EUROPEAN STRATEGIC INTELLIGENCE: HOW FAR INTEGRATION?

Nicholas Dorn[*]

Abstract

In the light of international and European pressures for greater cooperation in exchange of information, this paper attempts to assess the prospects for strong integration of the underlying information methodologies and systems and discusses the potential consequences of such system integration for risk assessment and security governance. The author draws on work by financial market analysts as well as on the criminological literature, arguing that there is a danger that the systemic integration of separate public and private intelligence functions would narrow perspectives to the point that minor risks could be over-emphasised and major vulnerabilities overlooked. He concludes that, with regard to the architecture of strategic intelligence best capable of informing and supporting policy, a multiplicity of loosely linked information sources and methodologies, connected though an 'arms length' cooperation structure, remains best for the European Union. Ironically, the capability to construct high-quality strategic intelligence may be safeguarded by the apparently 'bad' old habits of each agency constructing an information system fit for its own specific purpose. Fortunately, those 'bad' habits may be underpinned by certain structural conditions, briefly explored here through the literature on security governance.

[*] Nicholas Dorn is Professor of International Safety and Governance at the School of Law, Erasmus University Rotterdam.

1 Introduction

Common threat assessments are the best basis for common actions. This requires improved sharing of intelligence among Member States and with partners.[1]

Despite the existence of motivating factors for increased cooperation, obstacles… probably will prevent the creation of a supra-national European intelligence authority.[2]

When lawyers and criminologists encounter the world of strategic intelligence, they encounter a huge information-processing and risk-management machine that is, by definition, outside the criminal justice system, the courts, and the checks and balances involved in preparing cases for adjudication. Strategic criminal intelligence is 'big picture' information for the formulation of policies, as distinct from operational information for specific policing actions. It draws upon diverse information sources including policing and related agencies, auditors/forensic accountants, regulators, private sector firms, and of course 'open sources' such as media and academia. This paper describes contemporary international and European Union contexts for the development of strategic intelligence. It also notes some standard criticisms of risk assessments, risk mentalities, and 'risk society', and explores what can happen when previously 'siloed' (separated) information sources and methodologies are fused together.

At the level of policy, public-private cooperation in the sphere of intelligence appears to be quite formidable.[3] We may think of the linking of European Union internal and external security concerns, the increasing emphasis on partnership and cooperation, and the information exchange between the public and private sectors. More attention is also being paid to governance generally. Over the past few years, there has been greater sharing of both operational and strategic intelligence between public sector agencies and private sector actors. The development of the concept of security in Europe seems to imply a widening surveillance net, covering all public and private sectors, obviating all information 'silos'.

However, the information flow appears to have stronger quantitative than qualitative characteristics, and questions have arisen about quality. Surveillance agencies have reported being 'swamped' with low-grade

[1] EU Security Strategy - Council of the European Union 2003: 12.

[2] CIA study: O. Villadsen, 'Prospects for a European Common Intelligence Policy'(2000) 44 *Studies in Intelligence* (unpaginated) available at <https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/summer00/art07.html>.

[3] P. Gill, 'Not Just Joining the Dots But Crossing the Borders and Bridging the Voids: Constructing Security Networks after 11 September 2001' (2006) 16 *Policing & Society* 27.

information: for example, in relation to money laundering. In contrast, the sharing of higher-quality information may well have decreased. This may be partly because of 'needle in a haystack' problems – the bigger the haystack, the greater the potential difficulty in seeing the needle – and partly because sharing may be the exception rather than the rule when it comes to the most sensitive information.[4] Policy discussions about cooperation are not automatically reflected in practice, especially where there are structural, motivational, reputational, and competitive grounds for public and private sector entities to retain ownership of 'their' information on irregularities and illegalities.[5]

In the following pages, we suggest that policy-makers should in fact be grateful for these apparent difficulties. Negative consequences could follow the integration of currently distinct methodologies and systems – spanning both public and private sectors – that are relied upon for strategic criminal intelligence and thus for policymaking. It may be better, in the sense of being safer, to have access to diverse ('silo') approaches to risk management. In the following pages, we scan the international and European context and drivers of intelligence activities spanning the public and private sectors; discuss the pressures towards and away from further integration of those worlds; and examine possible consequences of further movement towards the integration of intelligence sources and systems.

2 Contexts and drivers of intelligence sharing

> Whether one looks at the worldwide reach of the ambitions of the last and only 'superpower' left, or to the rather different project of the creation of a European Union, the boundaries between what is 'internal' and what is 'external' in matters of security seem to have become irremediably fuzzy. This is quite clear also in the way in which disciplinary boundaries are giving way to the assault of historical change. Does one really know today in Europe when one is speaking of 'domestic' law, 'European' law, or 'international' law?[6]

A currently influential idea in strategic intelligence is combine into one comprehensive 'product' all available data from diverse public and private sector sources and approaches to risk assessment and risk reduction

[4] J. Walsh, 'Intelligence-Sharing in the European Union: Institutions Are Not Enough' (2006) 44 *Journal of Common Market Studies* 625.
[5] J. Williams, 'Reflections on the Private versus the Public Policing of Economic Crime' (2005) 45 *British Journal of Criminology* 316.
[6] D. Melossi, 'Security, Social Control, Democracy and Migration within the Constitution of the EU' (2005) 11 *European Law Journal* 5 at 5-6.

methodologies.[7] The resulting product would be more powerful than a multiplicity of discordant views.

