# What role for the private sector in 'societal security'?

## EPC Issue Paper No.56

October 2008

*By Alyson Bailes*

EPC Issue Papers reflect the views of the authors and not necessarily those of the EPC.

ISSN 1782-494X

EU INTEGRATION AND CITIZENSHIP
PROGRAMME

## The EPC's Programme on EU Integration and Citizenship

The European Policy Centre's Programme on EU Integration and Citizenship focuses on the EU's institutional framework; the prospects for, and consequences of, further enlargement; the search for appropriate policy responses to the challenges posed by Europe's increasingly multicultural societies; and broader citizenship issues.

Continued discussion and creative thinking on the EU's governance is essential to ensure that the European project can move forward and respond to the challenges facing it in the 21st century in a democratic and effective manner.

This debate is linked to key questions of how to involve European citizens in the discussions over the Union's future; the opportunities raised, and challenges posed, by the prospect of more countries joining the EU in future; and the issues raised by our increasingly diverse societies and moves towards common immigration and asylum policies.

This programme, which is chaired by former EU Counter-Terrorism Coordinator Gijs de Vries, focuses on these core themes. It brings together all the strands of the debate on these key issues, addressing them through a number of fora, task forces and projects. It also works with other programmes on cross-cutting issues such as the links between the EU's internal debate on migration issues and the wider one on globalisation and migration, the international ramifications of the debate on intercultural dialogue, and the integration of the Balkans in the Union.

For details of the EPC's activities under this programme, please visit our website: www.epc.eu

# Table of Contents

**About the author**

**Alyson Bailes is currently a Visiting Professor at the University of Iceland in Reykjavik. From 2002-2007, she was Director of the Stockholm International Peace Research Institute (SIPRI) – the first woman ever to hold that post – after a long and prestigious career in the British Diplomatic Service. She chairs the EPC's Human Security and Global Governance Forum and its Project Group on Reinforcing Societal Security in Europe.**

## Acknowledgements

This paper was originally conceived to offer an outsider's perspective on the merits of, and prospects for, Nordic-level cooperation on 'societal security'. It used the various Nordic countries' handling of the role of private business in societal security as a test case for exploring both the arguments for closer inter-state coordination (or parallel action), and the *prima facie* obstacles to it.

In both respects, however, the original study exposed wider issues and lessons that seem relevant to the future handling of the non-military dimensions covered by 'societal security' in the EU and Europe as a whole. The EPC therefore kindly agreed to publish a shortened and adapted version of the text.

The author wishes to thank Bengt Sundelius at the Swedish National Defence College (SNDC) for designing, sponsoring and guiding the project; Magnus Ekengren, Mark Rhinard and Tyra Hertz, at SNDC for their many valuable inputs and encouragement; and Antonio Missiroli at the EPC for making this publication possible.

## Foreword

*By Antonio Missiroli*

Following on from the pioneering work carried out by the European Policy Centre's Task Force on 'Societal Security' in 2006-2007, the EPC and the Swedish Emergency Management Agency (SEMA) have decided to re-launch reflection on this issue, which has moved back to the top of the public policy agenda (if it ever left) in recent months.

In March 2008, the European Commission and the Council jointly delivered a paper on 'Climate change and international security' which has been widely praised for its comprehensive approach and ability to connect the dots in an unconventional fashion.

Meanwhile, the EU Council Secretariat has been tasked with reviewing the European Security Strategy (ESS) of December 2003 and its implementation, and reporting back to the European Council in December 2008. This exercise is likely to take account of most of the issues – lying at the juncture between external and internal policy-making – which have been highlighted in the previous work done by the EPC's Task Force on Societal Security, which led to the publication of an Issue Paper on *Shocks without frontiers* and a Working Paper on *Building societal security in Europe: the EU's role in managing emergencies*.

Last and not least, both the current French EU Presidency and the forthcoming Swedish one – in the second half of 2009 – have shown particular interest in developing dedicated procedures and capabilities for civil protection and emergency management at the EU level. It therefore seems timely and appropriate to sit down again and discuss how best to achieve this by setting up a new Project Group to address this issue.

This is also why, similarly to the way we proceeded two years ago, we decided (in conjunction with SEMA) to kick-start the exercise with an Issue Paper addressing both the conceptual framework of societal security and its practical ramifications in a relevant area – namely, public-private cooperation.

There is arguably no better author to do this than Alyson Bailes, who has followed our reflections closely in the past and has now agreed to chair the new Project Group.

We are extremely pleased that she has accepted this new commitment with the EPC and has already delivered a ground-breaking analysis that will serve as a compass for our work. We are also grateful to SEMA for making it available for publication by the EPC – and confident that the final output from the Project Group will live up to the high standards set by this paper.

**Antonio Missiroli is Director of Studies at the European Policy Centre.**

# What role for the private sector in 'societal security'?

*By Alyson Bailes*

October 2008

## Introduction

Concern about protecting the societies of developed countries from a range of non-military and/or non-traditional threats and risks has grown steadily since the Cold War. There are both relative and objective reasons for the rising importance of this challenge.

In *relative* terms, and for European states in particular, the reduced threat of actual war – and possibly nuclear annihilation – has thrown other issues into higher relief. In *objective* terms, the exposure of European populations to life-threatening risks has grown in several specific areas:

- new and more 'transnational' forms of terrorism, crime, smuggling and illegal human movement;
- new risks of pandemic disease and epidemics affecting animals and crops, and, ultimately, also humans;
- greater 'diffusion' of risks between different continents and societies due to increased global travel, changing patterns of energy supply and other trade in vital commodities, commercial outsourcing, and legal migration or asylum seeking, etc.;
- the current and expected impact of environmental degradation and climate change, including an apparent rise in 'extreme weather' and natural disasters;
- growing human dependence on complex and often fragile infrastructures as a result of both continuing urbanisation and technological development, including greater exposure to (and likelihood of) cyber-sabotage.

What all of these new preoccupations have in common is that, firstly, the 'drivers' of such problems are generally of a non-state or non-human nature, instead of involving traditional ('Westphalian'-style) relations between sovereign states.

Secondly, the 'targets' (elements at risk, elements to be protected) are also primarily economic, social and ecological systems, and the non-state entities and individuals who depend on the integrity and proper functioning of these systems – although the state's own integrity and functioning (i.e. the governance process as such) could in many cases be simultaneously at risk.

Thirdly, the threats originate from both inside and outside the given society, and strike the citizens of that society both at home and abroad – thus breaking down traditional distinctions between 'external' and 'internal' security.

Fourthly, many of these threats and risks affect several countries/societies at once (at least once they reach a certain scale), or arise from transactions that cross several countries/societies. Often, they can also only be controlled and resolved by responses involving more than one state, increasingly coordinated through multi-state institutions; i.e. they pose 'transnational', or fully 'global', challenges.

Finally, the traditional military means and modes of defence are generally agreed not to be the first recourse or primary tool for addressing any of these challenges, although military resources and skills can often be a contingent and/or subordinate part of state-led responses.

Even if these problems confront all developed societies in comparable ways, finding a common vocabulary to encompass them is a tricky task and a permanent challenge. The expression *'societal security'* has, however, gained growing currency in the Norden group (the five officially recognised 'Nordic states' – Denmark, Finland, Iceland, Norway, Sweden) to the point where the Nordic Council of Ministers has used it to define an area of common concern in which all participants in Nordic Cooperation should explore the scope for working together more closely.

The EUROSEC project based at the Swedish National Defence College has been exploring the implications and practical requirements of the same approach in an EU framework, and the Union itself is using a similar, if not often identical, vocabulary in developing its collective approach to the challenges of non-military security.

## Aims of the present study

The aim of this paper is to explore the connection between 'societal security' – considered both in terms of its substantive content, and its merits as a conceptual and operational 'label' – and the growing role of the private sector in just about every relevant field of public policy.

Empirical observation suggests that the importance of this issue is acknowledged to different degrees and handled in sometimes strikingly different ways, both within Norden and among the states of Europe as a whole.

Before considering the public-private dimension, however, it is necessary to understand what 'societal security' means or may mean, specifically within a North European or wider European context. Chapter I of the paper explores this question in some detail.

Chapter II then considers the case for including the private sector within the purview of a 'societal security' or equivalent policy. It includes a brief discussion of the sometimes unhelpful impact of familiar terminology, and ends by considering the merits of a triangular approach in which civil society also plays an active role, both in actual security work, and in moderating the possible excesses both of business and government.

Chapter III contains a brief summary of the findings and some final reflections.

# I. What is 'societal security'?

*Habent sua fata libelli* – names also have fates of their own.

In the context of democratic public policy-making, the label placed on a sphere of governance, a process or a group taking part in it, immediately conveys signals about the nature of the thing described; its boundaries (what is included and excluded, what the elements that are included have in common); and, in the great majority of cases, whether it is viewed with instinctive approval or disapproval.

Names can also carry or acquire 'charisma', and have a catalytic and transformative effect – in a given historic and cultural setting – far beyond what one might expect from their dictionary definition and specific content.

However, names that seem the same from one country and language to another can be 'false friends'. Both the concrete understanding of what they define – and hence what outputs they will generate – and the judgemental overtones attached to them, can vary significantly, even between countries that are close neighbours. Politicians are well aware that you do not necessarily 'sell' something to partners abroad using the same labels and arguments as you use to win acceptance for it within your own country.

What, then, of the 'societal security' label? To any ordinary reader, even when not previously familiar with the field, it is a phrase that instantly implies a *broad* approach to identifying and combating the hazards of the modern world. A wider range of practical phenomena and fields of governance may be included within its scope than almost any other related concept in general currency – simply because the focus is on the whole of 'society' (whatever that may be) and on everything that could disrupt and damage it.

