



**HAL**  
open science

## **Risk calculation and precautionary uncertainty: two configurations within crime assessment**

Noel Klima, Nicholas Dorn, Tom Vander Beken

► **To cite this version:**

Noel Klima, Nicholas Dorn, Tom Vander Beken. Risk calculation and precautionary uncertainty: two configurations within crime assessment. *Crime, Law and Social Change*, 2010, 55 (1), pp.15-31. <10.1007/s10611-010-9265-2>. <hal-00651634>

**HAL Id: hal-00651634**

**<https://hal.science/hal-00651634v1>**

Submitted on 14 Dec 2011

**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

## **Risk calculation and precautionary uncertainty: two configurations within crime assessment**

[Revised and re-submitted, May 2010. The authors thank the referees; where differences of view might still occur, these are considered legitimate ones, at least by the authors, likewise the regional reference points.]

### **ABSTRACT**

This paper explores two configurations of thinking about crime amongst law enforcement agencies and private sector security managers: 'risk calculation' (concerned with everyday, calculable probabilities and impacts and their management) and 'precautionary uncertainty' (concerned with events that might be incapacitating, yet are not calculable by probability assessments). The paper explores their respective constituent concepts and fields of application in crime assessment, drawing upon qualitative research-in-progress in Belgium. Risk calculation, as applied to crime, starts with past data on routines that link perpetrators with targets that lack capable guardians. Precautionary uncertainty focuses on potential impacts that are highly disabling and potentially wide-spreading (contagion, knock-on effects), asking how such impacts can be contained and recovered from. Risk and uncertainty are shown to be related to 'rational-instrumental' and 'deliberative-constitutive' approaches as developed by Fisher's work the field of law, which offers a meta-narrative in relation to which they can be positioned. Finally, the paper asks if these two crime assessment methods should be seen as distinct or as merging. On the basis of criteria of conceptual sharpness, openness to public debate and justiciability, the authors champion the maintenance of a clear distinction between risk and uncertainty.

## INTRODUCTION

This paper draws upon international literature on risk and uncertainty and on pilot interviews with security personnel and other managers in the private sector and with law enforcement personnel in Belgium regarding the vulnerability of economic sectors to crime.<sup>1</sup> The aim of the paper is to draw attention to two configurations of thinking in crime assessing amongst security managers economic sectors and law enforcement agencies.

The literature on risk and uncertainty literature spans the disciplines ([2] p. 288), from the natural sciences to social sciences and law,<sup>2</sup> and some of the ideas have entered popular discourse.<sup>3</sup> Following O'Malley ([29] pp. 23-24) - who considers risk and uncertainty 'as distinguishable ways of imagining and governing the future' and analyses them in terms of 'configurations or assemblages' - we observe two such configurations concerning public sector and private sector thinking about crime in economic sectors in Belgium. Each of these has specific strengths, weaknesses and (we argue) purposes. We call these 'risk calculation' and 'precautionary uncertainty' and, in the second part of this paper, we link them to certain developments and thinking in law.<sup>4</sup>

On the one hand, one finds an established, technocratic and expert-based form of risk calculation for purposes of risk management, generating quantitative estimates of the probabilities and impacts of everyday (routine) crime events. Risk calculation specialists seek to make estimates of probabilities, using various conceptual models, known past cases and available historical data. Risk calculations are shared between senior managers in the private sector, policy makers, police and the public - all of whom are advised to support counter-measures, seeking to interpose barriers between perpetrators and their targets/victims, using techniques of guardianship, disruption and/or prosecution. In short, risk calculation specialists produce knowledge having implications for the thinking and conduct of others. For example, public policing agencies, the specialised security industry [47, 49] and security

---

<sup>1</sup> During the second half of 2008 and the first half of 2009, 8 pilot interviews were held: 5 with personnel in the transport sector (including import-export) and 3 in the hotel, restaurant and café business (horeca). We also studied 9 files of the police concerning these sectors and discussed issues with several agents of different police and customs services' sections. The interviews were carried out under the auspices of the federal office for Belgian Science Policy in the program 'Society and Future'.

<sup>2</sup> For the social sciences Zinn [49] made efforts to map the different conceptualisations of risk and uncertainty generated by various positions. A more multidisciplinary research project on risk and uncertainty was launched by the University of Kent (Peter Taylor-Gooby and Jens Zinn) linking conceptual and methodological analysis from psychology, economics and sociology. See <http://www.kent.ac.uk/scarr/index.htm>.

<sup>3</sup> Exemplarily for the enormous amount of contributions the notion "risk" shows circa 3.060.000 hints on [www.GoogleScholar.be](http://www.GoogleScholar.be) and "uncertainty" circa 2.220.000 (accessed on 20 May 2010), ISI Web of Science showed 73.243 articles dealing with the topic "risk" and 62.231 articles dealing with "uncertainty" among all subject areas. (accessed on 20. May 2010).

<sup>4</sup> These notions are chosen deliberately. 'Risk calculation' refers to what law enforcement and private sector interviewees refer to while talking about the described way of assessment. Other scholars employ other notions describing a similar mechanism dedicated to other contexts than crime. See eg. Weir [46] who uses 'clinical risk' in the context of medical diagnosis of pregnancy or Collier [11] who refers to 'archival-statistical' in the context of insurance. The aim is not to find 'the' generalised notion of description of what is happening but rather keep it close to the context under research. 'Precautionary uncertainty' is taken over from O'Malley ([29] p. 23) who label this set-up with regard to the precautionary logic behind it. This logic was observed during the interviews as well.

units inside large firms 'responsibilise' [22] firms, their managers and staff, in the sense of giving them forms of risk knowledge and risk solutions.

Whilst there may be nothing anti-democratic in the process of specialist risk calculation, it is not intrinsically democratic either: citizens should do what policy-makers tell them, and policy-makers are suitably informed by risk specialists. Citizens would be disadvantaged in querying specialists' assessments, since the models and language may be unfamiliar, the data bewildering and/or non-available (for reasons of confidentiality and security), and citizens are positioned as customers for, not co-authors of, such assessments.

