pharmaceutical products developed to manage health risks have side effects that produce new health risks. Auditing systems designed to effect financial system risk management are implicated in new risks to the financial system. Such failures and their unanticipated consequences are part of what Ulrich Beck (1999) calls "manufactured uncertainties": The very effort to achieve prosperity, well-being, and security through science and technology yields new risks and uncertainties. Indeed, such failures have become the focal point of the contemporary politics of uncertainty.

The post-9/11 race to develop surveillance technologies to identify terrorists exemplifies problems of technological failure. One example is the installation of facial recognition technology at Boston's Logan Airport, the origin of two of the flights involved in the 9/11 attacks. This technology produced too many false positives, creating problems not only for those falsely detained but also for the overall efficiency of airport operations. The technology was abandoned, illustrating that a key limit on the use of security technology is interference with the smooth flow of economic relations.

5. Reactive risk

When people act with knowledge of risk, they change the risk in the very course of their actions. "[R]isk perception is risk acted upon. It changes in the twinkling of an eye as the eye lights upon it" (Adams 1995: 30). For example, a driver continually assesses risk and immediately responds to it depending on the performance and safety features of the vehicle, road conditions, and so on. Risk taking and risk management are simultaneous. The person who is too cautious – too reflexive about risks in the driving environment, to the point of not taking reflexive driving action routinely – can pose the greatest risk.

Terrorism exemplifies reactive risk. In the business of uncertainty, terrorists threaten and carry out acts of intentional catastrophe that play on the fragility of risk-management systems. They know that "the true source of uncertainty lies in the intentions of others" (Bernstein 1998: 232). They are adept at revealing an irony of risk management: Every effort to refine it is also an exposure of its vulnerabilities that can be acted upon to create more risk.

6. Normal accidents

Uncertainties are embedded in risk-management systems. "The odd term *normal accident* is meant to signal that, given the system characteristics, multiple and unexpected interactions of failures are inevitable" (Perrow 1984: 5). Ironically, the very effort to refine scientific risk assessment, risk selection, risk technologies, and reactive risk processes yields complex risk-management systems that are prone to failure. Normal accidents are system-based accidents, a consequence of interactive complexity and tight coupling of system components aimed at efficient operations.

It is now widely recognized that risk-management system failures contributed to the inability to prevent the 9/11 terrorist attacks (Kean and Hamilton 2004). In this respect 9/11 was a normal accident. The threat of a major al-Qaeda attack on the United States was a known risk and under active investigation by the FBI and other authorities. Myriad surveillance mechanisms were in place to monitor characteristics of suspect populations. Airport security systems were operational, as were air traffic control flight-tracking systems. Nevertheless, the system failed to capture the catastrophic intentions of any of the culprits at any stage of their enterprise.

7. The risk management of everything

The response to inevitable failures in risk management is further refinement of risk-management systems. There is always the belief that more will work where less has not, to the point that there is now organizational obsession with "the risk management of everything" (Power 2004). Vigilance in attributing the probability of, responsibility for, and management of every conceivable source of harm reaches the point where risk management becomes *the* basis of organizing. On the one hand, risk management provides a rhetoric of reassurance, enacting myths of control, manageability, and accountability. Organizations are thereby infused with a renewed sense of strategic value regarding their capacity for control. "Risk management organizes what cannot be organized . . . holds out the promise of manageability in new areas . . . implies a new way of allocating responsibility for decisions which must be made in potentially undecideable situations" (Power 2004: 10). On the other hand, myths constitute realities. There is a new risk managerialism based on internal control systems of surveillance, audit, and regulation.

In these internal control systems, a risk-based approach and a rules-based approach go hand in hand. Efforts at risk management and regulation do create a safer world, as well as high expectations and trust that security will be provided. However, these efforts also expose the limits of knowledge and the extent of uncertainty: wrong decisions (e.g., false positives and false negatives), technological failures, normal accidents. Expectations are dashed, trust is eroded, and the risk management of everything intensifies.

The post-9/11 surveillance environment exemplifies the risk management of everything (Haggerty and Ericson 2006). Through the enactment of exceptional legislation that pre-empts legal principles and standards, and through multi-billion-dollar surveillance infrastructures enabled by this legislation, the U.S. government dreams of creating "total information awareness" (Whitaker 2006). Extraordinary economic and human costs are incurred in the hope that security benefits will accrue. However, security remains more within us as a yearning than outside us as a fact, and the risk management of everything inevitably produces new uncertainties.

8. Displacement to organizational risks

The risk management of everything includes increasing focus on operational risks to the organization. As Power (2004: 40) observes, "demand for the governance of the unknowable requires organizational proceduralisation." First, the elaboration of rules and procedures and intensification of surveillance creates a culture of "defendable compliance" and "responsibility aversity" as organizations' members are rewarded for demonstrating that they have followed procedures when things go wrong and thereby avoid blame. Second, the internal risk-management system is designed to collect data on everything possible. Many of the data collected are irrelevant to operations and consume resources unnecessarily.