Thus, it can be useful to compare the term 'societal' with some of the most commonly used alternatives.

To start with, the terms 'internal' and 'homeland' security may insufficiently acknowledge internal/external osmosis, the transnational diffusion of risks and exposure to them, and trans-state interdependence. Also, neither the 'society' nor the 'security' in 'societal security' need be limited to match nation-state boundaries.

Furthermore, as a matter of practical politics, 'internal' security could be narrowly interpreted to mean the field typically covered by 'Ministries of the Interior', while 'homeland security' is now inextricably associated (for good or ill) with US national policy.

For their part, the terms 'human' and 'civil' security may put the focus too exclusively on the individual level of risk and response, often implicitly casting the individual only as 'victim', and the government (or its absence) as part of the problem. 'Societal security' should instead lead one to think of society as more than an aggregation of individuals, and of its complex interplay with the state (where the ordinary citizen may have powers, responsibilities and duties as well as needs and rights).

The 'human security' concept has also been developed largely in the context of weak/fragile and developing states: EU citizens may have difficulty relating it to their own concerns.

In turn, 'functional' security is a useful term to encompass dimensions such as infrastructure, environment, energy, food and water provision, and other factors vital for the normal functioning of national and social structures. But it would be a stretch to include within it such things as terrorist attacks, other social violence or perhaps even exposure to diseases and public health responses – which are clearly all part of 'societal security'.

Finally, terms like 'civil emergency management', (internal) 'crisis management', and the like – even if they are themselves not always clearly defined – capture an important sub-set of the work of 'societal security' and can cover quite a wide 'horizontal' spread of hazards. But they all tend to focus on a specific phase of action; i.e. the handling of an individual crisis/emergency threatening the population, normally within the borders of its own country.

### Figure 1: 'Societal security': a crib-sheet

*Use of [ ] indicates uncertain or disputable entries*

**Dimensions/events covered**

[Civil disorder inc. major hooliganism]

Major and violent crime, sabotage

Trafficking (drugs, dangerous goods, persons)

Major economic crime, extortion, corruption

Terrorist attack, [terrorist transit and infiltration]

Major/uncontrolled migration

Large accidents* (including industrial), nuclear, chemical and biological (NCB) events

Infrastructure breakdowns* (including transport and goods delivery)

IT/cyber collapse*

Disruption of energy supplies*

Major pollution*/sharp environmental degradation

All natural disasters

Epidemic diseases among people, animals, crops*

Major social tension/divisions on ethnic or other lines*

[Severe social distress]

[Traffic accidents]

[Major economic/financial breakdown]

* Also when deliberately caused by terrorists

**What do we protect? (and who are 'we'?)**

National territory?

Government functioning?

'Vital functions', including the economy?

Society and individuals? 'Values'?

**Actors**

EU-level (Schengen, European Economic Area)

National government, including 'agencies'

Local government (regional, municipal)

Business entities

Sectoral/professional entities

Civil society groups/NGOs

**Levels:**

| of action | of regulation |
|---|---|
| | Global |
| | International |
| European | European |
| Sub-Regional | [Sub-Regional] |
| National | National |
| Provincial | [Provincial] |
| Municipal | |

A full 'societal security' concept should not only have an even wider horizontal reach, but also additional *phases* of risk analysis, crisis prevention and avoidance, planning, training, early warning, building resilience, recovery and reconstruction capacities – plus a more developed approach to safeguards, restraints and balances (notably between security and freedom).

It implies reviewing relevant systems of governance across a broader field in order, among other things, to 'mainstream' societal security awareness in a wide range of peacetime structures and activities – whereas 'civil protection' duties tend to be associated with quite specific points in the structure.

All this said, the basic question of the scope of the 'societal security' concept cannot be regarded as having been finally settled, and is by no means simple. As shown in Figure 1, the 'middle range' of what it covers is both broad and clear. An additional strength of the concept is that it addresses a given range of hazards regardless of their origin – allowing it to cover the actions of non-state actors and natural forces as well as actions (other than traditional military attacks) by possible state foes.

The remaining definitional problems relate mainly to three key questions:

1. *Who or what is being protected by whom?*

In different usages and interpretations, the focus of protection may variously include, and shift between:

a) society in its own right, or even individual existences;
b) the more abstract values and traditions enshrined in that society;
c) the 'vital functions' of a particular country, made up of interactions between government, the private sector and society;
d) the government's own survival and viability;
e) safeguarding the territory, integrity and independence of the state itself (although this is less often an issue in Europe).

While there is a tendency to start by thinking of 'societal security' as something that the state provides for the citizen, there is also room to debate how far society provides (and should provide) for its own security, as well as the role of business.

These are much more than just conceptual or abstract definitional issues, because the choice of what needs to be protected above all else – and what instead is regarded as secondary, auxiliary or instrumental – should logically determine the design of policy-making and priority-setting mechanisms, and also – when it comes to substantive choices – who is going to be called on (or even coerced into) making compromises and sacrifices.

If the view is taken that the state has sole responsibility and competence to protect all sub-state entities, authoritarianism at home and aggressive selfishness towards others abroad could be only a step away.

2. *Where is the 'softer' or 'lower' boundary of the concept?*

It may be debateable to what extent 'societal security' should cover problems and tensions arising within the economy and society itself of a sort which have not normally been 'securitised' (i.e. incorporated into a security policy-related approach) and which can reach their highest pitch in what we think of as 'peacetime'. This includes issues such as unemployment, growing inequalities of wealth, the condition of the rural population, social marginalisation, gender-based and other forms of discrimination, and ageing. A particularly sensitive question is whether an increasingly multi-ethnic society is to be seen as a risk factor and an issue for 'societal' security in itself.[1]

A middle position on this – which the author prefers – is to concede that all these factors affect the openness and vulnerability of a society to certain kinds of threats and risks, and thus need to be taken into account when planning both for general resilience and for emergency responses.

On the question of a 'lower limit', does 'societal security' include violence (including sexual violence) at the individual level and within the family? Or the damage done by drug taking, as distinct from drug peddling, or by alcohol and inappropriate diets, for that matter? Or traffic accidents?

The range of solutions to these individualised phenomena is quite distinct from the range normally applied by public authorities under the 'societal security' heading. It is probably best to conclude that official conclusions on these questions will owe a lot to subjective national 'cultures' and that it could be difficult to draw a clear dividing line for all circumstances.

3. *Does the 'obvious' scope of the societal security notion need to be challenged?*

The subjectivity and historically contingent nature of all security concepts cannot be stressed too much. Today's multi-dimensional, human- or society-related security agendas can reasonably be thought of as 'post-modern' – since they follow and react against (at least in the developed West) the highly militarised, state- and bloc-driven security regime of the Cold War.

In a longer historical perspective, however, it is the traditional international ('Westphalian') system – with its 'division of powers' between state strategy (executed by a professional military), market economics, and society proper – that looks like an aberration. Some other models – like the Indian caste system – may have presaged it, but others from the hunter-gatherer period, from the Greek city states to Celtic and Viking societies, attached normative as well as practical value to the idea of largely undifferentiated (male) roles in society and a universal ability to defend oneself.

The point of this historical parenthesis is to underline that what today seems to be the most 'advanced', 'enlightened' or 'inclusive' security agenda could also be just a point in a repeated cycle of alternatives, and that the fact that it is currently in vogue may turn out to be a product of transient impulses and fashions.

It is shaped partly by incidents (the most recent local conflicts, 9/11, the SARS outbreak, Hurricane Katrina, the Asian tsunami) and by the question of which additional elites have been 'co-opted' into the security policy-making process and what agendas and interests they have brought with them.

The possibility always remains open that the current scope of 'societal security' may be, both philosophically and, in the light of longer-term interests, too large (i.e. 'securitising' more than needs to be securitised); too narrow (i.e. leaving out some major challenge to security that is still a 'blind spot' for the elite);[2] or – most likely of all – incorrectly balanced and prioritised.

This does not necessarily invalidate attempts to give security a 'societal' base (which is arguably less likely to lend itself to biased or purely arbitrary priorities than a government- or elite-based approach). But it does call for constant testing of the *content* of the concept through reference back to the most unprejudiced possible view of society's actual vulnerabilities, needs and even wishes.

## What is society?

There is one further generic problem in building a security concept on 'society', and a more specific vocabulary issue in the context of typically North European *social* security policy.

The generic issue is who belongs to society and how far this does (or does not) coincide with national boundaries. Different assumptions can be made about how far different groups of people physically present in a country are to be treated as part of the 'societal security' profile, constituency, and tool-set of that country.

Are all immigrants fully part of the state's 'responsibility to protect' and are they also bound by the same responsibility to protect themselves, regardless of how long they have been in the country and what level of citizenship they hold? Or does the 'native core' of the population (including any historic immigrant groups) retain a special claim on the state's protection so that, for example, recent immigrants might be expelled if that is considered necessary for the social good? What about citizens of other EU countries exercising their right of free movement? What about US, Japanese or Russian expatriates who cannot claim even the (still somewhat fuzzy and controversial) benefits of common European citizenship? What about tourists?

Conversely, how far should (and realistically can) a Nordic or EU Member State's societal security strategy cover its citizens when they are abroad for short or long periods? Or economic assets and investments owned abroad by individuals and companies registered in EU countries, which today are both massive and far-flung? What priorities and resources is it appropriate to devote to similar protection of other EU citizens abroad, or to the pooling of consular resources under joint EU mechanisms, in line with the commitment to consular cooperation?[3] For all the Nordic and EU countries, is there a principled and/or practical argument for trying to 'export' societal security (or at the least, provide a good model of it) to other less fortunate countries, extending perhaps to the whole world?

