Introduction

Business and security: public–private sector interface and interdependence at the turn of the 21st century

Alyson J. K. Bailes

I. Introduction: interdependence old and new

On 11 September 2001, when terrorists struck at the United States, 1000 employees of the investment bank Cantor Fitzgerald Securities were working in one of the towers of the New York World Trade Center. Nearly 700 of them perished in the attack, a greater loss than that suffered by any other single employer, and the firm's headquarters was physically wiped out. Many other companies and their employees also suffered. This attack was one of the plainest and most painful demonstrations of the shared vulnerability of the state, society and the business community, even on the territory of the world's sole superpower. Logically enough, in the weeks and months that followed, these events were to prompt a whole new debate on the several and joint roles of the public and private sectors in tackling their common security challenges.

Interdependence and interaction between these two spheres of human activity are of course nothing new. Since the first organized societies came into being, the guarantee of physical security has been a condition for productive economic activity, and the economy has needed to produce surplus resources to feed and equip its defenders. Should the relationship between the public and private sectors malfunction or get out of balance, everyone would suffer. The inadequate provision of defence for a prosperous community tempts aggressors and undermines confidence and stability. Spending too much on defence, on the other hand, can quickly drain the economic resources which such policies are designed to protect—even if the spending brings great profit for a while to one part of the business sector.

There are other complexities in the basic relationship between defence and business, involving elements of both parallelism and complementarity. Economic strength is in itself a source of influence which helps states to steer security perceptions and processes in directions that are profitable to themselves. To a certain degree it may also be a deterrent: a rich society can not only afford good defences but also recover faster and retaliate harder against anyone who harms it. Defence-related production is a branch of the economy, often an extremely profitable one, which can make major contribu-

tions to full employment and produce shared and spun-off technologies that are also useful for the civil sector. Where defence exports are possible, they may earn money, influence and respect all at the same time. Economic 'sticks and carrots'—sanctions on the one hand, and aid payments or trading privileges on the other—can play an explicit and effective part in the pursuit of security-policy goals.

In modern conditions, these interactions have increasingly been played out not only at the national level but also in the framework of regional and global multilateral institutions concerned with defence and security, or economic cooperation, or both. The experience of the 20th century raised governmental and popular awareness of certain aspects of the business–security linkage, especially during World War II and thereafter. Access to raw materials and protection of trade routes were important aims and conditions of Allied victory in that war. During the cold war which followed, the West's economic and technological superiority was a consciously wielded and perhaps ultimately decisive weapon in its strategic competition with the Communist bloc. Western strategic export controls were developed, not for the first time in history but at the international level and far more systematically than before, to prevent the leakage of such valuable assets to the East. At the same time, the Communist experience showed that attempting to integrate security and business in the simplest and apparently strongest way, by state control of the whole economy in peace as well as in war, did not foster prosperity or even produce an effective defence machine. The Western values that were seen as triumphing and conquering new ground with the collapse of the Soviet Union and the Warsaw Treaty Organization (WTO, or the Warsaw Pact) included the concepts of the market economy and free enterprise.

The principal Western defence alliance, the North Atlantic Treaty Organization (NATO), had developed its own systems to commandeer and mobilize private-sector assets in the event of a crisis, but these systems were based on a philosophy of minimal and latest-possible interference with economic processes. In peacetime, defence and economic goals could not simply be conflated because Western prosperity depended heavily on factors—and could be hit by dangers—existing outside the sphere of the East–West military confrontation. The clearest example was the oil supply, which was endangered by conflicts and political changes (notably in the Arab world) that were only marginally related to any kind of Communist action. The West did not organize its response to and defences against the oil crises of 1973–74 and 1979–80[1] through NATO. The methods which major Western powers used to protect their worldwide economic supplies and markets (and to influence their trade partner countries) did, to be sure, often include defence instruments—aid, training and defence sales, as well as force deployments. Until the 1990s, however, these instruments were typically used under national responsibility and with at best ad hoc coordination. The gradual shift towards a presumption

[1] See, e.g., Heinebäck, B., SIPRI, *Oil and Security* (Almqvist & Wiksell: Stockholm, 1974).

of multilateral security action even when dealing with shared interests outside the scope of NATO commitments might be traced back to the coordinated Western naval patrols and de-mining operations to protect international shipping in the Persian Gulf during the 1980–88 Iraq–Iran War. It came very clearly into focus with the 1991 Gulf War.

In some respects—and not just because of the obsolescence of much of the cold war-related planning or the expansion of free markets—the 1990s could be seen as a time when traditional notions of the defence–business linkage, and people's attitudes towards it, began to shift and diversify. This in turn reflected both the flow of events and a certain fragmentation of different countries' and constituencies' view of the security agenda. At the end of the cold war many predicted that the global policy focus would shift from military security to 'human' or 'soft' security issues such as development and the fight against poverty, disease, environmental threats and so forth.[2] One effect would have been to highlight the role of the private sector as the deliverer, and often initiator, of the processes and services involved in this dimension. In the early 1990s, however, the work of Western security institutions came to be dominated by crisis-management tasks (within and outside Europe) requiring the use of military forces. The need for civilian inputs—from non-governmental organizations (NGOs) and business as well as from government—for successful crisis containment and resolution and post-conflict reconstruction was increasingly appreciated as the decade progressed. The main policy push, however, was still towards rebuilding Western *military* capabilities which had been eroded in the rush to enjoy a 'peace dividend'.