The policy emphasis on international cooperation against serious ('organised', if one wishes) crime and, since 2001, terrorism is so well established that there is no need to labour the point here. A key aspect of this cooperation is intelligence sharing, which consists of (a) real-time sharing of specific, current, and sometimes highly sensitive information about targets, and (b) much more general appraisals of situations, trends, and possibilities, made on the basis of a very wide variety of sensitive and non-sensitive sources. It is the latter that is of primary concern in this paper.

A full analysis of the historical development of defence intelligence and the implications of its entry into criminal intelligence is beyond the scope of this paper. Suffice it to say that successive triggers to defence intelligence were the US-USSR ballistic missile race, subsequent concerns about biological weapons and counter-measures, concerns relating to domestic terrorism in some European countries (notably the UK, Germany, Italy, and Spain) in the post-war period, and international terrorism from the 1990s onwards. Military and security doctrine and language have developed through these historical shifts but the underlying concepts of threat and of threat assessment (or analysis) have remained fairly stable. The conceptual merging of international threats and organised crime threats progressed through roughly three stages: during the Cold War period, threats posed by Italian and other 'mafia'; in the aftermath of the break-up of communism, concerns about foreign corruption and international crime within and radiating outwards from weak and/or what were called 'rogue' states, including some on the immediate borders of the EU; finally, particularly post-2001, terrorism and its possible links with organised crime (an unsettled area). This attempt to provide a summary of the development enforcement preoccupations should not be read as an endorsement of them as necessary or rational, nor as implying that the intelligence activities were or are very effective, which seems unlikely.[8] At this point, we are merely giving an overview of the merging of views on external (defence) and internal (crime) aspects of security, a process in which terrorism – the threat within – was to become the lynchpin.

As part of this process of fusion of external and internal concerns, by 2000 an international threat assessment on international crime had been drawn together by a US interagency working Group, involving the Central Intelligence Agency, the Federal Bureau of Investigation, the Drug

[7] Gill, above n. 3.

[8] See for example the United States General Accounting Office (GAO), *International Crime Control: Sustained Executive-Level Coordination of Federal Response Needed* (2001) Available at <http://www.gao.gov/new.items/d01629.pdf> at 2.

Enforcement Administration, the US Customs Service, the US Secret Service, the Financial Crimes Enforcement Network, the National Drug Intelligence Centre, the Departments of State, the Treasury, Justice, and Transportation, the Office of National Drug Control Policy, and the National Security Council.[9] The 2000 report described global changes favouring crime and impeding crime control, growing geographical reach and operational sophistication of crime groups, involvement of 'insurgent, paramilitary, and extremist groups', corruption and institutional shortcomings,[10] and a range of international crimes 'affecting US interests'. These included terrorism, drug trafficking, alien smuggling, trafficking in women and children, environmental crimes, sanctions violations, illicit technology transfers and smuggling of materials, weapons of mass destruction, arms trafficking, trafficking in precious gems, piracy, non-drug contraband smuggling, intellectual property rights violations, foreign economic espionage, foreign corrupt business practices, counterfeiting, financial fraud, high-tech crime, and money laundering. The report went on to describe criminality in geographical and national terms.[11] In other words, this US report covered the broad environment for crime, some crime markets, and specific settings/national groups.

A number of European drivers for the development of intelligence can also be identified. These include: the perception of a need for security measures in the context of the development of the single market and the opening of internal borders; increasing concern from the 1980s onwards about and cooperation against trans-national organised crime; the use of financial systems for purposes of laundering the proceeds of crime; recognition that considerable damage may be done by serious/organised crime, not only to individuals but also to economic growth and competitiveness; the closer linking of anti-crime actions in the domestic sphere with those in foreign policy, with the enlargement process helping to form a 'bridge' between domestic and foreign policies; and, finally, linkage between security issues and the Lisbon Agenda on employment and innovation. Thus, the EU has emphasised the need for closer cooperation on security between the public and private sectors, as well as for sponsoring conferences and encouraging the formation of various fora, including a European Public Private Security Forum.[12] With regard to technical aspects

---

[9] US Government Interagency Working Group, *International Crime Threat Assessment* (Washington: 2000) (unpaginated) available at <http://clinton4.nara.gov/WH/EOP/NSC/html/documents/pub45270/pub45270index.html>

[10] *Id.,* Chapter 1.