Whatever answers of logic and principle might be given to this last set of questions, it will be clear that it is very much harder for a Nordic/EU state to provide 'societal security'-style protection to any kind of subject beyond its borders than within the homeland, not just for lack of resources (and possible complications relating to the legal framework), but also because the range and balance of threats becomes so different when you move even a little way from your own core territory. This leads on to the question of finding solutions at a more-than-national level, which will be returned to shortly below.

There is also a risk of the state (and/or any larger institutions it belongs to) promising more than it can realistically afford or deliver, and encouraging a degree of dependence on the part of citizens that outstrips its actual ability to protect – the result of which can only be a series of underperformances of the type seen in the response to the Asian tsunami and an erosion of overall trust between government and the governed.

Mobilising private sector capacities is (as will be argued below) an obvious option to explore in order to fill the gap.

# II. What role for the private sector?

## Business and societal security: the spectrum of relevance

Most non-experts in Europe, when asked for the first time how the private sector relates to national (including 'societal') security, are likely to give negative, limited or otherwise biased answers.

Part of the problem for those who are only distantly familiar with the issue is that the first concepts that come to mind are 'privatisation' and 'public-private partnership'. Both of these concepts were developed in a quite different field of public affairs, and both are potentially misleading when applied to defence/security-related phenomena.

Another part of the problem is the negative image created by one of the roles played by the private sector that regularly attracts publicity: namely, the growing activities of private military and security companies (PMCs/PSCs), and the various abuses they are suspected of or found guilty of.

Finally, even for public servants who have come into some practical contact with business, there is the syndrome of the 'six blind men and the elephant'; i.e. the fact that different people experience different, specialised and limited aspects of public/private interaction and may believe that what they perceive is the central and only really significant part of the agenda.

In reality, the potential public/private interface in the (modern) security domain is almost as wide and varied as the subject of security itself.

Business appears at several points along the axis of *threat analysis and policy response*, as:

- part of what needs to be protected (for the sake of national security and social welfare);
- a potential source of threat in itself, and the conscious or accidental abettor of other sources;
- the main target and victim of some specific categories of threat;
- a tool or adjunct of public-policy responses;
- (in some cases) the primary respondent itself.

Along the axis of *governance and systemic roles*, business can be:

- the passive *object* of state security policy (the thing protected), or the *target* of policy when the state limits or regulates its activities for security reasons;
- the performer of various 'downstream' functions where it provides goods and technology (or other information) for eventual government use, but is not active in their use itself;
- directly engaged in security processes in three different ways: (a) as the delegated agent or servant of government; (b) as a partner of government (in control/restraint and risk prevention as well as direct action); or (c), most controversially, acting in its own right as the provider of security services to other non-state entities – and possibly as a non-state 'combatant' itself (the notorious 'mercenary' role).

To make this huge topic manageable, this chapter will only examine the private sector roles that are relevant within an orderly, developed region such as Northern Europe, and that relate to the areas of public policy normally included in 'societal security'. This allows us to leave aside discussion of the roles played by private military and security companies in overseas operations and 'weak states'; and those which directly support military forces (for example, providing training, food and laundry services and military transport).

The role of the private sector in export control and in nuclear, chemical and biological (NCB) safety and security issues, will be briefly touched on insofar as it can be linked to the prevention of threats (attacks, accidents and pollution) that might materialise within a nation.

Thus, this chapter will first run through the set of *prima facie* relevant business roles set out in Figure 2 below, and end with a short discussion of the problems associated with common catchwords like 'privatisation' and 'public-private partnership', and the image of PMCs/PSCs. It will then look at possible stumbling blocks to effective and consensual public-private sector cooperation for societal security, and consider how a 'triangular' approach that empowers civil society as well as linking government and business might provide an optimal framework for solutions.

## The range of business roles

### *Business as something to be protected*

On any logical definition, 'societal security' should mean protecting society not just as a mass of disaggregated individuals, but in all its fine texture and structure, including the full range of legitimate non-state organisations that it encompasses and the level of prosperity and welfare it has attained.

The effective, consistent and sustainable operation of the private sector is linked with, and indeed is part of, these vital functions of society in many different ways. Businesses provide the majority of working citizens with their employment and their pay, while their profits feed back into the national economy through investment and consumption.

In the process of striving to compete and maximise profit, the private sector now carries out the majority of new technological exploration and innovation, as well as bringing into production many of the scientific discoveries made by governmental and academic experts.

Without the goods that business produces, the vast majority of people in a modern society would not have food, drink, medicines, clothes, housing or entertainment. Without the services of banks, insurance companies and other private financial institutions, they would have much more trouble paying for these things when they need them.

Commercial exports and imports allow national producers to gain markets abroad and consumers to enjoy a range of foreign products. The recent explosion of modern electronic media and communications, as well as traditional book and newspaper publishing, has been a private sector phenomenon and – for all its downsides – has brought new opportunities for culture, entertainment, communication and self-expression to even the remotest parts of a country.

Most of the roles mentioned so far are ones that business has played in Western nations since early modern times (15th-17th centuries), with the significant exception of the Communist era in Eastern Europe. They imply little or no transfer/sharing of state prerogatives, and the natural attitude of the state towards them is simply to promote, facilitate and (where necessary) defend them.

More recently, business has taken over a further set of government functions, albeit at varying speeds in different parts of the West (and beyond), as a result of state policies of denationalisation, privatisation and opening domestic markets to full foreign competition (notably in the EU's Single Market).

Most of these functions have more obvious strategic or security relevance than the first set. In several countries, there is still quite an active and heated debate on how far the state should retain – or regain – some measure of direct physical control or tight indirect control: for example, through regulation or restrictions on intra-business transfers, including foreign buy-outs. The sectors in question include:

- the defence industry itself (including its growing capacity to provide defence and security services);
- the industries with the most sensitive 'dual-use' applications, such as civil nuclear energy production, bio-science and bio-engineering, pharmaceuticals and poisonous or explosive chemicals);
- the major public transport networks and vehicle parks;
- the means of extracting or generating, transporting, converting and distributing energy in all its forms;
- the ownership and maintenance of other critical elements of infrastructure, including water and sewage utilities;

- the means of food distribution;
- whatever part of the provision of major social services (health, education, care of the elderly, prison management) has passed into private hands, although this still varies widely even within Europe.

This set of business activities is doubly 'vital' for societal security inasmuch as society depends, in an often literally life-and-death sense, on their being properly and effectively carried out at all times. The damage to societal security if any of these roles were mishandled, sabotaged, subverted or neglected would be much more obvious and immediate than the impact of, say, the collapse of a bank or even a whole manufacturing sector.

The state's interest in *protecting* this set of private sector activities should be correspondingly all the greater, but there is also an element of state concern to *regulate*, *supervise* and when necessary *restrain* or *correct* the way that business seeks to execute its relatively new responsibilities in these fields.

The process of *vulnerability analysis* for 'critical infrastructure' (identifying the most vital supplies, services, routes and major 'choke-points', and then seeking means to protect them and/or provide alternatives) which forms a part of many Western states' civil emergency planning today, applies first and foremost to this range of sectors.

This last point provides a transition to the recognition that business activity (including some things done by legitimate companies and not necessarily defined as illegal) can also be responsible for a number of threats to – and weaknesses in – societal security, whereby business actors damage each other, the interests of citizens, and the viability and authority of the state.

***Business as 'part of the problem'***

Starting at the end most obviously related to security, the range of examples of business as 'part of the problem' includes knowingly or carelessly abetting terrorism by providing financial services, assisting in travel and training, and supplying deadly equipment or technical knowledge.

Smuggling and trafficking more broadly covers all types of conventional weapons as well as Weapons of Mass Destruction (WMD) and dual-use objects and technologies, drugs, cigarettes and people. It can bring corrupt and criminal businesses into league with each other and also with hostile non-state movements and irresponsible states or sub-state factions engaged in conflict.

A sub-set of this problem is the much-publicised issue of the behaviour of foreign companies in conflict zones, which have sometimes made matters worse by siding with violent actors, seeking to profit from the instability (for example, to acquire mineral concessions), or using excessive violence to protect their own facilities.

Business, in other words, is not only a target of, but also sometimes an accomplice to, violent crime, including international crime rings, extortion and protection rackets, and the drugs and sex industries.

Even without such violent connotations, 'bad' businesses can do enormous damage to economies, political systems and public morals through corruption and other forms of economic and financial crime. Careless and irresponsible business practices, including private-sector collusion in wasteful consumption, imposes heavy costs on the environment and contributes in a myriad of ways (not just through energy use and misuse) to the threat of radical climate change.

Last and not least, there are a range of ways (although seen less often now in developed Europe) in which business leaders with socially reactionary or irresponsible attitudes can damage the fabric of society and citizens' interests directly: through the exploitation and unfair or discriminatory treatment of employees; dangerous and unhealthy working conditions; and, in general, the kind of behaviour that provokes major labour disputes with the risk of strikes and demonstrations turning violent.

Under the broad 'societal' approach, all these phenomena fit easily within the definition of threats to security at the individual level. Many of them also have the potential to harm public order, stability, and the unity and authority of the state. With the possible exception of the last (labour-related) category, all of them would now also be recognised as international or, more properly, *transnational* threats to which states have a duty and need to cooperate with each other on the widest possible basis.

An individual national government, therefore, has double reason to address itself to the roles and activities of companies (its own, and foreign) in these fields: for the sake of its own societal security, and in order to play its part in identifying and tackling such threats through international (and often institutional) action.