Many governments remained keenly interested in balancing such defence efforts with continuing or increased contributions in other realms of human security. The trouble here was that the Western community could not agree either on the issues to be given priority or on how to handle them. For example, West European and many other states saw the threat of human-provoked or -aggravated climate change as so severe that it justified accepting strong international discipline and possibly economic sacrifices. The USA did not agree on either the characterization of the threat or the responses. Population growth and control was another area of policy hit by conceptual divisions. As a result, the role which private business was exhorted or expected to play in helping to tackle such challenges was quite different, depending on whether it was listening to the US, or a European, or another government—a particular complication for multinational enterprises.

This is not to say that the role of business in the security process and discourse was reduced. On the contrary, it may be argued that in the last decade of the 20th century the independence, the variety and the salience of private-

[2] See Hagelin, B. and Sköns, E., 'The military sector in a changing context', *SIPRI Yearbook 2003: Armaments, Disarmament and International Security* (Oxford University Press: Oxford, 2003), pp. 281–300.

sector roles in global security all increased.[3] When supporting crisis operations, business acted as a voluntary partner in a way that could not have applied during mobilization for traditional national defence: meaning *inter alia* that it could expect reward at market rates. In some circumstances, companies were accused of having been motivated by profit to connive at or even foment violent conflict in territories where the results were expected to strengthen their commercial position.[4] Precisely because of earlier defence cutbacks, governments found themselves needing to use private services on contract for functions previously carried out by uniformed personnel (e.g., for transport and supply, laundry and catering, and even medical support). New crises created new openings and a demand for mercenary troops, private armies or at least private security guards.[5] The defence industry faced an overall drop in demand and sales, sharpest in the European region, but to the extent that it could still find customers it could engage with them more freely across a worldwide variety of markets without regard to previous cold war 'camps'. A number of non-ideological but insufficiently disciplined military transfers—for instance, from the former Warsaw Pact states saddled with poor-quality surplus equipment to cash-strapped developing states, including those in crisis regions—were thought to have had tangible effect in fuelling new conflicts or prolonging existing ones.[6] These phenomena contributed to a general concern and debate among policy analysts: both about the way in which the control of security processes was slipping out of the grip of states to sub-state, trans-state and non-state actors, and about the lack of any evident framework of international regulation or institutional competence for dealing with these new levels of action.[7]

During the 1990s, significant progress was made in defining the impacts of the private sector on security and in bringing them within the scope of public and institutional policy formation, in such specific fields as business behaviour in conflict zones and help in combating organized crime.[8] The most dramatic

[3] See, e.g., Wenger, A. and Möckli, D., *Conflict Prevention: The Untapped Potential of the Business Sector* (Lynne Rienner: Boulder, Colo., 2003); and Nelson, J., *The Business of Peace: The Private Sector as a Partner in Conflict Prevention and Resolution* (International Alert, Prince of Wales International Business Leaders Forum and Council on Economic Priorities: London, 2000).

[4] See also chapters 11 and 21 in this volume.

[5] There is increasing interest in the notion of 'private peacekeeping' and there have already been occasions on which non-governmental actors have completed substantial mediating and monitoring tasks. See Fidler, S., 'Proposal for private soldiers in peacekeeping gathers steam', *Financial Times*, 6 Nov. 2003; and for details of a new private-sector initiative, the Global Peace and Security Partnership (GPSP), see URL <http://www.gpsp.co.uk>. On mercenaries and private military and security companies see also chapters 13, 14 and 21 in this volume.

[6] Bailes, A. J. K., Melnyk, O. and Anthony, I., *Relics of Cold War: Europe's Challenge, Ukraine's Experience*, SIPRI Policy Paper no. 6 (SIPRI: Solna, Sweden, Nov. 2003), available at URL <http://editors.sipri.se/recpubs.html>.

[7] Guéhenno, J.-.M., *The End of the Nation-State* (University of Minnesota Press: Minneapolis, Minn., 2000); Cooper, R., *The Post-Modern State and the World Order*, 2nd edn (Demos: London, 2000); and British House of Commons, *Private Military Companies*: *Options for Regulation*, HC 577 (Stationery Office: London, 2002), available at URL <http://www.fco.gov.uk/Files/kfile/mercenaries,0.pdf>.

[8] See chapters 10 and 12 in this volume on these 2 issues.

security-related controversy surrounding the role of the private sector arose, however, in a different and much broader context.