By contrast with such technocratic assessments, we argue, one finds (especially since 2001) the rise of an ambiguous and contested politics of precaution concerning crime risks. This concerns not the most likely, rather the worse imaginable events – inspired by the precautionary 'turn' after the attacks of 9/11. Abandoning as futile the attempt to attach probabilities to rare but very high-impact events, this configuration focuses on the potential instability of targets, systems and victims, including those yet to be exploited by criminals (as far as is known). It aims at identifying the vulnerabilities that would lead to the most devastating consequences. It spans business continuity planning in the face of potential disruptions from a variety of sources including (for example) extortion by criminals, major frauds by managers or traders, industrial espionage and infrastructure misuse by business partners. Such disruptions may involve shut-downs, severe reputational damage, even bankruptcy (see eg. WorldCom, Enron etc.). Private sector interviewees of larger companies in Belgium report that such considerations have led to the introduction of back-up and replacement systems capable of supporting firms' normal activities, in the event of major disruptions caused by crime.

This precautionary approach potentially widens the responsibility for knowledge-production, from specialists (whose risk calculation techniques cannot quantify systemic uncertainties), to all those who have to live with consequences, since it is they who must decide how far precautionary measures may be justified. The democratisation implied is, if not a poisoned chalice, at least a bitter drink, as citizens get drawn into debates on what restrictions may be merited on liberty and privacy, what administrative actions may be taken against suspected persons and what changes may be made to legal standards of proof.

Caution is needed when considering the historical emergence of the two perspectives. The present authors wish to make clear that they are *not* saying that the more recently emerging precautionary uncertainty configuration have displaced or replaced risk calculation. It is more a case of both approaches being both widely being operationalised alongside each other, in policing and intelligence agencies, in private sector enterprises, etc., depending on the context. To give some brief examples from our respondents, very serious (and potentially difficult to reverse) consequences may arise from terrorism, or from the corruption of systemically-important markets or institutions, or from penetration of governments by top-level crime groups – meriting a precautionary approach. At the same time, however, there may be a continuing shower of thousands of lower-level offences, which by their number, persistence and uneven focus seriously effect some local communities and businesses – meriting everyday risk calculation and management [42]. Risk calculation is about 'known quantities' (historically-observed event frequencies, quantifiable data on losses, creating a sense of manageability). Precautionary uncertainty is about 'unknown quantities' (new categories of or single events, qualitative analysis and crisis management).

The authors acknowledge that risk calculation and precautionary uncertainty are not the only perspectives that can be used in this discussion against the preliminary results of the held interviews. It is for example possible to argue that exceeding the limits of calculative and instrumental rationality does not necessarily imply a shift into uncertainty deliberations. Some techniques or methods allow to work with uncertainties *within* a risk and rational perspective. Scenario-playing [author ref later to insert] or enactment<sup>5</sup> allow players to create new forms of knowledge and practices that allow rational reflections about uncertainties that can be employed in the private sector (in larger companies and in security consultancies) in order to conceptualise and fine-tune risks and uncertainties. Best [4] argues that risk and uncertainty are not just two sides of a coin, but part of a more mixed, sometimes overlapping or ambiguous continuum. O'Malley [29] denies such a view and considers risk as one specific way to manage uncertainty by calculative techniques.

In short, there are a variety and diversity of ways and techniques for deploying thinking and action in terms of risk and uncertainty. How, then, can they be positioned in relation to each other? There are practical difficulties in running the two perspectives alongside each other concerning crime, since evidently they differ considerably in terms of assumptions, content and outputs.<sup>6</sup> In what circumstances could decisive arguments be marshalled, by a law enforcement agency or a large private company or a security consultancy, in favour of having conducted a risk calculation – or by contrast in favour of an precautionary uncertainty analysis or other techniques? These are questions that security analysts and their customers, including citizens, may be called upon to answer. They are also among the questions raised by contemporary work on (crime) risk and uncertainty [23, 29]. Recent work by Elizabeth Fisher [20] and others on the justiciability of risk assessments – meaning the legal determination of their fitness for specific policy purposes – could be a way of exploring their optimal applications and their limitations.

Fisher constructs two 'ideal types': a rational-instrumental approach assessment of specific and relatively bounded risks (like our risk calculation), and a deliberative-constitutive approach to systemic and less bounded uncertainties and 'tipping points' (like our precautionary uncertainty). Fisher examines justiciability of risk and uncertainty assessments: the extent to which, as a result of judicial review, administrative decisions based on such assessments may upheld or struck down by the courts. What is stake here is the fitness-for-purpose of assessments, as established by legal action: justiciability is the equivalent in legal terms to the managerialist notion of fitness-for-purpose. This approach looks as much at the policy making process as it does at the sources of risk and uncertainty; and also it concerns itself with robustness of process/procedure in the face of possible legal challenges. Given the increasingly litigious environment – including the use of judicial review at national level and the increasing involvement of the European Court of Justice in matters of criminal law [28] – it would seem important as well as interesting for crime risk calculations in EU member states to be legally robust (or, to put it the other way around, it could be dangerous for assessments to be legally vulnerable). Nor can it be ruled out that a civil action could be brought by a legal person considering himself to have been harmed by a shortfall in security assessments (for example, by alleged inattention to certain crime risks or

---

<sup>5</sup> Collier [11] introduces 'enactment based knowledge produced by 'acting out' uncertain future threats in order to understand their impact.' as another configuration of assessment with regard to catastrophe insurance.

<sup>6</sup> Haggerty [23] observed that much crime prevention is precautionary in nature as there are not always probability assessments building the basis of decision but rather uncertainty. Concerning crime assessments the purpose and the way of measurement should be outlined clearly to avoid misleading communications and interpretations of the results towards other stakeholders and the public.

terrorist risks on the part of an enforcement ministry, state agency or private sector risk calculation contractor).

The structure of the paper is therefore as follows. First, the nature of, and some issues in, risk calculation are reviewed. Second, the same is done for the analysis of precautionary uncertainty. Finally, the relationship between both is analysed and linked to the fitness-for-purpose/justiciability discourse. From that a meta-narrative is proposed in relation to which risk calculation and precautionary uncertainty can be discussed. Throughout, we seek to bring in examples from pilot interviews with security personnel and other players in the private sectors in Belgium carried out in late 2008 and early 2009 and other examples from the literature.