However, the very nature of these challenges is such that government can only be fully effective by working *with* business: both to prevent as many companies as possible from doing the wrong thing in the first place, and to enlist the help of the good firms (hopefully and normally, the majority) in catching and punishing the bad.

***Business as victim and target***

Aside from its role as part of the social and economic fabric, with the same broad vulnerabilities as other non-governmental actors, the private sector may also be the victim and target of specific types of societal threat that call for specific government attention and action.

All private employees are subject to the same physical hazards as other citizens, from terrorist attacks (most of those killed in the Twin Towers attack on 9/11 were private sector employees) through to pandemic disease. But business leaders at home and abroad are also often preferred targets for kidnappers or assassins with terrorist or criminal motives.

Private airlines are the almost invariable targets of hi-jacking. Business premises are targeted by a range of 'single-issue' extremists protesting over animal rights, fur, damage to the environment or other purported abuses of globalisation. A recent variation on this was the spate of attacks on Danish business representatives and assets abroad by Islamic protestors during the 'cartoon crisis'.

Even without physical violence, businesses may suffer damage that also affects broader national interests if their competitive assets (technology, innovation and patents) are attacked through commercial espionage, intellectual property theft, or actual sabotage. Their investments (particularly abroad) and financial liquidity may also suffer through no fault of their own because of local government action, local conflict, and all the different crises and dynamics that can cause disturbance on the international money market.

A new front for this kind of vulnerability has recently been opened up by the process of 'outsourcing' various labour-intensive functions – service provision as well as manufacturing – to low-wage developing countries. Aside from the issue of quality, the outsourced locations and their employees are likely to be exposed to a much broader range and higher level of existential risk than the parent companies in stable developed nations.

So far, Western businesses seem to have given little thought to offsetting these risks, which include the danger that local employees might indulge in the 'part of the problem' behaviour described above, and thus get the parent company into trouble as well.

Apart from physical survival, liquidity and competitiveness, *reputation and brand image* are also absolutely crucial to a commercial organisation's success, and these can also be the subject of hostile attack – for example, when a disgruntled employee sabotages a company's products. (Indeed, there have been some recent major cases of such sabotage in the food sector, entailing massive costs both to recall the affected products and to rebuild the firm's reputation afterwards.)

The fate of major companies vying with each other for market share at home and abroad has often been defined by governments as well as business leaders themselves as a matter of strategic concern (see the recent French and German references to keeping 'strategic' or 'fortress' capacities in national hands, despite the contrary philosophy of the Single Market).

This opens up another wide area for potential state concern and intervention: both the efficiency and comparative advantages of one's own companies, and the regulations prevailing on foreign markets and the behaviour of foreign states towards their own firms (current economic disputes between Russia and the West offer plenty of relevant examples).

Finally, and completing the circle, private companies (including ones of strategic concern to the state) can be damaged by the indirect economic, financial and psychological consequences of security disasters in other locations and dimensions.

In recent years, the SARS epidemic resulted in global business losses estimated conservatively at US$11.5 billion,[4] and the impact of 9/11 on (notably) the travel, tourism and financial sectors was estimated at US$189 billion just two years after the event.[5] The final balance-sheet will no doubt be far more negative.

In such cases, and also after natural disasters like Hurricane Katrina, companies rely heavily for their survival and recovery on adequate and prompt insurance pay-outs. However, the viability of global insurance itself has become a topic of debate in recent years on several counts.

After 9/11, commercial aircraft insurance premiums soared to such levels that governments had to step in to guarantee them and have, in fact, never yet been able to shed that burden. It can be argued that the enormity of some globalised security hazards may make it necessary for governments to act as insurers of last resort more often. However, few state fiscal systems would be prepared for such a burden, and there are well-founded caveats about how such a practice might deliberately or inadvertently distort competition.

The globalised nature of economic processes also makes it more likely now than in the past that a single chain of events could trigger massive claims simultaneously in many parts of the world and that the present reinsurance system might be swamped as a result.

On a more specific issue, a debate is beginning over how to adapt insurance practices to the challenges of climate change and the demands of corrective policies. In the rich world, there is a strong case for tying premiums more closely to the actual degree of natural risk (and/or the environmental burden created by housing or business activity) in a given location, while commercial insurance is less likely to cover the populations in climate-sensitive developing countries which are likely to need it most.

### *Business as a partner*

It should be clear from the above that there are three broad reasons for the public authorities to engage with the private sector across the whole spectrum of societal security; namely to:

- ensure that they are able to protect the functions carried out by companies which are vital to society against general and business-specific threats;
- prevent the private sector from becoming part of the problem and to enlist its help in preventing harm to society by other agents; and
- harness useful business know-how and capacities, both to look after companies' own security needs and to help protect other actors.

In this chapter, a number of more detailed examples and types of this public-private interaction will be examined, but in a somewhat different sequence: namely, tracking the various stages of societal security planning and action from initial threat, risk and vulnerability analysis through to the handling of real-time emergencies.

It is often assumed that during the *first phase* of threat analysis, which will include efforts to prevent and mitigate threats and to ensure general preparedness, the private sector's only role and interest is to sell technical advice and equipment.

It is true that business has been booming in (non-military) security equipment of all types (from individual gadgets up to large and expensive rescue vehicles or oil-spill clearing systems) in recent years, and that the suppliers of such items are as keen as any other producers to find new markets for them. But it would be a grave misjudgement for public servants to keep business at arm's length throughout this phase for fear of coming under pressure to spend public money unwisely.

There are, first of all, a number of intangible and unpaid inputs that business people can make to the quality of risk assessment on situations both at home and abroad, if given the chance. Through their global involvement, often with permanent offices and other assets overseas (and sometimes in places where the state has no embassy), they can relay useful impressions of security conditions and trends, and also of the reliability and capacity of various possible local partners.

They may well also have experience of conforming with the security requirements of other countries (and institutions), which is of interest given the advantage in designing any new national measures for maximum 'interoperability'. Their input is particularly indispensable for carrying out 'vulnerability mapping', not just because they own and operate many of the objects that need to be protected but also because of their insight into the complex interdependence of any given productive sector, service provider, infrastructure system or utility with other parts of the economic and social system at home and abroad.

It would also be prudent – although it happens surprisingly rarely – for state planners to canvass some business opinions on the likely economic costs (absolute and relative) of any planned new security measures.

Last but not least, there is a considerable private business in risk analysis, forecasting and simulations aimed at the range of risks and threats of special interest to business itself.[6] The latter agenda will never overlap precisely with societal security concerns, and business requirements are often less sophisticated than governmental ones. For instance, a Western firm needs to know certain basic things about the risks of conflict in a given African country to decide whether to go there or not, while a Western state may seek a much deeper understanding in order to help solve the conflict.

It is always instructive to compare the results of such independent surveys with governmental assessments, and it would be prudent for public planners to pay special attention to companies' own estimates of the risks to the private sector. This could include kidnapping threats and violent protest, commercial espionage, exchange rate exposure, supply chain security, reliability of insurance, etc.

Moreover, the data management models created by business for multi-variable analysis, graphic display, scenario building, etc. are often among the most advanced available – and even the world's largest intelligence services have no scruples about borrowing from, or at least experimenting with, them.[7]

However, by going beyond just helping to identify threats to societal security – and ideally, contributing to early warning in specific cases – business can also help to prevent or mitigate at least some of these hazards.

For some time, efforts have been made to enlist the private sector as an active ally (and not just a subject for regulation) in fighting corruption, crime and smuggling. The whole Corporate Security Responsibility agenda also rests on avoiding 'anti-social', welfare-damaging treatment of employees and their local communities – and thus aims *inter alia* to contribute to 'social peace'.

More recently, and above all since 9/11, there has been a wave of new legislation at all levels – from the United Nations downwards[8] – designed to get private actors to take front-line responsibility in the fight against money-laundering for terrorists, the holding of terrorist funds, the intentional or careless leakage of 'dual-use' WMD-related items and knowledge, and their unlicensed transfer and ownership.

As export controls have become recognised as a key part of the arsenal against 'bad' non-state actors and their scope has expanded and become more refined, states and institutions have paid more attention to making sure that legitimate businesses know and can apply the rules. Business advice is also being taken on the necessary updating of watchlists and standards (to deal with technological advances, new customers and channels for smuggling, etc.).

Within the 'dual-use' industries (civil nuclear, chemical and biological) and the weapons, explosives, gas and petrochemicals sectors, business needs to be mobilised to ensure safety and security at its own installations: *safety* to avoid accidents, leakage, contamination and pollution; and *security* to prevent theft, infiltration and sabotage by criminals or terrorists, and betrayal by unreliable employees.

Defensive measures aimed at reducing vulnerability and enhancing survivability and resilience are as important for societal security as they are for 'civil defence' against traditional threats – and business has many roles to play here too.

The private sector can help reduce a society's exposure and vulnerabilities by playing its part in energy conservation and environmental protection efforts, as well as by accepting (or helping to design) the more specific restraints now being introduced in the hope of mitigating climate change. It can also hold strategic stocks of key products on its own account or as the agent of government policies.

Any significant 'native' capacity in the security-related industries and service functions discussed above may be seen as a contribution to national self-sufficiency – important in the context of crises that disrupt external supply. However, there is considerable room for argument over how far policy should seek to maximise such capacity for security's sake, given that doing so may deprive the nation of some of its best comparative advantages in the globalised economy as well as possibly infringing free trade and competition rules.