The last years of the 20th century were the heyday of a general anti-globalization agitation which inherited much of the role, as well as the activists, of earlier peace movements.[9] Constituencies in developing states and their Western sympathizers painted 'big business' in this context almost in the role of a traditional bloc adversary—as a force threatening to crush the identity and independence of its suppliers and consumers, not just to deny them their fair share of prosperity. Correspondingly violent methods were used by the extreme wing of protesters against private-sector targets (e.g., branches of the McDonald's restaurant chain) or governmental targets (e.g., summit meetings). Similar patterns of behaviour were seen in the 'eco-terrorist' movement (attacking targets seen as particularly guilty in the desecration of the environment, such as whaling vessels and logging companies) and the animal rights movement (attacking laboratories, privately as well as publicly owned).[10] More peaceful methods of product boycott and image spoiling were used by the anti-fur lobby and by groups concerned about the exploitation of labour in the developing countries, especially child labour, by companies in the sportswear industry. It was the economic results of these actions that made the corporate world take notice. Apart from any direct costs of hostile action, sales in all parts of the world were vulnerable to the shift of opinions and priorities among the segments of better-off consumers whose loyalty these companies needed to hold. The growth, to a great extent voluntary, of the private sector's corporate responsibility movement—with its various strands ranging from philanthropy in the local community to codes of conduct for subsidiaries in conflict regions[11]—can be seen in large part as an act of self-defence.

II. 11 September 2001 as catalyst

While far from comprehensive, this historical sketch shows that the issue of public–private sector interactions in security was undergoing flux and complex development even before the fatal events of September 2001. Beyond a doubt, however, the terrorist attacks and the reactions to them of the USA and other states gave the 'new security agenda' a massive boost, supplying perhaps the strongest motive felt since the cold war to bring business relationships back to the core of security policy. The attacks highlighted existing and new

[9] In terms of substance and popularization techniques, it also built on previous 'consumer rights' agitation.

[10] Coker, C., International Institute for Strategic Studies (IISS), *Globalisation and Insecurity in the Twenty-first Century: NATO and the Management of Risk*, Adelphi Paper no. 345 (Oxford University Press: Oxford, 2002).

[11] For institutional guidelines developed in these fields see United Nations, 'The Global Compact', URL <http://www.unglobalcompact.org>; and European Commission, Employment and Social Affairs, *Promoting a European Framework for Corporate Social Responsibility*, Green Paper (European Commission: Brussels, 2001), URL <http://europa.eu.int/comm/employment_social/soc-dial/csr/greenpaper_en.pdf>. See also chapter 12 in this volume; and the Internet site of the Business Humanitarian Forum, URL <http://www.bhforum.ch>.

elements of shared vulnerability; ways in which the state might seek more help from business to tackle threats; ways in which business might need more help from the state; and the need for more systematic frameworks of process and regulation to make all these interactions effective. At the same time, the events of September 2001 split the international security consensus—most dramatically within the 'wider West'—on the true nature of the most serious threats and the preferred approaches for dealing with them. Business found itself facing not so much a unitary 'new agenda' as a situation in which rival hypotheses were pursued on a trial-and-error basis, with the potential to bring sudden gains and also sudden new dangers to private-sector players, among others.

In the most simple and direct way, the attacks showed that government, business and society alike could find themselves being targeted by transnational terrorist movements, without compunction or discrimination and on a massively destructive scale. The damage suffered by the private sector extended far beyond the numbers of offices and documents destroyed or even the individuals lost—indeed, many of the worst-hit companies showed remarkable effectiveness and resilience in maintaining or rebuilding their operations.[12] The greatest sums were lost in the insurance, travel (especially airlines) and tourism sectors. Many other industries were affected by the damage to confidence and change in consumer habits.[13] Government did not find its own revenues hit to anything like the same extent, but it had to bear the executive burden of identifying and punishing the culprits and working out how to prevent further attacks. The US Government's response was to push to the top of its security agenda not only the 'war on terrorism' per se but also efforts to control the proliferation of weapons of mass destruction (WMD—or nuclear, biological, chemical, NBC, weapons) which could pose similar or greater 'asymmetric' threats to the world's population.

As 2001 moved into 2002, the fact that the al-Qaeda terrorist network had its main base in Afghanistan brought the problem of chaotic and irresponsible 'failed states' into the same perceived threat complex, to be joined soon by Iraq as a 'rogue state' suspected of both WMD proliferation and terrorist support.[14] Even where the private sector was not directly invoked as a partner or vehicle for carrying out this set of policies, it came to be affected in numerous practical ways: by spending under the new US 'Homeland Security' programme (see section III); by stricter aviation security norms; by other security rules and practices introduced to prevent the import of undesirable persons and objects; by the supplies and services purchased for the wars in Afghanistan and Iraq; by the contracts available or expected to be available for reconstruction in these countries; and by independent consumer decisions, such as the

[12] 'Devastated firms begin their fight for survival', *Financial Times,* 12 Sep. 2001; and 'Assault on America: aftermath', *Financial Times,* 13 Sep. 2001.

[13] Figures are provided in chapters 2 and 19 in this volume.

[14] Anthony, I. *et al.,* 'The Euro-Atlantic system and global security', *SIPRI Yearbook 2003* (note 2), pp. 47–78.

rush to buy gas masks and other protective items (fuelled also by the anthrax scare in the USA in late 2001).[15] To the extent that the crisis was a crisis also for the USA's allies and neighbours, and that most of the corrective measures required some form of contribution by other powers, private companies outside the United States were affected not just by the knock-on effects of US transactions but by parallel developments in their own countries and regions.