[11] *Id.,* Chapter 2.

[12] EPPSF, *Background & Approach* (Brussels: European Public Private Security Forum 2005) available at <http://www.eppsf.org/eppsf2006/website.asp?page=background>.

of security planning, products, and services, the EU has adopted a Work Programme on Security Research.[13] The overall development of strategic intelligence is intended to take place with reference to a 'strategic concept' of organised and cross-border crime.[14] This will involve an emphasis on greater cooperation, non-silo thinking, and information sharing on the basis of its availability, beyond a consideration of the purpose for which the intelligence may originally have been collected.

It was not just the US influence on the EU that prompted a joining of traditionally separate criminal intelligence and defence intelligence, nor was it just the events of September 2001. Rather, it was the disarray of EU member states when faced with the US demand to support and participate in the invasion of Iraq. The 'Iraq crisis' was a crisis for the European Union for two reasons: firstly, because it split it politically; secondly, when attempting to find common ground in terms of information about the existence or otherwise of Iraqi 'weapons of mass destruction', the EU found so no such common ground.

> The absence of a shared threat assessment was an important reason why EU countries ended up so divided. Each country first formed its own national viewpoint, and only then engaged in half-hearted attempts to form a common stance with its European neighbours. [Subsequently] EU leaders realised that, based on this dynamic, EU foreign policy would never succeed. A new clause was quickly inserted into the Constitution, stipulating that the EU should work out a coherent vision of its strategic objectives. Concretely, leaders tasked Javier Solana with drawing up an EU security strategy.[15]

The subsequent development of EU foreign policy came to provide a 'bridge' between (a) the international security situation after 2001, (b) EU enlargement to its east and, (c) action on organised crime and terrorism. In the process, boundaries between anti-crime policies within and outside of the EU, which had become more permeable in the 1990s, became even more fluid, with police being deployed in external security situations[16] and

---

[13] European Commission, *Decision of 9 February 2006 Concerning the Adoption of the Programme of Work 2006 for the Preparatory Action in the Field of Security Research*, C(2006) 331 (Brussels: EU 2006) available at: <http://www.tpa.lt/SMTP/Naujienos/files/2006-03-06/ANNEX3%20Work%20Programme%20PASR-2006.pdf>.

[14] European Commission, *Communication from the Commission to the Council and the European Parliament on "Developing a strategic concept on tackling organised crime",* COM(2005) 232 final (Brussels: EU 2005) available at: <http://ec.europa.eu/justice home/doc_centre/crime/doc/com_2005_232_en.pdf>

[15] S. Everts and D. Keohane, 'The European Convention and EU Foreign Policy: Learning from Failure' (2003) 45 *Survival* 167.

[16] European Commission, *Communication from the Commission: a Strategy on the External Dimension of the Area of Freedom, Security and Justice*, COM(2005) 491

defence-related methodologies being taken up by a range of agencies within the EU. Views diverge about the desirability of all this, amongst academics[17] as well as other groups; our point is that it is fact and is relevant to understanding how law enforcement agencies think about and compile assessments. In summary, in EU policy terms, the internal/external division has almost completely melted as far as security policy is concerned. High Representative Solana's statements on the European Security Strategy position large-scale organised crime within this wider theatre:

> … the European Security Strategy […] is, in a way, the European Union's 'strategic identity card': a global player, vigilant as regards both terrorism and the proliferation of WMDs, and more traditional sources of instability – regional conflicts, the break-up of states, large-scale organised crime – especially as these different types of threat fuel one another in many parts of the worlds.[18]

Within this context:

> The Secretary General/High Representative was mandated to report on the creation of an intelligence capacity on all aspects of the terrorist threat within the General Secretariat of the Council (SITCEN). […] The Council will now ask SG/HR Solana to implement such arrangements as soon as possible and to keep this question under constant review and to report on progress made at the December 2004 European Council.[19]

In 2004, the Council of the EU agreed that external (second pillar) and internal (third pillar) security assessments would be merged, with a

> compilation of Country Threat Assessments to be used by Second and Third Pillar formations in the development of policy. Further work will be taken forward in the context of the HR/SG Solana's report on the development of an intelligence capacity within the Council.[20]

---

final (Brussels: EU 2005) available at: <http://www.europarl.europa. eu/meetdocs/ 2004_2009/documents/com/com_com(2005)0491_/com_com(2005)0491_en.pdf>.

[17] D. Bigo and others, *The Changing Landscape of European Liberty and Security: Mid-Term Report on the Results of the CHALLENGE Project* (Brussels: CEPS 2007) available at <http://shop.ceps.be/downfree.php?item_id=1468>.

[18] J. Solana, 'Preface' in N. Gnesotto, (ed.) *EU Security and Defence Policy: The First Five Years (1999-2004)* (Paris: Institute for Security Studies 2004) at 6.