## **RISK CALCULATION: ASSESSING ROUTINE RISKS AS A TECHNOCRATIC PRODUCTION**

Practitioner and academic discourses on crime risks may be located within the broader context of new (reflexive, late, post-) modern 'risk society', in which risks such as criminality and the mastery of these risks have taken a major role [3, 22, 29]. According to Zinn ([49] p. 4) there are at least three different, although connected ways for the use of the term 'risk': (i) a *defensive* state of mind in which risk may refer to unwanted events, the word being used, with some interchangeability, alongside terms such as hazard, loss, damage or threat (although there may be significant distinctions between such categories, or between specialists' preference for use of some terms and dislike of others); (ii) a *calculative* frame of mind in which risk may indicate a concern with both costs and benefits and the balance between them, and (iii) a *positive* frame of mind in which the idea of risk appetite is represented, which refers to a willingness to take extreme risks in order to maximise returns (some criminals have greater risk appetite than others, and police also may differ in this respect (see e.g. [14])). From a crime-control perspective, type (i) risks, forms of risk that are to be avoided, in particular the risk of criminal victimisation, are of special interest. The demand for control and management of these risks caused the spread of risk analyses [45].

According to this way of thinking, risk is defined as a function of the probability of various risk events and the costs of their impacts. Strategic risk calculations of crime attempt to project this configuration into the future, through relying on past available data such as criminal statistics. In the private sector, security departments build the expertise on which higher company management rely on for decision making. Their knowledge is *inter alia* based on crime incident statistics. Police strategic risk analysis and assessments are regularly focussed on the risk of offending, rather than on the risk of victimisation, whereas it is the opposite for the private sector.

### **Risk calculation and situational crime prevention**

O'Malley & Hutchinson ([30] pp. 374-375), identify a threefold trend in crime prevention and control since the mid-1990s: "[...] first toward statistical and actuarial preventative technologies; second, toward the networked extension of the government of crime beyond police and the state [...]; third, toward to a focus on 'designing out' crime and on situational opportunity reduction rather than previous preventative models focussed on deterrence, correction and the social and psychological causes of crime". Several of our interviewees, mainly from the transport business, confirmed the influence of such measures. Methods

include incident statistics, interrogated by techniques such as crime scripting. Incidents are first 'mapped' in order to highlight hotspots of probable criminal victimisation, making possible a focussing of resources (this is called 'situational prevention'). Crime scripting goes further than this, by identifying the necessary steps of the perpetrators' *modus operandi*, for example with respect to vehicle or cargo theft. All identified risk-points are then confronted with a prevention measure, such as locks, alarms or GPS systems for trucks, trailers and/or the transported goods themselves (tracing devices). This is done within specific companies but may then be shared with other businesses, through organisations such as TAPA (Transported Asset Protection Association) [41] and its Incident Information Service (IIS) and with law enforcement agencies. Based on the measured probabilities for victimisation, new counter measures or prevention measures are applied, in an attempt to forestall future incidents. Concerning cargo theft, the Cargo Theft Report of Europol [17] demonstrates how risk calculation is handled in practice. The IIS of TAPA is promoted as a potential tool in combating cargo theft ([17] p. 22). Geographical Information System (GIS) is another instrument for identifying and mapping crime hotspots that law enforcement and environmental criminologists are using, contributing to crime pattern theory [5, 33, 34].

One well known model is routine activity theory [10]. In their original formulation, Cohen & Felson [10] explained crime as the product of the convergence of three minimal elements in time and space: (i) motivated offenders, (ii) suitable targets, and (ii) the absence of capable guardians. The capable guardian "serves by simple presence to prevent crime" ([19] p. 53). Situational crime prevention [8] focuses on concrete steps that can be taken to reduce crime opportunities.<sup>7</sup> Attempts have been made to expand this approach to organised crime [6]. For our interviewees in the Belgian transport and hotel, restaurant, café business, it seems beyond debate that surveillance (guardianship) by situational prevention measures, like cameras, alarm systems or guards, are useful, indeed indispensable tools for decreasing the probability of crime (at least for certain crime types). Law enforcement respondents also consider these measures as useful in prevention and also for investigation and detection of perpetrators. To give a mundane example, one security manager from a multinational transport company reported that a high incidence of casual thieves cutting the covering of lorry trailers with a knife to steal the load, leading the company to change to a hard protective cover, in order to avoid this *modus operandi* in the future.

The point for our analysis is this is a frequency-based analysis. Likewise, concerning targets, 'crime proofing' of products is seen by some as a way of decreasing the probability of theft. The acronym CRAVED - Concealable, Removable, Available, Valuable, Enjoyable, Disposable - was developed to forecast the probability of theft, based on those six risk factors [7] and to offer prevention measures [15]. Since the means of crime (transport) can also be a target of crime (trucks), anti-theft locks to prevent theft of the whole trucks are now routine, as observed by one of our interviewees at a transport company. Furthermore, small and highly valuable goods are accorded special measures, such as documentation, seal procedures, tracking [37] and bar codes) and also may be camouflaged: small, highly valuable goods may be transported inside big and unwieldy boxes, without external identification of the goods. Since some customers ask for these 'extra' measures, although not all companies are willing to supply them, since they are not organisationally and/or financially capable. Another development of crime proofing is 'legislative crime proofing', which aims to detect crime opportunities inadvertently created by legislation.<sup>8</sup>

---

<sup>7</sup> Clarke & Eck [9] identified 25 techniques of crime opportunity reducing measures.

<sup>8</sup> Research on legislation proving on European Union level is inter alia carried out by Vander Beken & Balcaen [44], Dorn & Levi [13]. See also: [1].

These examples show that probability-based risk calculation is widespread in the private sector and in law enforcement, forming the basis for crime assessment and prevention.