There were some respects in which the crisis refocused attention much more specifically on the role of business as a partner for government. One of the first initiatives, developed among United Nations (UN) member states and embodied in the UN Counter-Terrorism Committee (CTC), was to block private-sector financial transfers to known terrorists and to freeze their assets.[16] This added to pressures which had already been developing (in the context of corporate governance as well as anti-crime endeavours) to eliminate or at least clean up the activities of international channels which could be used for money laundering.[17] In the post-September 2001 climate it was easier to get consensus for doing so even at the expense of some inroads into banking privacy. Another existing policy topic that was strongly boosted by the new threat priorities was the control of exports of strategically sensitive goods and technologies, especially those connected with NBC weapons; delivery vehicles such as missiles; and associated 'intangibles' such as scientific knowledge and research results.[18] Clearly, these measures could not be enforced without the compliance, willing or enforced, of private-sector producers in all relevant countries. Last but not least, the aftermath of the war in Iraq (to a much greater extent than after the war in Afghanistan) highlighted the importance of private-sector support for post-conflict reconstruction in the form of both technical assistance and investment. It also showed how hard it could be to secure private-sector support and to ensure that it would be provided on terms regarded as fair by all.[19]

The converse process—of business seeking additional help from governments—was limited, at least in the short term, essentially to the problem of

[15] On the anthrax episode see Hart, J., Kuhlau, F. and Simon, J., 'Chemical and biological weapon developments and arms control', p. 675, and Zanders, J. P., 'Weapons of mass disruption?', *SIPRI Yearbook 2003* (note 2), pp. 683–90.

[16] The CTC was established by UN Security Council Resolution 1373, 28 Sep. 2001, and is mandated to monitor the implementation of the resolution by all states and to increase the capability of states to fight terrorism. On the CTC see URL <http://www.un.org/Docs/sc/committees/1373/>; and chapter 5 in this volume.

[17] See chapters 4 and 8 in this volume.

[18] Anthony, I., 'Supply-side measures', pp. 727–48, and Ahlström, C., 'Non-proliferation of ballistic missiles: the 2002 Code of Conduct', pp. 749–59, *SIPRI Yearbook 2003* (note 2).

[19] The difficulties experienced in Iraq included the physically insecure environment for repair and construction work, which both contributed to and was aggravated by the delay in re-establishing basic infrastructure; problems over establishing a trustworthy legal framework for the handling, e.g., of Iraqi debts and contracts old and new; accusations of favouritism and anti-competitive behaviour by the occupying powers in according contracts to their own companies; and suspicions of inflated pricing and inadequate performance by the latter. See Gregory, M., 'Rebuilding Iraq's oil installations', BBC News World Edition, 23 June 2003, URL <http://news.bbc.co.uk/2/hi/business/3013168.stm>; Gregory, M., 'Management challenges Iraq style', BBC News World Edition, 2 July 2003, URL <http://news.bbc.co.uk/1/hi/business/3038864.stm>; and Nordland, R. and Hirsh, M., 'The $87 billion money pit', *Newsweek*, 3 Nov. 2003, pp. 22–29.

insurance.[20] Insurers sought to cover themselves by dramatically increased premiums for air transport firms, which in turn claimed that they could not continue to conduct their business (in the face of an existing drop in profits) unless government provided support. The USA and the European Union (EU) agreed to do so, but only for limited periods at a time, aware of the risk of providing disguised anti-competitive subsidies which had long been a sore issue in this industry. More room for manoeuvre was perhaps seen at the level of reinsurance capacity. The US Congress moved to propose a federal reinsurance plan (covering 90 per cent of claims over the first $10 billion) on lines already familiar from European practice.

In general, however, it was noteworthy how self-reliant the business sector proved—or chose to remain—in finding ways to accommodate its losses and in making its own judgements on how to create or improve corporate survival plans. More time will need to pass before it can be judged whether these reactions reflected general and permanent characteristics of resilience in the globalized business system, or whether they were affected by special circumstances that might not apply in the case of repeated attacks. There could also be other, less visible or obvious expressions of the trauma suffered. One wonders, for example, whether reduced profit projections, an increased consciousness of risk and a strong instinct to protect one's own may have played some part in the faltering of world free trade endeavours in 2001–2003 and the failure of the 2003 World Trade Organization Cancún summit meeting.[21] (It is easier to identify the part played in worsening the atmosphere by the animosities between different world constituencies created by, in particular, US military countermeasures.)

III. Two years on: new agenda items, second thoughts?

As the world passed the second anniversary of 11 September 2001, the relatively simple lines of reaction and policy development sketched above had come to seem more inadequate than ever for capturing how the international security agenda actually has been, or should be, evolving. The threat analysis drawn up after the al-Qaeda attacks has come under stronger question (and from more directions) over time, as have the correctness and ultimate utility of the countermeasures chosen. Other challenges shared by the public and private sectors which are only indirectly linked with the original 'asymmetric threats' complex have risen to the forefront of policy and analytical attention. The creation of new rules and frameworks for public–private sector interaction, other than in very specifically targeted cases, remains an entirely open field.