[19] European Presidency, *Report to the European Council on the Implementation of the Declaration on Combating Terrorism*, 10009/3/04 (Brussels: EU 2004) available at: <http://ec.europa.eu/justice_home/doc_centre/criminal/terrorism/doc/cs_2004 _ 10009_1_en.pdf> at 7.

[20] European Council, *EU Plan of Action on Combating Terrorism*, 10586/04, LIMITE (Brussels: EU 2004) available at <http://www.um.dk/NR/rdonlyres/

And thus we come to the present time, with public sector criminal intelligence, in its strategic aspirations and context, being influenced to a certain extent by defence intelligence.

3 Structural limitations to integration of intelligence systems

A variety of views are expressed in the criminological and wider literature on 'security governance' – the extent to which the political and business ownership of public sector and private sector security and intelligence activities keep those activities separate or bind them together. Whatever position is arrived at, it has implications for how one understands the prospects for strategic intelligence sharing.

For example, if the security space is compact – in the sense of all public and private sector agencies being closely interconnected – then, in principle and from a policy point of view, integration of at least part of their intelligence procedures, practices, and products would be relatively simple, even if in practice some challenging technical barriers to cooperation might remain. If, however, the security space is highly dispersed, with different 'players' having widely diverse security interests, indeed with some competitive issues between them, then intelligence cooperation might be a more uncertain and edgy affair.

One may summarise the governance debate by referring to a dimension along which the concept of security governance may be placed. The mainstream view within criminology – going back well before terrorism and cooperation on it became such a major as well as controversial issue – is that there is a general convergence and 'blurring' between public and private policing systems.[21] Some experts go further, suggesting that all approaches to security come together to form a tight-knit bundle, the social effects of which are uniform and determinate. This is the view,

> postulated in some of the neo-Foucauldian writing on governmentality, that the diffusion of risk mentalities is the linear product of a singular governing rationality (neo-liberalism being the most obvious candidate) and that it leads ineluctably to the furtherance of coercion and control.[22]

BCE09042-A511-4A9A-8FED-4D323E6FA315/0/EUPlanofActiononCombating Terrorism.doc> at 71.

[21] T. Jones and T. Newburn, *Private Security and Public Policing* (Oxford: Clarendon Press 1998).

[22] For a critical summary, see I. Loader and N. Walker, 'State of Denial? Rethinking the Governance of Security' (review of Johnson and Shearing) (2005) 6 *Punishment and Society* 221 at 221.

That approach, called governmentality – the critical flipside of the wider, normative concept of 'good governance' – informs many analyses of the intersection of public and private security post-2001.[23] The work of Edwards and Gill describes policy making as a process of coalition-building between political groups.[24] Groups or interests constitute themselves around notions of their own moral qualities and, conversely, the dangers posed by other groups.

> [R]ecent history suggests that policy change and learning is fundamentally a product of the normative belief systems of advocacy coalitions and how these constrain lesson-drawing about policy within the parameters of what is thinkable and acceptable from the perspective of these normative beliefs. For example, if it is believed that crime is a product of moral turpitude […] [T]he axiomatic belief that crime is a product of moral deficits in debased individuals delimits the scope of policy-oriented learning to various projects for the re-assertion of moral authority and 'zero tolerance' for those who transgress this authority. [N]ormative beliefs are the foundations of competing governmentalities around which policy actors coalesce.[25]

This process of policy-making is said to occur in four stages: firstly, coalitions problematise an issue in 'such a way as to establish their own role as indispensable for its resolution'; secondly, they employ various 'devices of intéressement' to get their claims noticed; thirdly, they form and lead coalitions, typically using political and/or other inducements; finally, they ensure 'the disorganisation of competing coalitions'.[26] This description of the policy-making process relies upon the notion of competition between coalitions or alliances. It reads as a description and critique of the success of the political right wing in mobilising success for various approaches to security (fight, war, coalitions of the willing, and other neo-conservative motifs). It does not offer an alternative vision or direction.

How could it be that leftist and liberal criminologists adopt a perspective so closed and disempowering? Dario Melossi suggests,[27] as does the philosopher Richard Rorty,[28] that the work of Foucault and his school have acted as a conceptual bridge, over which the concerns of US social and

---

[23] G. Mythen and S. Walklate, 'Criminology and Terrorism: Which Thesis? Risk Society or Governmentality?' (2006) 46 *British Journal of Criminology* 379.
[24] A. Edwards and P. Gill, 'The Politics of "Transnational Organized Crime": Discourse, Reflexivity and the Narration of 'Threat' (2002) 4 *British Journal of Politics and International Relations* 245.
[25] *Id.,* at 249.
[26] *Id.,* at 250.
[27] Melossi, above n. 6.
[28] R. Rorty, *Consequences of Pragmatism* (Minnesota: University of Minnesota Press 1983).