Data collection continues, however, because it is what risk managers need to demonstrate that they are indeed managing some risk, if not those that are actually the greatest sources of potential harm to the organization. Third, since anything can be a possible source of operational risk, stakeholders external to the organization are also understood and managed as risks. This category includes customers of the organization, who are treated as risks on two levels: their capacity to contribute to the profits of the organization (market segmentation) and whether they are likely to be litigious about product safety and quality. Fourth, the organization engages in reputational risk management, for example, through corporate social responsibility measures that suggest the organization is concerned about the public good as well as the bottom line. Unless these measures are accompanied by substantive evidence of better performance, however, they will backfire. The greater the need for reputational risk management, the less successful it is likely to be. Fifth, all of the above processes displace expert judgement in favour of defendable compliance and reputation. Organizational actors think, act, and communicate within the four-square corners of risk classification schemes and internal procedures, and they avoid making hard decisions and expressing opinions that are more honest. "This trend is resulting in a dangerous flight from judgment and a culture of defensiveness that create their own risks for organizations in preparing for, and responding to, a future they cannot know" (Power 2004: 14–15). Sixth, without such judgement there will be more normal accidents. There is the real operational risk of "incubation" and "tunnel vision," whereby relevant risk information about real threats is available but is not accessed or acted upon because actors are operating within the narrow grooves of internal risk management and regulation. "[C]rises and catastrophes do not just happen suddenly; they are in an important sense 'organized' and have their origins in failures of management and intelligence processes over a long period of time" (Power 2004: 44).

It is likely that the proliferation of risk management systems and regulations in the wake of 9/11 has led to all of these facets of displacement to organizational risks. Indeed, the failure to prevent the events of 9/11 can itself be partly understood in these terms (Kean and Hamilton 2004). In this respect, the response to the radical uncertainty of terrorist activity has parallels to other fields of risk and regulation, for example, dealing with rogue traders on financial markets or contaminated products. In all such cases, uncertainty is translated into operational risks that are at least

> describable, and, in aspiration, manageable. Killer events and sources of fear become translated into routines, regulations and data collection processes; anxiety, as the secondary risk of attempting to manange the unmanageable, is "tamed" by a kind of naming. (Power 2004: 31; see also Hutter and Power 2005)

9. Too much precaution

The risk management of everything and displacement to organizational risks are driven by excessive precaution. Indeed, in many contexts the operating principle seems to be one of pre-caution: even being cautious about how one is being cautious. An increasing number of risks are seen as having catastrophic consequences, so that, regardless of the fact that the likelihood of actual harm is remote, extraordinary measures must be taken to pre-empt them. Most people overestimate the risk of low-frequency, high-severity events (catastrophes) and underestimate the risk of high-frequency, lower-severity events (home, school, work, and road accidents) (Sunstein 2002, 2005). For example, if people see violent crime, nuclear fallout, or a terrorist attack as a risk that has no price, they will invest in and support extreme precautionary measures, beyond any scientific assessment of risk. Indeed, they will be sceptical of or even ignore scientific knowledge (Sunstein 2002, 2005). If they do consult science, it will be less for the certainty it offers than for the doubt it insinuates (Ewald 2002).

Precautionary logic is evident in the mobilization of security measures against terrorism following 9/11. 9/11 crystallized a pre-existing societal trend toward precaution regarding various types of risk that have catastrophic potential, including health (AIDS, BSE, genetically modified foods, blood supplies), public safety (especially child safety), and the environment (pollution, nuclear energy production, global warming). The post-9/11 catastrophic imagination envisaged the World Trade Centre as "Ground Zero," language drawn from nuclear war. The U.S. government's build-up of extraordinary legal powers and police, military, and airport security measures is widely experienced. There has also been an extensive security build-up in commercial settings, underpinned by the private security industry

(Ericson and Doyle 2004a, 2004b). In New York alone, the City Comptroller estimated that over the four years following 9/11, there would be a 23% increase in private security personnel, at a cost of a billion dollars. He also noted that more than 1% of all workers in New York City are in private security (Thompson 2002). Under the Homeland Security regime, there is an effort to mobilize all U.S. citizens as watchers as well as watched and as bearers of their own control (see U.S. DHS 2006). Spying has become a civic duty, bolstered by an extravaganza of new surveillance technologies such as an $8.6 million CCTV system recently installed in Chicago that is "equipped with software that will raise the alarm when the cameras spot people loitering, wandering in circles, hanging around outside public buildings, or stopping their cars on the shoulders of highways" (Raban 2005: 25). Surveillance extends to all manner of communication. For example, the Department of Homeland Security co-sponsors, with the FBI and the Justice Department, the "Operation Predator" system to track paedophiles via their use of the Internet,

> presumably because pedophiles, whose civil liberties are held in high esteem by almost nobody, are indeed guinea pigs for a more sweeping exercise in cyberspying that might net terrorists... our e-mails, shared files, and visits to suspect Internet sites are obviously more likely to identify us as al-Qaedists than any tendency we may exhibit to wander in circles in front of tall buildings. (Raban 2005: 25)

10. Costs more than benefits

Ideally, risk-management systems maximize freedom of action to take risks while reducing that freedom's harmful consequences. While many risk-management regimes have great success in this regard, others come with extraordinary costs in terms of restricting freedom and perpetuating harmful consequences. Terrorism risk management post-9/11 is a case in point, to the extent that it has victimized those who have been wrongly incarcerated, transported, or more subtly excluded, and to the extent that it has victimized everyone through invasion of privacy, restriction of liberty, and compulsory spending on physical security infrastructures at the expense of health, education, and welfare sources of security. The risk management of everything can consume future resources excessively, thereby closing off options for the future. This cost can be overcome only through an appreciation that there will be inevitable failures in risk management and that more resources directed at intensified risk management may create new uncertainties and sources of failure.