### Criticisms and limitations

Criticisms of such risk calculation and management can be classified as technical or as social. Technical criticisms involve propositions that models are poorly designed or have not been implemented well [43]. The risks dealt with are always 'known' risks. Data is derived from the past and is extrapolated to the future. Decision makers rely on these models and for some it might be helpful – especially when the law of large numbers applies<sup>9</sup> – but for others not. Crime events that have never occurred before in a company or in an economic sector can cause more harm, as one is completely unprepared. This challenges risk calculation based on probability and focuses attention on 'improbable' events that could cause unknown consequences. Donald Rumsfeld, US Secretary for Defence from 2001 to 2006, famously (notoriously for some) distinguished between "known unknowns" (risks that are known to exist but whose timing or magnitude is not predictable) and "unknown unknowns" (risks that are not imagined until the moment they impact) [26]. If only statistical probabilities are used for risk analysis, statistically improbable events, the so-called Black Swans [40], stay out of the radar and are not prepared for. Decision makers (whether individuals or organizations) seem to have several blind spots when confronted with dangers in their environments.<sup>10</sup>

On the other hand, this blindness may have some advantages, since all actions have unanticipated consequences. Decisions based just on risk calculation that is based on past probabilities can open other crime risks, making an enterprise more vulnerable than before taking the prevention measure. Furthermore, if crime risks are represented by a few indicators, then in relation to more complex crime risks - where the time and space of the criminal act is not fixed, as routine activity theory demands – then it is difficult to find prevention measures. Where does the crime risk occur? Do statistics of past cases covered by the police have any value with regard to situational prevention measures regarding the future? Counting numbers of cases of cargo theft on Belgian highway parking places, and reacting by installing camera surveillance on the 'hot parking spaces' close to the Dutch boarder, reduced theft rates there (not taking into account a possible displacement of the perpetrators). Because the availability of highway parking spaces is limited, they can be observed (at some cost), making risk calculation there possible. However, is not the case in many other crime contexts, undermining risk assessments (for example, threat assessments on the basis of criminal statistics, where national crime rates do not say much about crime risks, particularly in particular localities [23]. These are just some of the technical criticisms of risk calculation

Some authors advance social criticisms of this form of assessment. Displacement of crime [36], from protected to unprotected areas, would mean that those not able to follow the prevention advice would be easy targets for the criminal. This would hit the financially weaker companies or persons in society [29]. Our own preliminary research is consistent with this. Consider for example the decision mentioned above, to change the usually used

---

<sup>9</sup> "[E]ven if individual events happen in a random way, when enough of these events are put together in a reasonably stable environment one can make predictions that have a reasonable chance of being accurate. So, for example, one cannot predict whether an individual coin toss will turn up heads or tails, but many coin tosses will follow a fixed probability ratio (an even chance)" [26].

<sup>10</sup> For a critique of the efforts of local governments, see for instance Wolensky & Wolensky [48].

trailers' cover to a hard protective cover to avoid cargo theft by cutting the cover with a knife: another respondent from a smaller company reported that many middle sized or smaller companies do not have the financial capacity to update their lorries with these sort of measures. On the wider social canvass, Power argued that a society preoccupied with "the management of everything" [32] is a dysfunctional society. Consider also the Foucauldian proposition that risk mentality is deployed as a strategy of governance, meaning that citizens follow leaders who point to possible risks and promise firm action against them [22]. Precaution invites one to anticipate what one does not yet know, to take into account doubtful hypotheses and simple suspicions" ([18], see also Haggerty op cit).

Thus, whilst probability-based crime risk calculation may seem like 'common sense' to its practitioners, it is open to technical and social criticisms.

### **DELIBERATING EXCEPTIONAL UNCERTAINTIES**

The starting point of this mentality is that attempts to quantify probability may be inherently misleading or not possible – hence precautionary approaches. These have arisen in many fields, including environmental protection (from the 1990s), terrorism (especially from 2001) and financial market security (from 2008). In this configuration, quantification of probability of crime risks is replaced by the avoidance or minimisation of harms, not relying on expertise because it is in doubt or not available but deploying "informal knowledge and techniques [in order] to achieve security"([29] p. 23).

This approach prioritises the highest-impact events, however they may be caused: for example what could follow if an aeroplane falls onto a chemical works, or if hundreds of thousands of mortgages are mis-sold, or if criminality taints or derails a nationally important procurement contract? The two main elements are (i) a willingness to expend considerable resources in order to try to prevent (insofar as is possible) the occurrence of events that would have the greatest impacts and, (ii) an acceptance that, despite all such efforts, some such events may occur, hence it is important to have sufficient resilience (back-up systems, redundancy, self-healing systems, ability to rapidly replace damaged capacity, etc.) in order to enable recovery. Alongside disaster recovery plans and business contingency plans, an important precautionary tool is redundancy (duplication of systems), especially in the logistic business. Interviewees from major transport companies reported that, instead of creating only a few big hubs through which to transport good, or depots in which to store them, it is considered safer to make several smaller hubs in different geographic locations. In case of an incident, the tasks of one unusable hub can be taken over by others.

Criticisms of precautionary uncertainty and similar approaches are diverse, including that they go beyond available data and become ideological [39]; that they have become discredited as a result of a realisation that high-handed action may be entered into as a precaution against threats that are subsequently found not to exist [39]; that they justify a never-ending stream of emergency actions and controls that become permanent. Nevertheless, there remains strong interest in precautionary uncertainty, for reasons of recent history.

### **From calculable crime risk to precaution: a short history**

Concerning crime we can say that, prior to 2001, strategic criminal assessment focussed on what we may call 'common criminals', meaning that they were conceptualised as acting for financial gain, and in some cases power, whether that be at a local level, regionally or across global markets. Following 2001, strategic analyses of crime became influenced by anti-terrorism policies, in some instances leading to so-called 'organised crime' being elevated from being a serious crime category, to being considered by some commentators to form, if not a bridge between criminality and terrorism, at least a facilitating factor. Anti-terrorist policies thus reinforced the tendency to pose some 'organised crime' phenomena as having potentially systemic consequences (penetration of the licit economy and/or of political elites, collapse of the state's monopoly of violence, breakdown of social order, etc. (see e.g. [38]).