political scientists have been imported into Europe. Thus, the governmentality discourse is similar to that of 'social control'. The key point is that the state is no longer seen as the factor, rather it itself is created, as the result of many social practices thorough society. As Melossi describes, Foucault set aside a historical political conception in which the state 'was seen as the "author" of social control, which "does" this and that, "organizes", "imposes", "prohibits" [etc]'.[29] In place of this state-focused view, Foucault

> allowed for the introduction within European social thought, through the elaboration of an apposite new vocabulary, of themes and motifs that had somehow been central to American political and social sciences for a long time already. And he did this exactly at the point when the social model produced in the North American context was readying itself to become hegemonic.[30]

Here Melossi is suggesting that Foucault provided a language in which mainstream North American concepts – according to which, social control is dispersed throughout society, is created through a complex mix of social relations, and involves the active involvement and consent of citizens, rather than being imposed by the state – could be made palatable within European social science. The most welcome starting point of this is a historical evolution of thought, reflecting democratic progress; however, a less welcome consequence is that of perceiving the old bogeyman of oppression as having been generalised from the state to every nook and cranny of society.

In contrast to that way of thinking about society, governance, and security – as a tightly woven social mesh – some commentators perceive the possibility of real and wide differences between the practices of many of the numerous entities that have an interest in crime control. Of course, the extent of variety and flexibility will depend upon the particular contexts concerned and, just as importantly, on how these are understood and developed by participants. Proponents of this activist perspective include criminologists Johnson and Shearing, whose work drawing on public and private policing is well known.[31] Loader and Walker have given a useful summary of the Johnson and Shearing position:

> Johnston and Shearing develop an argument for 're-aligning' security and justice under conditions of dispersed, multi-site governance… This strategy is informed by two theoretical propositions. Johnston and Shearing argue, first, for a 'problem-solving' as opposed to an 'interest-based' view of policing, one that makes no

[29] Melossi, above n. 6 at 6-7.
[30] *Id.*
[31] See for example L. Johnston and C. Shearing, *Governing Security: Explorations in Policing and Justice* (London: Routledge 2003).

'essentialist' claims about the functions, ends, means or historical trajectories of the police, and proposes, more generally, to conceive of the provision of security as 'the application of any means that will promote safe and secure spaces in which people live and work'. Second, and relatedly, in an argument which connects with broader debates within the study of social control, they contend that the relationship between the mentalities of security provision and its institutions, technologies and practices is 'enabling' and open-ended rather than either 'determining' or 'functionally differentiated' – one where the flow of influence between these different security modalities is reciprocal and a range of diverse rationalities vie for ascendancy in fluctuating political conditions.[32]

Likewise, Williams points to 'bifurcation' or 'structurally constituted boundaries' between public and private policing.[33] Lippert and O'Connor show that contracts between private sector purchasers and providers of private security disincline the latter to exchange information with public sector police.[34] The present author has suggested elsewhere that such limits reflect the normal market sensibilities of the private sector.[35] In this regard, Levi and Pithouse find little evidence of boundary maintenance by public authorities.[36]

Thus, are public and private security characterised by a nexus that is 'enabling and open-ended' (in the above words of Johnson and Shearing) – or is it a tight and indeed 'linear product'? On the one hand, the claims of the 'tight' position would be supported by the governmentality school and also by a face-value reading of public policy declarations on intelligence sharing and formal declarations of fealty by representatives.[37] On the other hand, the daily experience of those 'at the sharp end' of intelligence may point towards 'dispersal', as do some studies.[38] Perhaps it is always the case that a detailed examination of practices yields a more heterogeneous picture than does a top-down or normative analysis. At the end of the day, there

---

[32] Loader and Walker, above n. 22 at 221.
[33] Williams, above n. 5.
[34] R. Lippert and D. O'Connor, 'Security Intelligence Networks and the Transformation of Contract Private Security' (2006) 16 *Policing & Society* 50.
[35] N. Dorn, 'Proteiform Criminalities: The Formation of Organised Crime as Organisers' Responses to Developments in Four Fields of Control' in A. Edwards and P. Gill (eds.) *Transnational Organised Crime* (London: Routledge 2003).
[36] M. Levi and A. Pithouse, *White-Collar Crime and its Victims* (Oxford: Clarendon Press, forthcoming).
[37] Chairman's Conclusions, *Outcome of the European Public Private Security Forum 19-20 December* (Brussels: European Public Private Security Forum 2005) available at <http://www.eppsf.org/eppsf2006/website.asp?page=chairmans_conclusions>.
[38] N. Dorn and M. Levi 'Regulation of Insurance and Corporate Security: Integrating Crime and Terrorism Seriousness into the Analysis' (2006) 12 *European Journal on Criminal Policy and Research* 257.

must remain some element of choice for the analyst and policy-maker alike. Depending on the perspective adopted on the wider structural and political conditions – as a pervasive and ever-tightening net of social control, or as a looser and still-contingent world still open to surprises – so vary the possibilities for the future development of European strategic intelligence. And, we go on to suggest, so vary the consequences.