From the first, the language of the United States in calling for participation in a global 'war on terrorism'—with its image of a single, uniformly hostile

[20] See chapter 19 in this volume.

[21] World Trade Organization, 5th Ministerial Conference, Cancún, Mexico, 'The Ministerial Statement', 14 Sep. 2003, URL <http://www.wto.org/english/thewto_e/minist_e/min03_e/min03_14sept_e.htm>.

opponent—had been challenged by those who saw terrorism as an older, more diverse and diversely motivated phenomenon. Many doubted that simple connections could be drawn between terrorists, NBC weapon proliferators and 'rogue states';[22] others questioned whether this group of 'new threats' really deserved to be elevated so far above other (military and non-military) dangers to the West. It was possible to support new efforts against international terrorism and yet to argue that its causes could most effectively be addressed by legal, political, developmental and cultural measures—while forceful action might risk merely creating new terrorists.[23] It is interesting to note that, with the possible exception of those standing to profit from higher defence expenditure and spending on homeland security, business leaders did not on the whole join the militant or the scare-mongering tendency. As shown by the chapters in this volume,[24] their calculations of the seriousness of the terrorist challenge were made with the methods of risk assessment rather than defence-style analysis, and led to correspondingly nuanced conclusions. For a company operating globally, the physical and commercial risks arising from old-fashioned conflict and internal violence, crime, corruption and hostile or misplaced government action still come objectively further up the scale of concern than all but the most apocalyptic forms of terrorist action.[25] A survey of 331 large companies in July 2003 found that their expenditure on corporate security had gone up on average by just 4 per cent since 2001, much of which could be ascribed to higher insurance premiums.[26] The new US Homeland Security budget for 2002 represented a much larger and more sudden proportional hike in spending.[27]

The prominence given to WMD in the initial threat picture has been to an extent undermined by the inability of the occupying powers to find clear evidence of active programmes in Iraq after the fall of President Saddam Hussein. The reliability of related Western intelligence and the way it was used in the policy-making process have come under attack, *inter alia* through a formal enquiry process in the UK.[28] Over the same period, provocative and irresponsible behaviour by North Korea and suspicion over Iran's intentions have made clear that the nuclear proliferation danger is real and demands attention

[22] Delpech, T., *International Terrorism and Europe*, Chaillot Papers no. 56 (EU Institute for Security Studies: Paris, 2002), available at URL <www.iss-eu.org/chaillot/chai56e.pdf>.

[23] Simpson, G., 'Terrorism and the law: past and present international approaches', *SIPRI Yearbook 2003* (note 2), pp. 23–31; and Stepanova, E., *Anti-terrorism and Peace-building During and After Conflict*, SIPRI Policy Paper no. 2 (SIPRI: Solna, Sweden, June 2003), available at URL <http://editors.sipri.se/recpubs.html>.

[24] See especially chapters 15 and 19 in this volume.

[25] For a discussion of the range of risks and also the difficulties in evaluating them see Briggs, R., *Doing Business in a Dangerous World: Corporate Personnel Security in Emerging Markets* (Foreign Policy Centre: London, 2003).

[26] See chapters 15 and 19 in this volume.

[27] This is not meant to imply that government spending exceeded corporate spending in gross cash terms—given the scale of company budgets overall, the balance is probably very much the other way. It has been estimated that the US private sector alone had spent more than $150 billion on its own 'homeland security' measures since 21 Sep. 2001. Bernasek, A., 'The friction economy', *Fortune*, 18 Feb. 2002, pp. 103–12.

[28] On the Hutton Inquiry see URL <http://www.the-hutton-inquiry.org.uk>.

almost irrespective of the ultimate findings on Iraq: but the USA itself has chosen to address these cases by non-military methods. All that said, it is important to note that the *international/multilateral* measures taken under the impact of the September 2001 attacks in fields related to terrorism and WMD are not easily reversible and that no one is, in fact, proposing to reverse them. The EU has independently committed itself to an Action Plan to combat WMD proliferation which implies pushing even further for improvements in export controls (including investigation of the control of 'intangibles'), monitoring and inspection, and the destruction of surplus capacities among other things.[29] All these are fields where action will affect the environment for business and would best be pursued with the help of business. The same can be said of one major new initiative which has united the USA, leading European states and Australia, among others—the Proliferation Security Initiative (PSI), providing for searches of ships suspected of carrying WMD in international waters.[30]

Meanwhile, the consequences of the March 2003 attack on Iraq by the USA, the UK and their partners have taken on dimensions quite different from what the US Administration expected and have created a correspondingly wide range of issues for business. Dogs which have not barked yet include any new major slump in travel and consumer confidence or any significant change on the oil market—partly because it has turned out to be so difficult to restart Iraq's own oil exports even at the previous levels. The still difficult and in some ways deteriorating security environment in Iraq has delayed the start of major reconstruction, deterred the private-sector investments that this would require, and made it difficult for private contractors to help even in urgent tasks like restoring electricity supply.[31] The handling of Iraqi debt has become a sensitive issue, and one of those highlighting how hard it is to find practical (let alone widely accepted) solutions for Iraq except under the aegis of the UN.[32] Most dramatic from an economic viewpoint have perhaps been the escalating costs of the US operation, running at $3.9 billion per month in 2003,[33]

[29] Council of the European Union, 'Action Plan for the Implementation of the Basic Principles for an EU Strategy against Proliferation of Weapons of Mass Destruction', Brussels, 13 June 2003, URL <http://ue.eu.int/pressdata/EN/reports/76328.pdf>.