In parallel, and arising from the 1990s onwards and from neo-liberal tendencies in the market economy and political life, risk calculation took a far broader form: it became a standard management tool [29]. Initially, managerial risk calculation took the same broad strategy as in the security field, as it sought to identify specific risks and to calculate their probabilities and impacts, then trying to build up from these specific estimations to a notion of overall risk [16]. However, the 'bottom up', aggregating style of calculation of crime risk has been brought into question by the New York attacks of 2001, also by the financial crisis of 2007 onwards, which is seen as being conjoined with various criminal phenomena, such as Ponzi frauds, insider trading and conflicts of interest [author ref later to insert]. Increasingly, systemic vulnerabilities are seen as requiring a more holistic approach, looking not at individual risks but at connections between them [31, 35].

Identification of uncertainties that might have far-reaching effects cannot be accomplished by specialists alone, since they don't have a wide enough view (per definition, they are specialists). Such issues require inputs from the widest possible set of perspectives [3]. As interdisciplinary work published by the New York Federal Reserve puts it: "To identify systemic risks, one has to look at everything. Since no one can really capture all of the relevant perspectives, systemic risks must be assessed through consultations with multiple players, which ultimately converge on a picture of the most important risks" ([24] p. 36).

Thus, anti-terrorist and financial market developments and policies introduced, alongside the assessment of discrete risks, an enhanced awareness of the uncertainties attaching to systemic turning points, and a certain humility amongst security assessment specialists. This has led to an enrichment of the interdisciplinary debate, as scholars from different disciplines – natural science, environmental studies, disaster-management, business, markets – are brought together to explore what if any general statements might be arrived at, concerning uncertainty. According to some recent analyses from studies of resilience in natural and man-made environments and in financial markets, attempts to lowering specific risks by linking together support mechanisms might have the effect of increasing systemic risks, whilst attempts to lowering systemic risks by reducing interlinkages might deepen the risks to specific elements. For example: "When a system is too homogeneous, it cannot adapt. Modularity – the degree to which a system can be decoupled into discrete components – also influences robustness. A basic principle in the management of forest fires and epidemics is that if systems are all connected, a perturbation will encounter nothing to stop it from spreading. But when a system is compartmentalized (when firebreaks exist or high-risk parts of a population are vaccinated against an epidemic), then the spread may be contained. Modularity can thus be an important part of robustness if it ensures that an affected component will be isolated from destabilizing feedbacks. However, modularity often involves a trade-off between local and systemic risk [uncertainty]. Because the

compartmentalized elements of a system will be less able to withstand some shocks, modularity tends to increase the risk that individual elements will be critically damaged” ([24] p. 28). The possibility that ‘best practice’ in security policies – based on too close an attachment to probability sampling – might be envisaged as a form of ‘herding’ and a deepening of shared vulnerabilities may be a bitter pill to swallow for those advocating and enforcing greater cooperation and convergence in security planning [author ref later to insert]. This leads to the question, to be addressed at the end of this paper, what basis could be adopted for judging (literally) the reasonableness of reliance upon risk calculation and on systemic uncertainty?

### **Reducing impacts in conditions of uncertainty: difficulties and criticisms**

The key characteristic here is a willingness to ‘think the unthinkable’, in the sense of identifying what could be the worse things that might happen, in terms of their impacts, whilst disregarding any preconceptions about their likelihood. This Cassandra-like style of assessment is not, therefore, about events that seem likely to happen – rather, it is about events that would have the greatest negative consequences. One security manager gave us the following example: “We are sitting with a bunch of people around the table ... to think about the totally unexpected ... for example, within our company we follow of policy of screening our employees, under the slogan: all old criminals out of our house! And now we start thinking we had to employ only criminals, what would be the consequence?”<sup>11</sup>

Such a ‘blue sky (could turn black)’ thinking is not easy to maintain in an operational setting, since it does not easily fit with the ‘action’ frame or frame of thinking about existing, known risks and the need to manage them. Furthermore, a precautionary uncertainty approach, focusing on events that would have the biggest impacts (should they ever occur) would seem to draw attention away from events that may entail much lesser impacts – even quite trivial impacts – yet which are actually known to be occurring every day. Therefore one potential criticism of such an approach would be that it is socially irresponsible and economically wasteful, since it can result in insufficient attention being paid to known risks and their accompanying hurts which, in aggregate, are no doubt considerable. For example the international literature suggests that locally-focussed crime against businesses and, in some districts, households, may be both ‘organised’ (meeting national and/or EU criteria for ‘organised crime’) and considerably burdensome for those affected [42]. If these known and constantly ongoing hurts were to be neglected in favour of allocating police resources to possible yet shadowy or non-existent ‘Mr Bigs’, then questions may arise about priorities and use of resources.<sup>12</sup>

Another potential criticism of precautionary uncertainty – which emerges both from anti-terrorist policies and, more recently, from financial market precautionary policies post-2008 – is that the precautionary interventions taken to forestall possible future, uncertain but big-impact events may carry with them their own risks [39]. This is now a familiar theme in relation to the interventions into Afghanistan and Iraq, which definitely triggered unexpected difficulties and which may on balance, have magnified political dissatisfactions and hence threats. However, such large interventions are difficult to evaluate, because of

---

<sup>11</sup> Translated from Dutch to English by the authors.

<sup>12</sup> If on the other hand all analytic attention and operational resources are targeted upon the best-known and more easily manageable risks, then uncertain but potentially gravely harmful possibilities may be neglected: it seems therefore that some way of balancing known risk and unknowable uncertainties may be needed.

the lack of a 'control group' – what would have happened if the intervention had not been made? That aside, large interventions made in order to forestall possible disasters may be very costly in economic terms, even to the point of being unaffordable, an evaluation that some commentators have made not only in relation to anti-terrorist policies but also to current approaches to the financial market crisis [12]. There may be similar, but unknown, risks in relation to some of the precautionary tactics that enforcement agencies adopt. For example, *disruption* is sometimes directed towards objectives such as weakening crime groups that are difficult to bring to court - for example undercover agents may try to sow mistrust between criminal groups/networks, thus discouraging them from cooperating together – yet it can be difficult to know all the consequences, side-effects and unintended consequences, when acting against targets that are only partially in sight.

A provisional conclusion might be, either that precautionary action should be conducted only in exceptional situations (criteria for which need to be clearly delineated); or that the precautionary approach should extend its logic from identification of possible but uncertain threats, to encompass also all the possible (but uncertain) consequences of taking actions against those threats. If any of the imaginable consequences appear to be unacceptable, then that would be reason for reconsideration of the proposed action. To be credible, such checks and balances would need to be intrinsic aspects of the model, not afterthoughts.