4 Consequences

Each of the above approaches involves an assumption that risk assessment is a technical matter, in which experts or specialists take the lead in determining the nature and levels of risk. Communication to 'customers', in particular the general public, occurs after the technical exercise has been completed. However, there are approaches to risk assessment in which the public is placed at centre stage. The growing realisation – or to put it more honestly, the acceptance – of the difficulties of understanding risk and particularly the difficulty of predicting it, has resulted in some acceptance that wider stakeholders, not just policy-makers, managers, and experts, need to be involved in risk assessments. The public is installed 'inside' risk assessment, as a producer of information, rather than being viewed simply as an end-user/consumer of the information.

> The limitations of risk science, the importance and difficulty of maintaining trust, and the complex, socio-political nature of risk point to the need for a new approach—one that focuses upon introducing more public participation into both risk assessment and risk decision making in order to make the decision process more democratic, improve the relevance and quality of technical analysis, and increase the legitimacy and public acceptance of the resulting decisions.[39]

Psychologists such as Slovic argue in favour of

> introducing more public participation into both risk assessment and risk decision making in order to make the decision process more democratic, [to] improve the relevance and quality of technical analysis, and [to] increase the legitimacy and public acceptance of the resulting decisions.[40]

Indeed, from the point of view of efficiency of risk assessment, the involvement of wider constituencies of stakeholders may lead to a better quality of assessments. Additionally, looking at things from the point of view of accountability and responsibility, wider involvement spreads the

---

[39] P. Slovic**,** 'Trust, Emotion, Sex, Politics, and Science: Surveying the Risk-Assessment Battlefield' (1999) 19 *Risk Analysis* 689.
[40] *Id*. at 699.

blame in those cases when something occurs that was not predicted or not even imagined as a possibility. In an unpredictable world, it is not surprising to find the government turning to public consultation.

4.1 Stimulation of social anxieties

Mainstream criminological accounts concern the consequences of paying close attention to possible risks, assessing them, trying to measure them, and disseminating the results. Risk assessment increases the extent to which risk is perceived, because it brings it more clearly into focus:

> Implicit also is the notion that more knowledge leads to more risk. […] whatever else risk may refer to outside technical definitions it is to some degree a social and psychological construct. A risk must be identified and appraised. Without human attention it is not a risk in the modern sense of the word. […] Attention and judgement create a risk in this sense; modern systems of risk assessment, that classify, select and respond, bring attention to bear on a danger and give the newly formed risk meaning and technical precision.[41]

Accordingly, some commentators have suggested reducing the expectations being placed upon risk assessment 'experts' and their methods, suggesting that a greater degree of disorganisation and ambiguity should be tolerated. Perhaps public faith in risk assessment could also be safeguarded by greater modesty.

> Risk management would [should] be characterised more by learning and experiment, rather than rule-based processes. It would depend essentially on human capacities to imagine alternative futures to the present, rather than quantitative ambitions to predict the future. [...] A new politics of uncertainty would not seek to assuage public anxiety and concerns with images and rhetoric of manageability and control, and would challenge assumptions that all risk is manageable. States and corporations would not need to act as if all risk is controllable and would contest media assumptions to that effect. Public understandings of expert fallibility would be a basis for trust in them, rather than its opposite. Regulatory organisations would be publicly conceived of more as laboratories, rather than as insurers.[42]

---

[41] J. Jackson, N. Allum, and G. Gaskell, *Perceptions of Risk in Cyberspace* (London: Cyber Trust and Crime Prevention Project 2004) available at: <http://www.lse.ac.uk/collections/methodologyInstitute/pdf/JonJackson/Perceptions%20of%20risk%20in%20cyberspace.pdf>.

[42] M. Power, *The Risk Management of Everything: Rethinking the Politics of Uncertainty* (London: Demos 2004) at 62-63.

4.2 Magnification of disaster

Turning from subjectivist to objectivist perspectives, another line of criticism concerns the consequences of actively trying to manage and reduce the risks, if the means involve standardised approaches to good practice, governance, and regulation. In an analytically radical move, some students of market and regulation suggest that risks may actually ('really') increase as a result of attempts to manage them in standardised ways.

> Avinash Persaud, global head of research at State Street Bank, believes not only that such an early warning system does not exist but that the regulatory and risk management systems in place today are creating additional risk. He says the regulatory mantras of common standards and market-based risk management encourage the herd mentality that characterises investment flows and increase the correlation between events that spread instability through financial markets.[43]

The technical details of this view are beyond the scope of this discussion, but relate to observations of several financial crises in which a large number of financial market players were pursuing the same hedging (risk reduction) strategies.[44] As a result of that, the strategies no longer reduced risk. When market conditions became unfavourable, many large financial players all tried to reduce their exposure but, in doing so, exacerbated the volatility that they had sought to avoid.