[30] Boese, W., 'U.S. pushes initiative to block shipments of WMD, missiles', *Arms Control Today*, vol. 33, no. 6 (July/Aug. 2003), p. 26, available at URL <http://www.armscontrol.org/act/2003_07-08/securityinitiative_julaug03.asp>; and Weiner, R., Center for Nonproliferation, Monterey Institute of International Studies, 'Proliferation Security Initiative to stem flow of WMD matériel', 16 July 2003, URL <http://cns.miis.edu/pubs/week/030716.htm>. The PSI was established as a global initiative by the United States on 31 May 2003; the Statement of Interdiction Principles was released on 4 Sep. 2003 by 11 state participants (Australia, Canada, France, Germany, Italy, Japan, the Netherlands, Poland, Portugal, Spain and the USA). See 'Proliferation Security Initiative', URL <http://www.globalsecurity.org/military/ops/psi.htm>.

[31] On the other hand, the post-conflict environment has provided new ground for experiment with the provision of private security services by Western companies. See Catán, T. and Fidler, S., 'The military can't provide security. It had to be outsourced to the private sector and that was our opportunity', *Financial Times*, 30 Sep. 2003, p. 13.

[32] Monderer, M. and Mulford, D., 'Iraqi debt, like war, divides the West', *Financial Times*, 23 June 2003, p. 13.

[33] See United Press International, 'Rumsfeld doubles Iraq cost estimate', *Washington Times*, 10 July 2003.

with further costs in 2004–13 estimated to reach $85 billion to $200 billion, depending on the assumptions made about force levels.[34] On 25 March 2003 the US Administration asked Congress for a supplementary budget of $74.7 billion and in October for a further $87.9 billion for costs connected with Iraq. Together with the large sums still being spent on homeland security and the estimated further increase of 6.1 per cent in the main US defence budget in 2003, these expenses pushed the federal budget overall into a record end-year deficit. At the same time, the US external trade budget was expected to post a deficit of some $401 billion in 2003 (equivalent to 3.7 per cent of gross domestic product), rising to $480 billion in 2004.[35] Opinions differ on how dangerous these trends are. The US Administration continues to maintain that high spending and tax concessions can actually boost recovery. What seems clear is that the financial and economic price of military action in Iraq is influencing the business environment both in the USA and abroad, for good or ill, much more than any *direct* costs of the terrorist action of 11 September 2001 could have done.

As time has passed, some in the USA have also begun to question the effectiveness and proportionate costs of specific measures taken in the context of homeland security. Tougher entry visa rules for a range of Islamic and developing countries have obstructed customers' and clients' entry to the USA as well as handicapping, for example, educational exchanges.[36] It is feared that the USA's proposals under the Visa Waiver Program (VWP)[37] to enforce new standards of machine-readable passports incorporating bio-data for hitherto visa-free entrants—still under discussion with other countries—may involve both large conversion costs and, at least during a transitional period, processing delays. New security measures in the field of aviation have to a great extent been accepted as necessary by air passengers but have undoubtedly extended overall travel times, while some of them have entailed significant material costs for the operators. The US Administration's Container Security Initiative (CSI) and Custom–Trade Partnership Against Terrorism (C-TPAT), which have attracted comment from foreign firms and governments because of their substantial extraterritorial effects, have been more contentious.[38] In the

[34] See Holtz-Eakin, D., 'Letter to the Honorable John M. Spratt, Jr. regarding the estimated costs for the occupation of Iraq', US Congressional Budget Office, URL <http://www.cbo.gov/showdoc.cfm?index=46838sequence=0>.

[35] See US Congressional Budget Office, 'CBO's current budget projections', URL <http://www.cbo.gov/showdoc.cfm?index=1944&sequence=0>.

[36] See the annex to Part VI, on the education issue in the United States. The revelation on 23 Oct. 2003 that 125 000 special screenings of visa applications since 11 Sep. 2001 had not yielded a single case of refusal on security grounds set off a new wave of protest from Congress and business representatives. Alden, E., 'Security screening "hurts US interests"', *Financial Times*, 24 Oct. 2003, p. 6. For further criticisms see Alden, E., 'US companies say visa restrictions hamper business', *Financial Times*, 4 Nov. 2003, p. 4.

[37] For details of the countries to which the requirements will apply, the deadlines and developments in the VWP see US Department of State, 'Visa Waiver Program', URL <http://travel.state.gov/vwp.html>.

[38] For a critical account of the C-TPAT see chapter 15 in this volume, and for full details of the CSI and the C-TPAT see chapter 19. A good journalist's review is Murray, S., 'Importers pay the price of heavy security', *Financial Times*, 13 Jan. 2004, p. 8.