Survivability can also be enhanced by the physical 'hardening' of vital private sector installations, and the diversification of (and acceptance of some redundancy in) key infrastructures and the sources and routes of supply. Companies in all sectors can be encouraged and helped to carry out their own 'survival' or 'business continuation' planning. This practice was boosted in the US by the experience of 9/11, and in many Western countries by the prospect of a possible 'bird flu' pandemic.

Finally, this series of possible pre-crisis roles concludes with the question of *equipment* for civilian crisis-handling. Today this is produced, more or less exclusively, by the private sector for all types of customers: individuals (witness the huge surge in sales of gas masks and home shelters in the US after 9/11); business itself; the government; and, at least potentially, international organisations.

During the *active phase* of a crisis, as a very minimum, communication and interaction must take place with the private sector in the context of either protecting, suspending or modifying, companies' own activities. Several types of emergency may require areas including business establishments to be closed down (or cordoned off) as well as curfews and restrictions on movement. In a few scenarios, such as a major financial panic or panic-buying of fuel and foodstuffs, government may need to close down or impose special rules on business establishments even while other parts of society continue as normal. *Ad hoc* restrictions on exports are also often relevant.

Other more positive interactions may involve government calling upon business to:

- release/activate prepared stocks (e.g. of pharmaceuticals, fuels, foods, tents);
- operate emergency vehicles and special equipment either purchased in advance by the state, or now provided under lease;
- put various kinds of 'normal' business assets and products at the state's disposal, including those that may

be required for emergency supplies, emergency transport and distribution, rescue services, or to meet special communication and information needs;

- lend the government all the necessary kinds of manpower and human expertise as well as releasing reservists in the event that the armed forces have a role to play;
- help in the evacuation and repatriation of citizens in the event of emergencies abroad, and providing medical evacuation and initial care for the injured;
- provide 'welfare services' at home for permanently vulnerable parts of society as well as victims of emergencies, beyond whatever role private actors are allowed to play in health and social services 'in peacetime'.

In real-life emergencies such as the recent US hurricanes, business people have often performed many of these roles on a voluntary basis, so long as the state did not actively forbid them to do so. A number of reports after Hurricane Katrina suggested that private sector rescue and goods delivery efforts compared very favourably with the performance of official agencies.

It is important to recognise that all these possible roles will involve financial costs and losses to business, and could lead to the destruction of private property and risks to the life and limb of private employees.

In wartime and under 'total defence' systems, these issues are normally covered by general rules drawn up to define the government's 'war powers' or the legal consequences of a 'state of national emergency'. Modern 'societal security' challenges, however, may well arise in spheres not covered by such traditional planning, and will almost certainly have to be handled under a different legal framework; i.e. without a declaration of war or perhaps even of a state of national emergency.

Politically, a government's aim under most of these scenarios will be to limit panic and restore normality as fast as possible. This implies a different logic for handling the productive sector (and media) compared with the all-out national effort and 'sacrifice mentality' of wartime.

States are only gradually facing up to the need to construct a framework of law and administrative prerogative that will be sufficiently clear yet flexible to satisfy these new requirements, and there is an understandable tendency to make regulations piecemeal – for a terrorist incident, for a major pollution incident, for a pandemic or anything else – despite the fact that a really major catastrophe could combine several of these elements.

It is always a good move to draw up *contracts* beforehand with business providers, at local and/or national level as appropriate, for easily foreseeable emergency transfers of property, manpower and services. Not only will this avoid wasting time on financial and legal issues at the moment of crisis; but it also makes it easier for the private sector to accommodate such needs within its own crisis-reaction planning.

It is also crucially important to establish channels of emergency *communication*, not just within the official structure or between the civil authorities and the military, but also with key business players. These will normally include national employers' organisations and branch organisations as well as the owners of important 'target' facilities, repair capacities, stocks, and other 'critical' assets and services.

Finally, *after* a crisis, the business sector will be a major player in returning conditions to normality, both in terms of restoring normal supply and of rebuilding normal patterns of movement, work and recreation.

Beyond the return to a *status quo ante*, however, the private sector may have to be asked to carry out special repair and restoration activities, or to loan equipment and personnel to the government (different from those loaned during the crisis) for the same purposes. It is also common for companies to play a role in executing government programmes for the temporary accommodation and care of displaced populations, or to provide heath care to victims.

Another possible model during a transitional phase is for an emergency function provided by government (perhaps using the military) during the acute phase of a crisis to be made the subject of a special business arrangement – or, of course to use civil society volunteers – before returning to full normality and the customary division of responsibility.

Last but not least, it is in this phase that the strategic importance of insurance becomes evident. It is a great help for government and citizens alike – as well as for those businesses which have themselves been damaged – if insurance payouts are adequate and arrive promptly. There is a lesson here for the pre-crisis stage about the importance of ensuring that as many hazards as possible can be, and *are*, covered by normal commercial insurance contracts.

Under some scenarios, as noted above, government may have to step in to help a domestic or international insurance industry that cannot cope with the unexpected financial burden. Conversely, there could be cases in which a commercial actor could be held legally liable for a significant part of the crisis if, for instance, a large transport accident, an explosion or a release of dangerous materials occurred as a result of its negligence. Then it would be the business of government to extract suitable payment from the culprits to help with the costs of repair and compensation.

**Figure 2: Potential roles of the private sector**
(in a developed/European context)

| | |
|---|---|
| 1. As part of 'vital functions of society' | |
| Basic functions | Employment and wealth creation<br>Technological *acquis* and development<br>Goods production and supply (esp. food, fuel, medicine)<br>Financial services including insurance<br>Import/export<br>Media and communications |
| 'Privatised' | Defence production (services?)<br>Means of transport<br>Energy production, import, distribution<br>Infrastructure and utilities<br>Social services delivery: education, health, welfare |
| 2. As 'part of the problem' | Support and supply for terrorism<br>Smuggling and trafficking<br>Support for violent crime, extortion<br>Corruption, other economic crime<br>Resource misuse, environmental damage, pollution<br>Provocation resulting in labour unrest, abuse of employees, damage to health |
| 3. As 'victim' or 'target' (of specific threats and disasters) | |
| | Individual employees<br>Premises and assets<br>Technological base<br>Investments, financial value<br>Reputation and credit<br>Foreign markets, competitiveness<br>(Indirect loss of business from damage elsewhere) |

4. As partners in 'societal security'

| | |
|---|---|
| Pre-crisis | Source of info, analysis, early warning<br>Planning advice (e.g. on interdependence, efficiency, international practice)<br>Threat mitigation (anti-crime, -terrorist, -proliferation roles)<br>Vulnerability mitigation (e.g. energy conservation, reduced eco-impact, self-sufficiency)<br>Improving 'robustness' ('hardening', diversification, stocks, 'business survival')<br>Supply of equipment and technology |
| In-crisis | Loan/requisition of equipment, technology, experts<br>Emergency supplies<br>Emergency services e.g. information, movement rescue, welfare support |
| Post-crisis | Physical reconstruction and repair, human support<br>Temporary/transitional services<br>Insurance pay-outs |

## 'Health warnings' on terminology

### *'Privatisation' and its pitfalls*

Some very serious and sophisticated published works on the growing involvement of non-state actors in modern defence and security trends have used the term 'privatisation' in their titles. The temptation to do so is almost irresistible, not just because it is a single snappy word to sum up a complex phenomenon, but also because it invites an engaged and even emotional response on the part of the reader.

For the last couple of decades privatisation has been a prominent feature in the civilian sector of the economy, driven into ever newer fields by the most free market-oriented of the Western democracies, and more recently figuring as a kind of touchstone of the will to reform during the transformation of post-Communist countries in Europe and Asia.

It has also been the focus of growing expert criticism and public concern, for reasons that sometimes lie outside the realm of security (such as corruption and favouritism, disproportionate costs and inefficiency), but also in contexts very much related to human life and death.

Thus, the expansion of private medicine is blamed for reducing the level and choice of care available to the poor, privatised transport networks have been involved in scandals over poor security inspection and performance, and privatisation in the civil nuclear industry is linked with public worries over possible pollution and accidents. There have also been reservations – on security as well as ethical grounds – about placing prisons and the transport of prisoners in private ownership.

There is not a great emotional or, indeed, logical distance from these latter worries to the ones that many people feel over the spectacle of private military and security companies taking an ever more active and varied part in defence operations at home and abroad, or over irresponsible sales and inequitable profits in the defence (and homeland security) hardware market.

However, no matter how understandable it may be, using the word 'privatisation' to describe trends in the security and defence field is rarely accurate and often more likely to be misleading.

Strictly speaking, a material object (like a factory or a bridge) is *privatised* when it is transferred permanently from government to private ownership, by gift or sale. Moreover, a service – such as medical care or guarding the delivery of cash – is *privatised* when a government wholly or partially transfers the right, or at least the option, of carrying it out, from the public to the private sector.

What happens at present in the defence sector is rarely if ever about transferring property into private hands. The transition of defence industrial production from direct government manufacture (the old 'arsenal' system) into the corporate sector is a phenomenon which is many decades old in Western states. The initiative is passing further into corporate hands because most of today's new technological breakthroughs are dual- or multi-use (i.e. not exclusively military) ones achieved in a private industrial, or possibly academic setting.

The same applies to the increasingly important and profitable range of equipment produced for security purposes other than military defence, including various fields of 'homeland security'.

Many European countries (including such military leaders as France) maintain a system of large state share-holdings in the defence and aerospace enterprises. But even there, the very fact that there are shares to own underlines that production is being organised and workers employed under a free-market corporate model, quite distinct even from the pseudo-enterprises created by 20th-century Communist states for their 'command economies'.

Typically, any direct manufacturing capacity retained by the state will be applied in limited areas at the top and bottom end of the technology scale: i.e. for the production of nuclear weapons and/or low-tech items such as ammunition.