In this way, an precautionary uncertainty configuration might come more closely to approach the more conventional risk calculation approach, insofar as risk management involves analysis not only of the problems but also a cost-benefit analysis of alternative interventions. None of this undercuts the case for analysis in conditions of uncertainty, rather it makes it more complex. And it begins to raise the question of which approach, risk or uncertainty (or some mix of the two) may be suitable in particular circumstances.

## **JUSTICIABILITY: ADJUDICATING FITNESS FOR PURPOSE**

Here we examine some issues of concern to security policy-makers and managers, whether in the public sector or the private sector, who are in a position of deciding in what circumstances to apply probability-based risk assessments, and/or precautionary uncertainty assessments. When is each of these most appropriate or, more worryingly, when is one or the other inappropriate? On what basis, could it be decided in principle to rely on one or the other; or possibly to employ both but in respect of different issues?

We give two answers, one 'commonsensical' and pragmatic (and consistent with our interviews with security managers and others in Belgium), the other based in law.

From the commonsensical and pragmatic point of view, the following views have been expressed to us. If the concern is something like low-level pilfering of goods by staff or customers, that could be calculated by routine risk calculations. By contrast, centralised IT communication and control systems seem to call out for a 'worst case scenario' approach, involving wide-ranging 'what if?' discussions. However, there may also be circumstances which, at the start, it is difficult to define issues exclusively in terms of *either* routine risks *or* exceptional vulnerability: the two forms of thinking will co-exist as techniques of 'knowing'. Inputs from lawyers at the risk/uncertainty intersection come from the perspective of the justiciability of policy assessments, meaning the legal determination of their fitness for specific policy purposes. This claims to be an authoritative way of exploring the optimal

applications of, and limitations to, the risk calculation and precautionary uncertainty configurations. It is from this perspective that we now consider the two ‘ideal types’ of forms of procedure in the assessment of risk/uncertainty as proposed by Elizabeth Fisher [20, 21]: the rational-instrumental (our risk calculation) and the deliberative-constitutive (our precautionary uncertainty).

The present authors point to parallels between, on the one hand, a degree of correspondence between probability-based crime risk calculation and Fisher’s rational-instrumental category. On the other hand, there is also some correspondence, we suggest, between precautionary assessments of uncertainty, and her deliberative-constitutive category. These links are indicated in Figure 1 below.

Figure 1. Two configurations, drawing upon, social sciences, security studies and law

<i>Ideal types</i>	PROBABILITY RISK CALCULATION	PRECAUTIONARY UNCERTAINTY
<i>Main contents of model</i>	‘RISK’, where probabilities are knowable, possibly quantifiable	‘UNCERTAINTY’, where ‘tipping points’ are unknowable
<i>Types of problems addressed</i>	ASSESSABLE, routine, known, predictable problems	CATASTROPHIC potential events
<i>Conceptual starting point</i>	PROBABILITY, calculated from past frequencies, of the co-presence of perpetrators, targets and insufficient guardianship	POTENTIAL INSTABILITY of targets or systems, meaning that, if hit, they might fall
<i>Who describes the problems</i>	EXPERTS, specialists, technocrats	ALL STAKEHOLDERS: policy-makers, citizens, experts
<i>What is the deliverable</i>	Intelligence ‘PRODUCT’, which aims to be correct (the model represents reality)	Emphasis on ‘PROCESS’, which must be widely ‘owned’ (the model is a tool for thinking)
<i>What society is thereby reproduced</i>	One in which technocratic experts lead, policy makers and civil society follow	One in which civil society and the private sector face difficult decisions about precaution
<i>Corresponding to Fisher’s legal categories</i>	Rational-instrumental	Deliberative-constitutive

Fisher suggests that her ‘rational-instrumental’ approach (our risk calculation: objectivist, ‘scientific’ and technocratic) will continue to co-exist with her ‘deliberative-constitutive’ approach (our precautionary uncertainty), rather than merging. She opines that: “the most legitimate state of affairs is the simultaneous operation of both paradigms. This is what is occurring in many contexts and, while, resulting in risk evaluation being a rather messy practice, it guarantees the most acceptable balance between enabling and restraining public administration” [20]. Refining this view, we argue that depending on the context they might sit alongside each other whilst remaining distinct modes of thought, merge or be complemented by other paradigms.

Fisher’s rational-instrumental approach relies upon (and assumes the possibility of) a sound scientific basis for risk calculation. Risks are taken as knowable in principle, and information

about them being assessable, reasonably robust and free of too much latitude in terms of alternative interpretations. The models are taken to represent social and natural realities and, when populated with data, cause and effect relations can be clearly and confidently identified.

By contrast, Fisher's deliberative-constitutive approach maintains that scientific methods can neither grasp nor decide the phenomena in question, because these are complex, uncertain and socially-politically ambiguous. This does not mean that technical modelling of the issues cannot be done, it means that models and data are inadequate as a substitute for judgement, especially since some of the apparent findings of modelling ('outputs') may be strongly influenced by model assumptions ('inputs'). At best, models act as a contribution to reasoning, the latter having a primarily normative basis [20, 21].

This objectivist/subjectivist, science/norms, technocratic/democratic split is deeply rooted in western cultures and in their social sciences, including in criminology and security studies. However, consensus does not exist on where and how to draw the line between these tendencies.

Some commentators would argue for the exclusion of models of systemic uncertainty, on the grounds that the models and data are insufficient to support robust findings [25]. On those grounds, one might (at least in principle) arrive at quite a neat conclusion, in which further public and private investment should be made in the continuing development of risk calculations, whilst uncertainty modelling should be abandoned.

By contrast, from the more overtly normative position implied in Fisher's deliberative/constitutive approach, the supposed precision of technical risk calculations should be viewed with some scepticism. Indeed the acknowledged lack of a firm science base for discussions of systemic and precautionary matters could be all the more reason to advance those discussions in an exploratory and open manner in the public policy arena. In short, 'scientific' risk calculation assessments and 'political' precautionary uncertainty approaches are matters of contention.