United States, particular criticism has been directed against choices made in the area of biological weapon (BW) defence: a massive planned programme of smallpox vaccination faltered against the resistance of many personnel in the health sector and because of legal complications, and has been criticized for diverting resources from *inter alia* research and development of defensive measures against anthrax.[39]

As pointed out above, there are of course winners as well as losers in the business world under almost any imaginable contingency. One of the most dramatic changes in US security behaviour since September 2001 was the increase of 11.4 per cent in real terms in the national defence budget for 2002, followed by a further 6.1 per cent in 2003 and a planned 2.4 per cent increase in 2004. The resources are designed to be spent mainly on new-technology items where US manufacturers have a lead, while existing procurement programmes will continue to run with only slight readjustments or compensating cuts.[40] Coincidentally (although basically reflecting a similar concern to protect the US heartland), spending on the US ballistic missile defence programme was estimated at $6.71 billion in 2003 and to be about $7.73 billion in 2004.[41] For the US defence industry there is little downside to these facts, but—aside from the question of possible macroeconomic damage—they do create issues for the US Administration's defence modernization policy and for relations with foreign governments and suppliers. Defense Secretary Donald Rumsfeld has shown a general preference for 'lean' US forces stripped of surplus roles and costs, and the Department of Defense has been concerned for some time about the results of industrial mergers which have put certain private-sector suppliers in a near-monopoly position, risking non-competitive pricing.[42] The experiences of 11 September 2001 and the wars in Afghanistan and Iraq have, however, provided new impetus for the US forces to invest in advanced technologies for which few if any non-US suppliers are available, while the political backwash prompted some Republicans in Congress to draft clauses for the US fiscal year 2003/2004 defence appropriations bill which would virtually outlaw purchase from non-US sources.[43] The impact of all this on the already troubled US–European defence insutrial relationship will need

[39] On the obstacles to the smallpox programme (but from a point of view committed to its continuance) see Bicknell, W. J. and Bloem, K. D., *Smallpox and Bioterrorism: Why the Plan to Protect the Nation is Stalled and What to Do*, Cato Institute Briefing Paper no. 85 (Cato Institute: Washington, DC, 5 Sep. 2003), available at URL <http://www.cato.org/pubs/briefs/bp-085es.html>. For a more critical report see MacKenzie, D., 'US "too busy" to spot a smallpox outbreak', *New Scientist*, vol. 177, no. 2384 (1 Mar. 2003), p. 10.

[40] Sköns, E. *et al.*, 'Military expenditure', *SIPRI Yearbook 2003* (note 2), pp. 307–12.

[41] US Missile Defense Agency estimates for FYs 2003 and 2004, URL <http://www.acq.osd.mil/bmdo/bmdolink/pdf/fy03aft.pdf> and URL <http://www.acq.osd.mil/bmdo/bmdolink/pdf/budget04.pdf>, respectively.

[42] Sköns, E. and Baumann, H., 'Arms production', *SIPRI Yearbook 2003* (note 2), pp. 373–403.

[43] See Brun-Rovety, M., 'US Senate set to approve $400bn defence spending bill', *Financial Times*, 13 Nov. 2003, p. 4. On the embarrassment caused to the US Defense Department by this development see Spiegel, P. and Alden, E., '"Buy American" stance toned down', p. 1, and 'Rumsfeld blinked after "Buy America" veto call', p. 3, *Financial Times*, 27/28 Sep. 2003. The administration finally succeeded in watering down the offending clause to one with purely advisory effect. It is fair to add that the protectionist aspects of the proposals have been opposed by both US and European trade associations.

to be monitored, but it can safely be predicted that it will, among other things, feed the tendencies both for more self-assertive European approaches to the US defence market and for closer intra-European collaboration.[44]

While these consequences of the original post-September 2001 agenda are still working themselves out, there has been time for further and newer themes to emerge within the spectrum of security issues concerning both business and government. The one flowing most directly from new analyses of the terrorist risk is the preoccupation with critical infrastructure protection (CIP)—the question of how to maintain energy delivery and distribution, telecommunications, and critical transport links within and between nations in the face of either terrorist sabotage or more natural and accidental risks. Heightened concern about this is logical, given the constantly increasing dependence of government itself (and official defence mechanisms) on computerized systems and long-range energy supply; the steady trend towards privatization and internationalization of all such supplies and services; the instant and massive disruption which a breakdown in any part of the system may cause to society (as shown by a string of electricity blackouts in the USA and Canada, the UK, Italy, and Denmark and Sweden in August–September 2003);[45] and the relative vulnerability of these networks to physical and more insidious attacks (*vide* computer viruses and hacking). Studies of this problem—supported by both governments and industry—are increasingly taking on an international character, and CIP is now firmly on the agenda of the EU, NATO and the NATO Partnership for Peace among others. It may be linked with, or seen as a specialized aspect of, civil emergency planning, which is undergoing a similar revival of interest after something of a lull since the end of the cold war.[46]

In actuality, the issues arising outside the terrorism–WMD complex which have had the greatest impact on business conditions in the two years since September 2001 have come from quite a different realm: that of human and animal health. The epidemic of foot-and-mouth disease in early 2001 caused the death of millions of animals in Europe, mainly through compulsory slaughter, and a protracted stoppage of the affected countries' meat trade. Concern about human immunodeficiency virus (HIV) infection and acquired immune deficiency syndrome (AIDS) peaked again in 2003 with the announcement of a new US policy initiative,[47] a UN report about the lack of funding for anti-AIDS work in Africa[48] and alarming new statistics on the advance of the disease[49]—all of which underlined that this has become a front-

[44] This issue is also discussed in Sköns and Baumann (note 42).