The last nail in the coffin of traditional state ownership is the increasingly *multinational* character and structure of the largest defence manufacturing companies – at least outside the US.

When it comes to defence and security services, some private-sector activity in this field exists because (developed) states have divested themselves of formerly state-owned capacities. This is certainly true of non-specialist services like catering, clothing, medical care and some aspects of training, where forces' requirements could be 'outsourced' from existing sectors of the private economy.

In countries like the UK, however, it is also true of defence-related research and development, where new capacities were created in the private sector as a result of selling off former state functions. It is appropriate to speak here of a 'privatisation' of productive capacity, not least because it is hard (for financial and structural reasons) to imagine the state ever renationalising the functions concerned.

However, there are other modes where private defence and security services are used which do not fit the same definition.

Firstly, when non-manpower private assets are used for individual operations, such as airlift and sealift or the hire of other specialised equipment. This is a simple case of *leasing* in which the state draws temporarily from the stock of privately-created and -owned property rather than transferring anything in the opposite direction.

Secondly, when a developed state employs private manpower (from private military and security companies) to supplement its own forces, e.g. for guarding and protection (at home or abroad) or for more active functions typically provided by service personnel or state-employed civilians during *ad hoc* operations. Here the state is not permanently relinquishing the right or even the capacity to perform such functions itself: it is *supplementing* such capacity by *delegating* additional duties to private providers on a contract basis.

Such contracts are by definition mission-specific and subject to revocation – and, in practice, are often revoked or revised. If private personnel misbehave or underperform in terms of legal and humanitarian norms, standards and value for money, this is generally because the state has not awarded and written its contracts carefully enough, and has omitted to provide adequate control and monitoring arrangements. There is also the well-known problem of making any international legal responsibility on such individuals 'stick'.

Thirdly, when a state employs private personnel to carry out an internal security task, either on a permanent basis or in a given type of emergency (for example guard duties, rescue services, first aid provision, distribution of emergency supplies), the *ownership* in these manpower resources can be said to have been privatised because the state is not their permanent employer.

Once again, the way they are used on state business is as *agents* performing delegated duties (a human equivalent of the leased airlift or sealift mentioned above). The state does not relinquish the right either to provide the given service to the public or to control the way it is provided; it merely employs a different kind of tool for the purpose.

Fourthly, when private military and security companies intervene on their own initiative to play roles (potentially supporting non-state as well as state factions) during the more chaotic type of conflicts and in weak-state situations.

In this case, the state is not actively and willingly 'privatising' its functions: the private actors, including local armed factions, are either f*illing a gap* left by the complete absence of state capacity or are actively usurping roles from a state they do not recognise or respect.

It is not completely wrong to speak of such an environment as one broadly characterised by the 'privatisation' (or fragmentation, or deconstruction) of security functions – but this means stretching the original analogy very far, since 'privatising' properly means knowingly and deliberately relinquishing control of state property.

Finally, when private suppliers sell equipment to, or perform security services for, other parts of the private sector, it is clear that no transfer is taking place from the state side that could be characterised as 'privatisation'. It could be described as companies *supplementing* whatever fundamental protection they receive from the state in their dealings at home and abroad. As a result, there is a change of balance and distribution between the sum total of security-related activity carried out/mandated by the state and that part which develops independently from any state initiative.

***Public-private partnership (PPP)***

The notion of public-private partnership (PPP) was first developed in the civilian economy, usually in the context of the construction or renovation of major buildings and institutions (hospitals, schools) or public infrastructure (roads, bridges, railways, ports).

Its purpose was to relieve the state budget – at least in the short term – of major capital costs, by inducing private companies to co-finance such projects in return for rewards that might be purely financial (longer-term state repayments) or, more typically, derived from the right to co-own and co-manage the newly-constructed facilities.

In this regard, PPP has almost always involved an element of 'privatisation' of ownership, service provision or both, although privatisation can also occur without PPP (for example, through the direct sale of state assets). In countries like the UK where the process has been developing for several decades, there has been time for second thoughts and for growing criticism of PPP on several grounds:

- 'phoney' accounting (since the state may lose rather than save money over the whole life of the deal and, in particular, has to retain an unfair share of the liability should projects overrun their costs or go wrong in other ways);

- lack of fair competition in the awarding of PPP contracts;
- poor performance by companies, particularly as a result of inexperience and/or cost-cutting to maximise profits; and so on.

For a considerable sector of opinion, 'PPP' has thus come to carry the same dubious overtones as 'privatisation' in general.

**Figure 3: The matrix of ownership in the defence sector**

| | State produced | Privately produced |
|---|---|---|
| State owned | Nuclear weapons | Most conventional arms<br>(state shareholding possible) |
| | Some conventional items<br>e.g. ammunition, naval dockyards | Homeland security equipment |
| | | Military applications of multi-function high technologies |
| Privately owned | | Leased items (e.g. aircraft)<br>Ad hoc charters (airlift + sealift)<br>Some training assets |
| | | Defence and security services<br>(+ manpower and equipment) |

Just as with 'privatisation', however, 'PPP' in its classic sense is much rarer in the defence and security field. The cases that best fit the formula are those where the state invites a defence company to produce an asset at its own expense (say, trainer aircraft). Instead of paying the full price to purchase these aircraft, the state allows the company to recoup its costs by retaining ownership of them (or giving the state a lease) and providing the related training in return for on-going payment.

It is easier to apply this approach to the construction of buildings and other fixed facilities of a non-warlike kind, but here it can be equated to the outsourcing of non-specialised and non-warlike *services* such as laundry and catering, and should not raise any issues of principle aside from the importance of value for money.

Other types of transaction where private industry makes a profit by designing assets for state security purposes may at first glance seem to fit the PPP label but, actually fall into different categories. Civilian sealift and airlift assets, specialised rescue vehicles and craft, specialised equipment to deal with oil-spills and so forth, are either, purchased outright by the state and kept in readiness (in which case they equate to traditional arms purchases), or they remain in private hands and are temporarily leased by the government when required, having no primary or delegated public purpose for the rest of the time.

The other type of case that fits the definition better is when the state regularly or permanently delegates a security-related *service* (and pays for it) to a private security provider that creates and continues to own the relevant assets – manpower and equipment.

However, the greatest scope for confusion lies in the difference between PPP in capital letters and public-private partnership in its wider, more natural sense. The latter term (in small letters) describes just about anything that public and private authorities do together in the security/defence field with a presumed common purpose. This could range from business releasing reservists to join the forces or cooperating in risk assessments and complying with export control regulations, through to the closest possible collaboration between private personnel and state forces in the field of action.

All these forms of public-private interaction have their pros and cons and their own various ethical or political overtones, but the issues involved are not the same as for PPP in the narrower sense – and should not be confused with the latter.

In fact, it would be safest to avoid even the small-lettered form of the phrase when speaking of defence and security transactions (other than in the narrow set of cases mentioned above). Synonyms such as public-private 'cooperation', 'collaboration', 'interaction', 'interplay' or just 'relationships' are not hard to find.

### *Private military and security companies*

Discussion of private sector roles in security is often coloured – in European states and others with a strong tradition of democratic centrally-controlled defence – by negative attitudes to the ongoing growth of private military and security companies (PMCs/PSCs). Several of these have their commercial bases in the same European region (notably the UK and France).

These companies, which are already tainted by the historical association with 'mercenary' activities, have seen their reputations take a further knock from the revelations of widespread abuses by private contractors working with the US-led coalition forces in Iraq, and, to a lesser extent, Afghanistan. Reported and increasingly well-documented problems range from reckless violence (killing and torture) by private military agents to outrageous profiteering and sub-standard service delivery, even by firms performing relatively innocuous tasks such as catering.

Nobody can condone such behaviour, which demonstrates the need for much stricter regulation (both international-legal and commercial) of this whole sector. But it should also be pointed out that a good deal of PMC/PSC activity takes place without causing such problems and provides some genuine economies and efficiency gains for the states – including several EU members – that use it.

Most importantly, however, the area of potential and actual abuse by PMCs/PSCs is almost entirely confined to their *overseas* activities in *less-developed* (especially conflict-ridden) locations.

These companies' internal (or 'societal') security activities in developed states are typically limited to guard services for both commercial and official premises; secure delivery of valuables, emergency rescue and transport (for example, private ambulance services); non-combat support services such as clothing, laundry, catering and transport for state military and paramilitary forces (including those being used for internal security tasks); and, in some countries, tasks connected with the prison system.

Although some of these offer scope for misplaced violence, the carrying of arms by private personnel in such circumstances is either forbidden or very tightly regulated under European legal systems. Large-scale abuses of the sort that could actually damage societal security are almost impossible to envisage, except in the field of efficient delivery on contract and financial probity.

Moreover, the private security industry performing services within Europe has a representative body, the Confederation of European Security Services (CoESS),[9] which is extremely open to dialogue with government and NGOs on the question of standard-setting and is also in communication with the European Commission.

## The downside: objective and subjective obstacles

If it was easy for public and private sector authorities to work together, for societal security or anything else, we could expect far higher levels of mutual awareness of their potential synergies, and the actual collaboration at all stages of the security cycle, than actually occurs anywhere in Europe today.

However both subjective and objective obstacles get in the way of a rational interaction, in combinations that vary from state to state and also from one functional area to another.

Broadly speaking, there is more likely to be closer cooperation at local level and in sectoral fields where the largest and longest-standing transfers of property and capability to private owners have taken place (transport and other infrastructure, energy, IT). Levels of mutual awareness and appreciation of the need to cooperate are also likely to be higher in societies that have experienced internal strife and endemic terrorism, repeated natural disasters or other persistent security challenges, and where the reality of interdependence has been learned the hard way.