The problem is not that market participants try to hedge their risk but rather that they have a tendency to use the same risk models, and may hedge in very similar ways – not realising that the assumptions of the models did not include that common behaviour. Whatever the validity of the risk assessment models might have been at the onset, they become increasingly less valid as more parties follow them. This is a version of the 'madness of crowds', as found in financial markets.

4.3 The exceptional is not rule-bound

Further support for such observations could be derived from debates about the nature of statistical distributions. Whilst some categories of events follow the 'bell curve' familiar from textbooks, in which unusual events and extreme values are so unusual as to be dismissed as 'outliers' and smoothed

---

[43] V. Boland, 'Spotting the dangers in risk management', *Financial Times* (London, 11 March 2002) available at http://62.237.131.23/inmedia/inmedia2002/in-media-2002-15.pdf.

[44] See for example A. Persaud, 'Sending the Herd off the Cliff Edge: The Disturbing Interaction between Herding and Market-Sensitive Risk Management Practices', *BIS Papers No. 2*, 233-240 (2002) available at <http://www.bis.org/publ/bispap02l.pdf>.

out of the analysis, other categories characteristically exhibit discontinuity and extreme values. As Benoit Mandelbrot and Nassim Taleb put it:

> What is wild randomness? Simply put, it is an environment in which a single observation or a particular number can impact the total in a disproportionate way. [… For example, considering people,] while weight, height and calorie consumption are Gaussian [so-called normal distribution], wealth is not. Nor are income, market returns, size of hedge funds, returns in the financial markets, number of deaths in wars or casualties in terrorist attacks.[45]

For present purposes, the point is that the future likelihood of large planes flying into tall buildings and killing thousands of people could not be deduced from the number of past instances of smaller planes flying into smaller buildings containing fewer people, as a 'normal' risk analysis might attempt to do. The likelihood of occurrence of a new category of event cannot be extrapolated from a past lacking such an incident; it has to seen as a new response to the closing off of other opportunities – a form of displacement – although not entirely a new category, since the events of September 2001 followed many years of attacks on infrastructure and shipping.

The connection between this and observations arising from lemming-like behaviour in financial markets is that, in both arenas, the adoption of a single risk model — whether by traders, using industry-standard, 'state of the art' risk modelling, or by government agencies bringing consistency into top-level strategic intelligence[46] — can create a blind-spot corresponding to the increasing probability of new types of event. The practical issue in risk management is whether future trends and events may be anticipated, using methodologies developed by the private sector, the specialist risk industry, law enforcement agencies, and regulatory bodies. This paper suggests not, for a number of reasons. These include: (a) over-reliance on narrow fields of technical expertise undermines the possibilities for prediction, (b) social and market risk-amplification via 'the madness of crowds' is a danger inherent in strong integration of public and private strategic intelligence, and (c) traditional ideas about statistically 'normal' distributions, underpinning virtually all forecasting tools, can dull our

---

[45] B. Mandelbrot and N. Taleb, 'A focus on the exceptions that prove the rule,' *Financial Times,* (London. 23 March 2006) <http://news.ft.com/cms/s/5372968a-ba82-11da-980d-0000779e2340,dwp_uuid=77a9a0e8-b442-11da-bd61-0000779e2340.html> (accessed 16 June 2008) at 1, see also N. Taleb, *Fooled by Randomness: the Hidden Role of Chance in Life and in the Markets* (New York: Random House 2004).

[46] National Commission on Terrorist Attacks upon the United States, *The 9-11 Report*, (Washington: National Archives and Records Administration 2004) available at http://govinfo.library.unt.edu/911/report/911Report.pdf.

sensitivity to the unexpected. Any one of these considerations would be reasonable grounds for concern about the prediction of uncommon but highly adverse events, such as terrorist impacts. Taken together, they certainly signal a need for caution.

5 Conclusion

It used to be seriously believed by policy-makers that, by gathering into one place increasingly more information about the past, one could glimpse the possible future – and could then change it. However, this belief has weakened, following the intelligence failures that led to the events of 11 September 2001 and the failures of financial regulation that resulted in the business crash of 2007-2008.

The security- and market-based critiques touched upon above suggest that increasing the commonality of methods and systems between the public and private sector could actually increase risks. This could be true in three senses. Firstly, the greater the convergence between intelligence systems, the greater the danger that divergent views and insights become squeezed out (see sections above).

Secondly, even an intelligence model that may have been quite reasonably specified at one time could become dangerously vulnerable at another. For instance, if the model has been adopted by all key 'customers', and if their actions on the basis of their common adoption change the situation, the model's assumptions are rendered invalid. Even were the model to be well specified at the start, common adoption by all public and private intelligence entities would necessarily generate 'blind spots', which could be large. In such cases, risk management becomes its own worse enemy.