Frantic efforts at risk management in the name of precaution can tear at the social fabric. The risk management of everything can bear the cost of declining trust in experts and institutions. This decline is intensified if the risk-management system is widely viewed as restricting freedom and perpetuating discrimination and other forms of injustice. The result can be a fierce politics of uncertainty involving fundamental disagreements over questions relating to social cohesion and solidarity: Who is willing to embrace what risk at what price? Who will share risk distribution, at what levels of exposure? Who will be included and excluded? Such judgements about risk are value judgements, and cost–benefit analyses are infused with values. In order to limit the restriction of freedom, the normalization of injustice, unnecessary consumption of future resources, and erosion of the social fabric through risk-management systems, there is a need to keep value questions at the forefront, beyond technical risk management (Ignatieff 2004). These value questions include human rights, economic development that spreads prosperity and well-being more equitably, and collective solidarity. If these values are not embedded in the creative design of risk-management systems, these systems are more likely to have many of the self-defeating costs outlined here, and uncertainties will accelerate.

References

Adams, John
1995 Risk. London: UCL Press.

Adams, John
2003 Risk and morality: Three framing devices. In Richard V. Ericson and Aaron Doyle (eds.), Risk and Morality. Toronto: University of Toronto Press.

Beck, Ulrich
1999 World Risk Society. Cambridge: Polity Press.

Bernstein, Peter
1998 Against the Gods: The Remarkable Story of Risk. New York: Wiley.

Douglas, Mary
1990 Risk as a Forensic Resource. Daedalus 119: 1–16.

Ericson, Richard V. and Aaron Doyle
2004a Uncertain Business: Risk, Insurance and the Limits of Knowledge. Toronto: University of Toronto Press.

Ericson, Richard V. and Aaron Doyle
2004b Catastrophe risk, insurance and terrorism. Economy and Society 33: 135–173.

Ewald, François
2002 The return of Descartes's malicious demon: An outline of a philosophy of precaution. In Tom Baker and Jonathan Simon (eds.), Embracing Risk: The Changing Culture of Insurance and Responsibility. Chicago: University of Chicago Press.

Greenberg, Karen and Joshua Dratel
2005 The Torture Papers: The Road to Abu Ghraib. New York: Cambridge University Press.

Hacking, Ian
2003 Risk and dirt. In Richard V. Ericson and Aaron Doyle (eds.), Risk and Morality. Toronto: University of Toronto Press.

Haggerty, Kevin and Richard V. Ericson, eds.
2006 The New Politics of Surveillance and Visibility. Toronto: University of Toronto Press.

Hood, Christopher, Henry Rothstein, and Robert Baldwin
2001 The Government of Risk: Understanding Risk Regulation Regimes. Oxford: Oxford University Press.

Hutter, Bridget and Michael Power (eds.)
2005 Organisational Encounters with Risk. Cambridge: Cambridge University Press.

Ignatieff, Michael
2004 The Lesser Evil: Political Ethics in an Age of Terror. Princeton, NJ: Princeton University Press.

Kean, Thomas and Lee Hamilton
2004 The 9/11 Report. New York: St. Martin's Press.

Perrow, Charles

1984 Normal Accidents: Living with High-Risk Technologies. New York: Basic Books.

Power, Michael

2004 The Risk Management of Everything. London: Demos.

Raban, Jonathan

2005 The truth about terrorism. New York Review of Books, January 13: 22–26.

Reuter, Christoph

2004 My Life Is a Weapon: A Modern History of Suicide Bombing. Princeton, NJ: Princeton University Press.

Stafford Smith, Clive

2005 Representing "the enemy": Human rights and the war on terror. Criminal Justice Matters 58: 44–47.

Sunstein, Cass R.

2002 Risk and Reason: Safety, Law and the Environment. Cambridge: Cambridge University Press.

Sunstein, Cass R.

2005 Laws of Fear: Beyond the Precautionary Principle. Cambridge: Cambridge University Press.

Thompson, William

2002 One Year Later: The Fiscal Impact of 9/11 on New York City. New York: Comptroller of the City of New York.

U.S. Department of Homeland Security [DHS]

2006 Ready.gov – U.S. Department of Homeland Security. http://www.ready.gov

Whitaker, Reginald

2006 A Faustian bargain? America and the dream of total information awareness. In Kevin Haggerty and Richard V. Ericson (eds.), The New Politics of Surveillance and Visibility. Toronto: University of Toronto Press.