Another general phenomenon must be factored in at this stage: the tempo of modern business is mercilessly fast. Large companies, in particular, have to learn to react within seconds to changes in their competitive and regulatory environments (the crisis in the financial markets and oil prices are current obvious examples); to new phenomena that threaten them; or to faults and mistakes that they are found to have committed.

This helps explain why companies are good at finding and rapidly exploiting loopholes in official measures. It also explains why corporate actors are quite often ahead of national and international governmental bodies in more positive fields of action, such as adapting to pressure for 'greener' policies or drawing up survival strategies against bird flu or simply getting to the spot faster in an emergency (the Asian tsunami and the US hurricanes).

When this happens, it can be equally frustrating for governments to find themselves facing a *fait accompli*, and for businesses to see governments trailing behind and sometimes never catching up with new corporate (and consumer) patterns of behaviour.

More broadly, these differing timescales are among the mechanisms driving the perceived drainage of power away from states towards multinationals over the last two to three decades.

### *Practical and structural obstacles*

*Contact points and channels*

Once the demand for public-private interaction moves beyond the sectoral level (where major companies will have regular contact with respective ministries and safety agencies), cooperation in all phases but especially during a live emergency can be impeded by the lack of a clear 'docking' or 'contact point'. Business actors need to know whom to contact on the government side, while the government needs to know whom to communicate with and mobilise on the business side.

Although every Western country has a business federation or Chamber of Commerce or equivalent, it does not follow that this organisation will necessarily agree, or be suited, to play a central contact-point role. Additionally, it may not have the horizontal and vertical links with different groups of business actors needed for effective coordination.

*Other aspects of national 'architecture'*

The way a business organises its branches and activities within a national space need not correspond to the pattern of central, regional and municipal government or to the division of delegated powers within this official structure. However, any structural mismatch will make it harder to achieve a consistent interface at all levels. Another obvious mismatch is when a foreign company provides a major security-relevant service and its top management are not even accessible within the same country.

As already noted, it is often the case that one business sector is better 'plugged into' government for security purposes than others, and that business in general works better with government at regional level or in certain sensitive regions than it does at the central level.

All these discrepancies cause particular problems when an emergency (or urgent policy challenge) is large enough to demand cross-sectoral and cross-regional coordination. They also make it harder for a national government to have the comprehensive vision of business actions and capacities desirable to coordinate emergency response with other local governments, distant governments (as in the case of the tsunami) and/or Brussels.

*Micro-obstacles at the human level*

These include a lack of familiarity between respective elites (which means, *inter alia*, that trust and mutual understanding of capacities have to be built up after a crisis has started), and the lack of practical communications links including channels that are both secure and lasting.

*Issues of security and confidentiality*

It is obvious how these can limit government options for drawing business actors into joint planning, joint crisis handling and so on – especially in cases that may involve military inputs or counter-terrorism. It is perhaps less obvious that business also has concerns of its own.

At the risk-analysis stage, business actors may be reluctant to share their own insights with government if they are unsure how the information will be handled, and will not want to talk too openly about their own vulnerabilities if this is likely to help their rivals or damage consumer confidence. Demands for information-sharing in the field of terrorist financing are seen by some banks as infringing client confidence.[10]

There are other contexts in which business may be anxious to avoid disclosing proprietary information, for example about drugs in development or new surveillance and encryption techniques. Successful public-private contracts for permanent or *ad hoc* security cooperation will include provisions on information handling and confidentiality to allay such concerns.

At the same time, it is important for government to make clear that it does not intend to privilege any of its private partners over others in ways that would distort normal peacetime competition.[11]

*Issues of financial and commercial liability*

While these are of the greatest importance to business, the government elites involved in societal security work will not necessarily be aware of the broad issues involved – let alone the optimum legal and contractual solutions to them.

Generally speaking, private actors offering security-related services to government or taking on delegated roles on a full-time or *ad hoc* basis will want to know what they are to be paid and if the price is fair (and reviewable over time). They will also want to know whether they are expected to share costs (on a PPP model) and if so, what the incentive to do so will be; their liability towards persons or property that may be inadvertently damaged during their operations; and what insurance cover or compensation they will have if they are damaged themselves.

Clearly, the longer in advance and the more consistently these issues can be addressed by government the better, and it is obviously important to make the right kind of legal and contract-drafting expertise available to the relevant government bodies.

## Figure 4: Potential obstacles to public-private cooperation

| | |
|---|---|
| Philosophical/psychological | Duality of political and business establishments<br>Public image of business as ‘mercenary’, ‘exploitative’<br>Assumption that ‘business is on the right’ |
| | Business fear of state interference, assumption of state<br>Incompetence<br>Excessive business reliance on state subsidy and protection<br>Attitude that ‘security isn’t our business’ |
| | Confusion over terminology/concepts, esp. ‘PPP’,<br>‘PSCs’, ‘privatisation’ > misconception of the agenda |
| Frames of reference | Business has more ‘transnational’ (or global) forms<br>of ownership, fields of activity and frames of reference<br>Business sees a different spectrum of ‘threat’<br>Differing prioritisations of threat linked with<br>■ actual exposure<br>■ sense of responsibility<br>■ capacity to influence/react<br>■ cost/benefit analysis |
| | Differing experience/concept of regulatory framework<br>(international and national), different conscious<br>or unconscious ‘norms’<br>Differing timelines |
| Objective and structural | Lack of clear organisation/hierarchy/contact-point:<br>on public side, on business side<br>Different ‘architecture’ within the country<br>Differential contacts/experiences<br>■ in different sectors<br>■ in different locations |
| | Lack of personal networks (contact, familiarity, solidarity)<br>Lack of (secure, lasting) communications links |
| | Sensitivity/classification of information (on both sides) |
| | Issues of pricing (or cost-sharing) and liability, lack<br>of or unfamiliarity with contractual models |

### The role of civil society and the ideal triangle

There is a practical case to be made that a ‘societal security’ strategy should not exclude business. But there is also both a practical and moral case that it should not exclude the people either.

As argued in an earlier chapter, if a societal security concept remains the exclusive property of state authorities both in conception and execution, it is hard to be sure that it is really providing what society needs in the way that society prefers. At worst, protective security can become a pretext for authoritarian coercion – including corrosive intra-societal discrimination.

More directly relevant to the purpose of this paper, however, is the effect that drawing civil society into the provision of 'societal security' can have on the conduct and effectiveness of business and government.

In economic life, generally, it is clear that the population at large relates to business and also exercises influence over it in ways the state cannot imitate. In the employee-employer relationship, the power is generally assumed to lie on the business side. In the consumer-producer and shareholder-management relationships, however, the social actors at least have the opportunity to wield much greater influence.

In recent decades, for instance, organised consumer and popular movements have forced the private sector to change its behaviour markedly on various issues. These range from 'green' issues, including organic production methods and recyclability, to the use of foreign child labour and sweatshops, the fur trade, activities that make use of animals, and other issues that fall under the – now professionally well-developed – concept of Corporate Social Responsibility (CSR).

Government was indifferent on some of these issues, but even where it shared popular attitudes, official action alone would have been less likely to have achieved such sweeping results. Official edicts can ban certain business methods, but they cannot force business to put large assets and energy into developing better methods, whereas informed consumer demand, underpinned sometimes by shareholder activism, has done just that. This has been particularly effective in the Anglo-Saxon and Nordic countries, where business is most exposed to everyday scrutiny and most concerned to 'clean up' its image.

How does this general recognition of business dependence on (and sensitivity to) citizens' power translate into the security field? Perhaps not as powerfully as it should, given that we have not recently seen many mass campaigns on direct security issues such as arms' manufacture or the actions of companies with a stake in conflict regions. Even the much-publicised concerns regarding private military firms have yet to give rise to any major NGO campaign, including action in the streets.

However, many 'ethical' share funds do select the companies to invest in on the grounds of their non-involvement in the arms trade and other violent or oppressive behaviour, as well as general 'green-ness' and CSR. There are also many cases of civic activism against actual or supposed security hazards created by business activities, most notably the civil nuclear industry and waste disposal generally.

Whether well-founded or not, the concerns behind these protests have generally led both companies and governments to ostentatiously tighten up their safety rules. In these ways, citizens can act as a useful normative 'back-stop' or the other half of the pincers, together with government, in restraining possible corporate abuses and ensuring that the private sector does not cause and aggravate societal disasters of various kinds.[12]

In an actual crisis, the interdependence of people, business and government is much clearer. Just as government relies on reservists and volunteers to fly into action as soon as they are needed, business depends on its workers to keep coming to work as long as they can (or work from home), and on consumers to keep buying its products and acting normally for as long and as far as possible.

When the converse happens and there is consumer panic (including panic buying) beyond what the situation really justifies, business can incur large and possibly permanent losses. This is particularly true of banks and credit institutions, whose fortunes are determined so much by the intangible of 'confidence', as so graphically demonstrated by the impact of the 'credit crunch' on financial markets across the globe.

Conversely, how does business help individuals in an emergency (over and above the indirect contribution it makes by helping the state effectively)? It makes and sells individual safety and security equipment, including genuinely necessary items that the state is unlikely to provide. However this market, like any other, is subject to partly irrational forces, and cases of exaggerated consumer buying are often reported (e.g. gasmasks and duct tape in the US after 9/11).

An interesting special case is that of pharmaceuticals. Here recent debate over, for example, preparing for a possible bird flu epidemic, has demonstrated the wisdom of not leaving everything to normal producer-consumer dynamics (which could lead to mal-distribution and irrational hoarding of remedies), but instead having the government purchase and distribute strategic supplies.