The answer, according to Fisher, to be found through the legal system. Legal challenges have been mounted to a variety of policy decisions, on the basis that they relied on unsound science, or took on a precautionary basis that was unmerited. Thus, courts (especially but by no means exclusively in the US) and various commissions of enquiry have been drawn into a critical exploration of the fitness for purpose of such approaches, in principle and in terms of their execution in practice. As a sympathetic Belgian commentator puts it, the aim of Fisher's work is "recasting the terms of the debate [on risk and uncertainty] and, more specifically, rehabilitating the role of law and centrality of public administration" [27]. Indeed, this work clearly signals its objective as overcoming a perceived *sidelining* of legal analysis in relation to risk and uncertainty, which has been dominated by concepts from economics, psychology and policing. Fisher asserts that "the legal dimension is a significant one and the body of law in this area is a complex, dynamic and constantly shaping understandings" [20]. We agree, and we argue for greater attention in risk/uncertainties to the legal dimension.

## **DISCUSSION: RISK/UNCERTAINTY DICHOTOMY OR CONTINUUM?**

The social science, security studies and legal literatures suggest that security issues may be constructed or modelled either in terms of repetitive relations between elements (known, cause and effect relations) or in terms of unpredictability of relations. This difference may be represented in terms of the two configurations, as we have in this paper, or as a continuum, as some others have suggested: “At one end of this continuum are systems in which all the variables are predictable (A always follows B). Then there are systems that have low uncertainty (A almost always follows B) and medium uncertainty (we can calculate the probability that A will follow B). At the far end of this continuum are high uncertainty or stochastic systems (in which we cannot even predict a probability that A will follow B). In systems where uncertainty is relatively low it is easier to plan for any possible dangers, while in highly uncertain systems security becomes more problematic” ([26] p. 9).

So, categories or a continuum? There can be no settlement of this question except by appeal to criteria, which might be theoretical, practical or (more frankly) political. The concepts and techniques chosen for representing security (and other) issues depend also on cultural background, language, history (see [49]) and, for some academics, on past intellectual investments or commitments. Risk calculation and precautionary uncertainty are therefore likely to remaining matters of healthy debate concerning crime assessments, as is the question of whether they are best seen as being categorically distinct approaches, as a continuum or even as a homogenous blur.

Our reasons for preferring a categorical approach rest upon the following criteria and value judgements: conceptual sharpness; openness to public debate; and justiciability. Valuing conceptual sharpness, in our view, favours the categorist road: Occam’s Razor might be thought to favour a blurring or a continuum, however much then is lost in terms of differences in risk/uncertainty narratives, methodologies and fitness-for-purpose. A criterion of openness to public debate strongly favours distinct perspectives on crime risk probability and on precautionary uncertainty: their analytical styles have very different policy implications, which should not be inadvertently ‘bought’ as the technical output of a methodology, but should be appreciated at the onset of the analysis (what kind of policy are actors trying to construct, when they model security problems?). Lastly, justiciability is an important issue in all societies of law: courts provide another valuable forum for challenge and debate, and so the contributions to legal theory provided by Fisher (above) must be valued and linked to other aspects of scholarship.

## **CONCLUSION**

Risk calculation and precautionary uncertainty are two configurations that characterise the *Zeitgeist* in public and private sector thinking about crime and insecurity. Placing the social sciences and legal scholarship alongside each, risk calculation is seen to correspond to Elizabeth Fishers’ legally-based ‘rational-instrumental’ approach, whilst precautionary uncertainty corresponds to her ‘deliberative-constitutive’ approach. The justiciability of risk and uncertainty assessments provides a framework for exploring the optimal applications and limitations of both configurations. This legal determination of their fitness for specific policy purposes provides a way to disentangle the discussion of risk calculation and precautionary uncertainty. We have argued here that the two forms of knowledge differ considerably in terms of assumptions – Gaussian continuities versus sudden breaks), types of content (quantitative versus qualitative), policy uses and participation (technocratic expertise versus wider stakeholder deliberation – and so should be regarded as distinct

configurations, not as a continuum. However, whether or not in practice risk calculation and precautionary uncertainty eventually merge, in crime assessments and in other fields of application, or remain distinct, remains an area for empirical research in the coming years.

## References

1. Albrecht, H.-J., & Kilchling, M. (2002). Crime Risk Assessment, Legislation, and the Prevention of Serious Crime - Comparative Perspectives. *European Journal of Crime, Criminal Law and Criminal Justice*, 10, 22-38.
2. Bammer, G., & Smithson, M. (Eds.). (2008). *Uncertainty and risk: Multidisciplinary perspectives* London, UK: Earthscan.
3. Beck, U. (1992). *The risk society: Towards a new modernity*. London: Sage.
4. Best, J. (2008). Ambiguity, uncertainty, and risk: rethinking indeterminacy. *International Political Sociology*, 2, 355-374.
5. Brantingham, P. J., & Brantingham, P. L. (Eds.). (1981). *Environmental Criminology*. Beverly Hills: Sage Publications.
6. Bullock, K., Clarke, R. V., & Tilley, N. (Eds.). (2010). *Situational Prevention of Organised Crimes*. Devon, England: Willan Publishing.
7. Clarke, R. V. (1999) Hot products: Understanding, anticipating and reducing demand for stolen goods. *Police Research Series Paper 112*. London.
8. Clarke, R. V. (Ed.). (1997). *Situational Crime Prevention: successful case studies* (2 ed.). New York: Harrow and Heston.
9. Clarke, R. V., & Eck, J. E. (2005). *Crime analysis for problem solvers: In 60 small steps*. from <http://www.cops.usdoj.gov/files/RIC/Publications/CrimeAnalysis60Steps.pdf>.
10. Cohen, L. E., & Felson, M. (1979). Social Change and Crime Rate Trends: A Routine Activity Approach. *American Sociological Review*, 44, 588-608.
11. Collier, S. J. (2008). Enacting Catastrophe: Preparedness, Insurance, Budgetary Rationalization. *Economy and Society*, 37(2), 224-250.
12. Dizard, J. (2009, April 12, 2009). Who can afford the next national recovery plan? *Financial Times* from [http://www.ft.com/cms/s/0/f715e3b0-25ef-11de-be57-00144feabdc0.html?nclick\\_check=1](http://www.ft.com/cms/s/0/f715e3b0-25ef-11de-be57-00144feabdc0.html?nclick_check=1)
13. Dorn, N., & Levi, M. (2006). From Delphi to Brussels, The Policy Context: Crime Prophecy, Proofing, Assessment. *European Journal on Criminal Policy and Research*, 12, 213-220.
14. Dorn, N., Oette, L., & White, S. (1998). Drugs importation and the bifurcation of risk. Capitalization, cut outs and organized crime. *British Journal of Criminology*, 38(4), 537-560.
15. Ekblom, P. (2008). Designing products against crime. In R. Wortley, Mazerolle, L. (Ed.), *Environmental Criminology and Crime Analysis*. Cornwall: Willan Publishing.
16. Europol (2006). *EU Organised Crime Threat Assessment*. The Hague: Europol.
17. Europol (2009). *Cargo Theft Report*. The Hague: Europol.
18. Ewald, F. (2002). The Return of Descartes' Malicious Demon: An Outline of a Philosophy of Precaution. In T. Baker & J. Simon (Eds.), *Embracing Risk: The Changing Culture of Insurance and Responsibility*. Chicago: University of Chicago Press.
19. Felson, M. (1995). Those Who Discourage Crime. In J. E. Eck, Weisburd, D. (Ed.), *Crime and Place: Crime Prevention Studies* (Vol. 4). Monsey, NY: Criminal Justice Press.
20. Fisher, E. (2007). *Risk regulation and administrative constitutionalism*. Oxford: Hart.