Thirdly, as readers will be well aware, sophisticated criminals and terrorists are surely capable of thinking, learning, and innovation, and they are flexible and entrepreneurial in their activities. As a consequence, they could outflank any necessarily slower-moving strategic intelligence systems based in public-private partnership – which necessarily become even more slow-moving as more partners integrate. Hence, with regard to operational intelligence, too much convergence and standardisation of intelligence methods could magnify the advantages enjoyed by 'small is beautiful' economic crime networks and terrorists. Suppose, furthermore, that currently-converging but still somewhat diverse public-private intelligence were to be replaced by one standardised approach. If potential criminals could be confident that all security thinking and systems were more or less the same, then they would have the information needed to evade them. Since the level of investment needed to connect all public and private sector intelligence capabilities would be huge, they could not be changed in a

hurry; hence, the tilt to the advantage of criminals would be long-lasting. In contrast, individuals and groups currently considering illegal action face a situation in which different scrutinisers – police, auditors, regulators, private firms, and others – have a variety of means of collecting information. This puts criminals at risk.

5.1 The leading edges of political action

Interestingly, for political reasons the prospects for (and danger of) tighter integration of European strategic intelligence would seem to be greater in relation to economic crime in the context of the internal market (EU first pillar) than in that of justice and home affairs (third pillar). In important areas of public law, such as competition law, anti-money laundering measures, and environmental protection,[47] the EU has strong competencies and these are likely to remain stable. In contrast, in the 'third pillar' the competencies of the EU remain patchy, even after the (currently stalled) 2007 Treaty of Lisbon ('Reform Treaty'). Even if the headline policy focus has been on intelligence regarding terrorism and other aspects of criminal law, social scientists and lawyers will not forget the first pillar aspects of strategic intelligence as they track ongoing shifts in the relationship between public and private sector criminal intelligence and cooperation.

Safeguarding the rights of individuals is an essential aspect of information gathering and sharing.[48] This has been underlined by the well-known cases on SWIFT, air travel, and the freezing of financial assets of suspected terrorists/sympathisers. Whilst the EC court had no difficulty in finding illegalities in the former two cases, it has had to develop its jurisprudence on the basis of jus cogens in order to address the actions of the UN Security Council in freezing assets and the actions of the EU through its member states in implementing measures.[49] Taken together, these cases demonstrate aspects of information collection and the use of that information in the short term. The aspect that is most germane to this paper regards what use is being made of the combined datasets in the broader and longer-term task of constructing a strategic intelligence overview – which in turn informs the further development of policies, including the possibility of creating

[47] Case 176/03, Judgment of the Court (Grand Chamber), Action for annulment, Articles 29 EU, 31(e) EU, 34 EU and 47 EU, Framework Decision 2003/80/JHA [2005] OJ 2005 C 315/2.

[48] J. Vervaele 'Terrorism and Information Sharing between the Intelligence and Law Enforcement Communities in the US and the Netherlands: Emergency Criminal Law?'(2005) 1 *Utrecht Law Review* 1.

[49] Case C-403/06 P, *Appeal brought on 27 September 2006 by Chafiq Ayadi against the judgment of the Court of First Instance (Second Chamber) delivered on 12 July 2006 in Case T-253/02: Chafiq Ayadi v Council of the European Union* [2006] OJ C 294/32.

further surveillance powers. The possibility exists that, in order to be capable of drawing together a wide range of data from many different private and public sector sources, the authorities might wish to encourage further and rapid convergence of information collection categories and methodologies. If so, we move closer to the prospect of having a 'one-tune band', with the attendant aforementioned dangers.

In conclusion, the considerations presented point to serious issues. They call into question any idea that crime and terrorist risk assessment methodologies should become standardised between public bodies, and between them and the private sector. A common public-private methodology could generate authoritative outputs, thus reducing the variety of views available and increasing the risk of everyone getting it all wrong. We need checks and balances. To maximise flexibility, the EU should encourage a security model of public-private partnership, emphasising excellence in diversity in relation to information systems, data collection, model assumptions, analytic models, and reporting. Difference, a degree of incompatibility, the toleration of some mutual incomprehension, and a willingness to give and accept challenges are hallmarks of a learning system. Vive la difference.

There may be lessons here not only for enforcement and intelligence agencies but also for universities – and particularly for law schools and criminology departments. These cannot help but be part of the wider 'intelligence community', contributing models and making critiques, and preparing students to enter the security sector and government. The recent tendency in academia to understand 'research skills' in terms of quantitative methods needs to be balanced by a degree of scepticism about the utility and predictive power of such approaches. Following the events in New York in September 2001, some observers at least have understood that crunching ever-larger historical datasets does not open a sightline to the future. Business schools and financial regulators also are reviewing the implications of an over-reliance on 'quant' skills, as they digest the financial meltdown of 2007-2008. Where scholarship is constituted by a creative confrontation of traditions from law, the social sciences, and business schools, our opportunities for learning deepen.