Just as significant for both social survival and morale and good order, however, is that during a crisis, companies should continue to produce the full range of their products and offer the full range of their normal services (including non-vital ones that are important for morale, like entertainment).

It should do so without drawing on more than the minimum of government help, which would otherwise divert resources from tasks of an even more life-and-death nature. There is also a strong case for using the commercial media (and the privately-run Internet) to disseminate useful information and instructions at all stages.

Business's own survivability and discipline remains crucial as the crisis moves into the phase of reconstruction and return to normality. At this stage, the adequate capacity and smooth running of insurance systems becomes a major issue of welfare at the individual level as well as for other businesses and state concerns.

In some countries, the strict concept of public-private partnership as described above – shared financing tied to various form of subsequent shared ownership and management – has been applied to major rebuilding tasks after conflict or natural disasters.

The natural conclusion from all this is that the goal of 'societal security' at both national and international level will best be served by approaches that harness and link the capacities of civil society and its groupings, private business and the state in a *triangular system* with elements of mutual dependence along all three sides.

Even this ideal model, however, can be interpreted in some more and some less satisfactory ways. It could be very efficient in Communist and other dictatorial states where society and business had little choice about the roles they played. Under the classic 'total defence model', the same interactions would have taken place under an ultimate military command, which is generally felt unsuitable for today's societal security endeavours.

In a modern democratic context, and in the 'peacetime' environment where most concrete emergencies are expected to arise, there is both an opportunity and a need to enlist business and society as actors with a mind of their own and with their own ideas on the optimum form of partnership.

In practical terms this means involving business and society representatives at the early stages of planning, policy conception, process design and role allocation – both at central levels and in dispersed locations (where much of this probably happens more naturally already). It is particularly interesting to reflect on how this three-way interaction could be realised beyond the national level, for example in a Nordic regional setting and in the context of EU and NATO civil protection policies.

Last but not least, if both business and civil society actors can be empowered in this ideal fashion, a responsible governmental elite should recognise that these two other actors may sometimes wish to 'gang up' against the state on security-related issues – and that it may be no bad thing for them to do so.

This has been especially clear in the US, where business leaders have been even more strident than civil rights advocates in protesting against the terrorism-motivated clamp-down on foreign visitors. In another example, when the UK government tried to bring in legislation against religious hate crimes, civil rights groups and the media both drew attention to possible problems for freedom of speech and of worship which influenced Parliament's eventual decision to reject the measure.

Such joint protests from these two other sectors are hard for government to ignore, and will often be a signal that it is actually in the best national interest to abandon the plans in question – or to make a greater effort to persuade international partners to modify them. And where government remains convinced that it is in the right on a given measure, joint protests from business and society should still impel it to at least make a greater effort and find more convincing ways of putting its case across.

After all, in many of the fields in question, the government's aims and its performance in relation to outside partners can only be fully ensured if both business partners and the general population are ready to help – not hinder its actions.

### Figure 5: The government-business-society triangle (selective examples)

| | | |
|---|---|---|
| **help government:** | ***THE PEOPLE*** | **help business:** |
| Conscripts and reservists (used internally)<br>Volunteer civic service (e.g. Red Cross)<br>Taxation + requisition | | Pressure on business abuses and ethics<br>Individual roles in business continuity<br>Keeping confidence (no 'run on banks') |
| International protection<br>Advice and leadership<br>All state security functions/assets | | Individual safety/security products<br>Strategic supplies, pharmaceuticals<br>Maintaining supply/service during crisis |
| **helps the people:**<br>***GOVERNMENT***<br>**helps business:** | | **helps the people:**<br>***BUSINESS***<br>**helps government:** |
| Protects assets + investments<br>Combats economic crime/espionage<br>Safety regulations and agencies | | Advice, info and risk mapping<br>Control of dangerous goods/technologies<br>Inputs of goods + services for crisis response<br>Recovery, reconstruction, insurance |

Also: ***Business helps business*** – supply chain, business safety equipment and security services
***People help people*** – discipline, civic organisations, rescue and support for the vulnerable
***Government helps government*** – aid for official continuity of function during crisis

# III. Final summary and reflections

## On 'societal' security

This definition of security is fitted to present-day thinking about the breadth and hierarchy of threats/risks to developed democratic states. It is potentially wider than some of its close analogues in functional scope, and can extend backwards and forwards in time from 'hot' emergency management.

However, it creates inherent problems of definition over: a) 'who protects whom' (including the dangers of authoritarianism in a 'top-down' approach); b) whether to include foreign residents and visitors and national citizens abroad; and c) how far a broader world 'society' deserves protection.

## On the role of private business

Contrary to the natural assumption of many European citizens, the private sector is relevant to societal security in a wide range of ways. It is part of what needs to be protected for the viability of the state and the public's well-being. It is a potential source of damage when it acts malignantly or irresponsibly. It is a preferred target for certain kinds of human and non-human risk agents. And it is a potential partner for government in designing and executing a good societal security policy both at home and abroad.

In this last role, business can help in different ways at the stage of risk analysis and policy design, in concrete emergency planning, in tackling *ad hoc* events and hazards; and in the process of post-crisis return to normality and reconstruction.

It is important not to let the hard-headed assessment of the private sector's potential – for good or ill – in all these capacities be blurred by misunderstandings over the application of terms like 'privatisation' and 'public-private partnership', or by negative perceptions of private military companies.

There are, however, plenty of more concrete difficulties standing in the way of effective public-private cooperation over societal security. They fall into the broad categories of:

- philosophical and political attitudes (excessive separation and even alienation between governmental and corporate elites);
- different frames of reference and physical or mental 'maps' of threat and response, leading to different priorities and preferences;
- a variety of 'micro' practical problems – including difficulties over contact points, matching structures, communications, confidentiality and financial/legal arrangements.

The healthiest and most effective 'societal security' policies will be those that build on a triad of government, business and civil society. Business and civil society are interdependent in practical terms, and recognising the potential of citizens to help themselves is a further safeguard against excessive 'top-down' approaches. Consumers have great power to change business behaviour – also in security-relevant fields – while business and the citizens may sometime have a common grievance against heavy-handed state intervention.

# Endnotes

1. In general terms, it could be argued that the 'societal security' doctrine must face up to the question of whether there could be *several different 'societies'*, defined on ethnic, confessional, geographical or other grounds, competing for 'security' within a single state. The next question would then be whether the 'societal' concept is the ideal one for finding a peaceful and productive solution to such competition, or whether something else – e.g. an accommodation couched in political and constitutional terms, or a division of economic benefits – might solve the problem faster while leaving room for a wider 'societal' tolerance and solidarity to evolve later. Examples like Bosnia-Herzegovina, Iraq and Sudan show that this is far from an academic issue.
2. The danger of ignoring 'unknown unknowns' is explored at length in the latest book by Nassim N. Taleb (2007)*The Black Swan: The Impact of the Highly Improbable*, London: Allen Lane.
3. The report presented to the EU by Michel Barnier in May 2006, requested by the European Commission President, includes proposals for: a unified information base for all EU citizens travelling abroad; the pooling of EU Member States' consular resources; an emergency reserve fund and common funding for the full costs of major evacuation operations; the creation of consular 'flying squads'; an experiment with 'European consulates' in four holiday regions; and a common consular code (see http://ec.europa.eu/commission_barroso/president/pdf/rapport_barnier_en.pdf).
4. This covers direct losses to business in South-east Asia, North-east Asia and Canada, and does not take account of knock-on effects elsewhere.
5. Plus US$100 billion of directly related government spending.
6. A sophisticated example is the series of global risk assessments by the World Economic Forum, available at www.weforum.org/en/iniatives/globalrisk/index.htm
7. It is important to distinguish the set of business roles advocated here from the actual collection of *intelligence* by private actors or the delegation to business of responsibility for making *intelligence assessments*, at home or abroad.
8. The reference is to UNSC Resolutions 1373 of 2002 and 1540 of 2004 on terrorist financing and on WMD transfer and possession, respectively.
9. See the CoESS website www.coess.org which includes a survey of national regulations at www.coess.org/studies.htm, and the CoESS/Uni Europa voluntary 'Code of Conduct and Ethics for the Private Security Sector'.
10. See Georges S. Baur (2004) 'Banking in an international and European framework: the case of Liechtenstein' in Alyson J.K. Bailes and Isabel Frommelt (eds.) *Business and Security: Public-Private Relationships in a New Security Environment*, OUP for SIPRI.
12. During the clean-up after Hurricane Katrina there were accusations that the US Administration was granting reconstruction contracts on partisan grounds rather than to the best qualified and lowest bidder.
12. Another interesting aspect of this issue, which has not been sufficiently explored in security studies, is the restraining and guiding role exerted over business by insurers, credit suppliers (including venture capitalists), auditors and management consultants. All these have become involved in the effort to inculcate standards of environmental responsibility, and in the enforcement of government-made rules such as the US Sarbanes-Oxley Act of 2002 on corporate governance.

    Put simply, if insurers will not insure any business that does not enforce a given standard (say, a rule of climate protection or workplace safety), those which refuse or ignore the standard will lose competitive advantages and the market itself will drive them out before long.

    Thinking about ways of harnessing these intra-business dynamics for emergency management-related purposes is in its infancy, but a number of ongoing initiatives are linked with the work of the non-governmental International Standards Organization (ISO). The ISO already creates standards on aspects of health and safety at work and on supply chain security, and is now considering a set of norms explicitly dedicated to societal security, as well as a standard of non-proliferation and export control compliance.