21. Fisher, E. (2008). *Models, regulation and legal cultures: A transatlantic perspective*. Paper presented at the A new look at the interaction of scientific models and policy making, James Martin 21st century school, University of Oxford.
22. Garland, D. (2001). *The culture of control: crime and social order in contemporary society*. Oxford: Oxford University Press.
23. Haggerty, K. (2003). From Risk to Precaution: The Rationalities of Personal Crime Prevention. In R. V. Ericson & A. Doyle (Eds.), *Risk and Morality*. Toronto: University of Toronto Press.
24. Kambhu, J., Weidman, S., & Krishnan, N. (2007). Part3: Systemic risk in ecology and engineering. *Economic Policy Review*, 13(2).
25. Kopp, P., & Besson, F. (2009). A methodology to measure the impact of organised crime activities at the EU level, Examining the feasibility of the methodology: a pilot study on international fraud. In E. S. e. al (Ed.), *Organised Crime in the EU: A Methodology for Risk Assessment, a study financed by the European Commission - DG Research under the Sixth Framework*. Rotterdam: Erasmus University Rotterdam.
26. Longstaff, P. H. (2005). *Security, resilience and communication in unpredictable environments such as terrorism, natural disasters and complex technology*. Cambridge MA: Harvard University.
27. Meuwese, A. (2008). Book review: Risk Regulation and Administrative Constitutionalism by Elisabeth Fisher. *Journal of Law and Society*, 35(3), 417-421.
28. Mitsilegas, V. (2009). *EU Criminal Law*. Oxford: Hart.
29. O'Malley, P. (2004). *Risk, Uncertainty and Government*. New York: Glasshouse Press.
30. O'Malley, P., & Hutchinson, S. (2007). Reinventing Prevention. Why did 'crime prevention' develop so late? *British Journal of Criminology*, 47(3), 373-389.
31. OECD (2003). *Emerging Systemic Risks in the 21st Century: An Agenda for Action*. Paris, France: OECD.
32. Power, M. (2004). *The risk management of everything: rethinking the politics of uncertainty*. London: Demos.
33. Ratcliffe, J. H. (2004a). Crime mapping and the training needs of law enforcement. *European Journal on Criminal Policy and Research*, 10, 65-83.
34. Ratcliffe, J. H. (2004b). The hotspot Matrix: A framework for the spatio-temporal targeting of crime reduction. *Police Practice and Research*, 5(1), 05-23.
35. Renn, O., & Klinke, A. (2004). Systemic risks: a new challenge for risk management. *EMBO reports*, 5(special issue), 41-46.
36. Repetto, T. A. (1976). Crime prevention and the displacement phenomenon. *Crime and Delinquency*, 22, 166-177.
37. RFID Journal. from <<http://www.rfidjournal.com>>
38. Shelley, L., Scott, E., & Latta, A. (Eds.). (2007). *Organised Crime and Corruption in Georgia*. London and New York: Routledge.
39. Sunstein, C. R. (2003). Beyond the precautionary principle. *University of Pennsylvania Law Review*, 151(3), 1003-1058.
40. Taleb, N. N. (2007). *The Black Swan: The Impact of the highly Improbable*. New York: Random House.
41. TAPA. Transported Asset Protection Association, from <<http://www.tapaemea.com>>
42. Tilley, N., & Hopkins, M. (2008). Organized crime and local businesses. *Criminology & Criminal Justice*, 8(4), 443-459.
43. Van Duyne, P., & Vander Beken, T. (2009). The indications of the EU organised crime policy making. *Crime, Law and Social Change*, 51(2), 261-281.
44. Vander Beken, T., & Balcaen, A. (2006). Crime Opportunities Provided by Legislation in Market Sectors: Mobile Phones, Waste Disposal, Banking, Pharmaceuticals. *European Journal on Criminal Policy and Research*, 12(299-323).

45. Walklate, S. (1997). Risk and criminal victimization. A modernist dilemma? *British Journal of Criminology*, 37, 35-45.
46. Weir, L. (1996). Recent developments in the government of pregnancy. *Economy & Society*, 25(3), 372-392.
47. Williams, J. W. (2005). Reflections on the private versus public policing of economic crime. *British Journal of Criminology*, 45(3), 316-339.
48. Wolensky, R. P., & Wolensky, K. C. (1990). Local governments problem with disaster management: a literature review and structural analysis. *Policy Studies Review*, 9(4), 703-725.
49. Zinn, J. O. (2008). *Social theories of risk and uncertainty: an introduction*. Malden MA: Blackwell.