[45] See chapter 18 in this volume.

[46] See chapters 16 and 17 in this volume.

[47] 'The president's Emergency Plan for AIDS Relief', Fact sheet (White House, Office of the Press Secretary: Washington, DC, 28 Jan. 2003), available at URL <http://www.whitehouse.gov/news/releases/2003/01/20030129-1.html>.

[48] Joint United Nations Programme on HIV/AIDS (UNAIDS), *Accelerating Action against AIDS in Africa* (UNAIDS: Geneva, 21 Sep. 2003), available at URL <http://www.unaids.org/html/pub/UNAdocs/ICASA_Report_2003_en_pdf.pdf>.

[49] UNAIDS and the World Health Organization (WHO) estimated that 34–46 million people were living with HIV/AIDS worldwide and that total deaths had reached 2.5–3.5 million by late 2003. Joint

rank *security* issue for many countries in Africa and elsewhere. It is an increasing challenge for business, too, as illustrated by a headline in *The Financial Times*—'Outsourcing the business of life and death'[50]—where the 'business' is procuring AIDS protection for workers in South African companies. Dwarfing these concerns in the short term, however, was the spring 2003 epidemic of human severe acute respiratory syndrome (SARS) in East Asia and Canada. The epidemic caused an estimated $9 billion in economic losses in North-East Asia and a further $1 billion in South-East Asia, through factory shutdowns, slumps in travel and tourism, and the cost of countermeasures.[51] While security experts have sought lessons in the episode for the nature of and best responses to possible deliberate BW attacks,[52] it is more to the point to note that SARS itself has not been eliminated nor foolproof techniques agreed upon for preventing or controlling any future outbreak. Meanwhile, in an instance where human action (albeit with non-hostile intent) has developed into a security scare of comparable scale and economic impact, the USA continues to argue both with developing-world aid recipients and with European customers about the safety of its food exports produced from genetically modified crops. This last issue is a reminder that, even with the best of intentions, developments in commercial science and technology may not only be a source of solutions for new security challenges, but can also produce phenomena which are at least perceived by the general public as threats in themselves.

Last but not least, the crisis of confidence faced by several Western governments over the credibility of the information underpinning their security-policy decisions and—in some cases—also about the ethical quality of their tactics has found an echo in the continuing heart-searching over the quality of 'governance' in the private economic sector.[53] Without overstretching the

United Nations Programme on HIV/AIDS (UNAIDS), *AIDS Epidemic Update, December 2003,* UNAIDS/03.39E (UNAIDS: Geneva, Dec. 2003), available at URL <http://www.unaids.org/EN/resources/publications/corporate+publications/aids+epidemic+update+-+december+2003.asp>.

[50] Reed, J., 'Outsourcing the business of life and death', *Financial Times,* 18 Sep. 2003, p. 10.

[51] Asian Development Bank (ADB), 'Assessing the impact and cost of SARS in developing Asia', *Asian Development Outlook 2003 Update* (ADB: Manila, Oct. 2003), pp. 75–92, available at URL <http://www.adb.org/Documents/Books/ADO/2003/Update/sars.pdf>. The Canadian Tourism Research Institute of the Conference Board of Canada suggested that up to that date Canada had similarly lost some C$1.5 billion, equivalent to 0.15% of Canada's annual real gross domestic product. Darby, P., 'The economic impact of SARS', Special Briefing, May 2003, URL <http://www.dfait-maeci.gc.ca/mexicocity/economic/may/sarsbriefMay03.pdf>. As for air travel, in May 2003 SARS brought a 21% drop in flight bookings over the previous year, and bookings did not start to rise again above the 2002 level until Sep. 2003. International Air Transport Association figures, quoted in 'Passengers return to international flights', *Financial Times*, 4 Nov. 2003, p. 8.

[52] Prescott, E. M., 'SARS: a warning', *Survival*, vol. 45, no. 3 (2003), pp. 207–26.

[53] The aspects of this which are already being tackled most systematically at the international level are the financial operations associated with organized crime and the problem of corruption. The United Nations Convention Against Transnational Organized Crime, adopted by the UN General Assembly and opened for signature in Dec. 2000—covering i.a. money laundering and human trafficking—entered into force on 29 Sep. 2003, albeit without the adherence of the USA or of most EU member states. For the text of the convention see URL <http://www.unodc.org/unodc/en/crime_cicp_convention.html>. On 1 Oct. 2003, negotiations were completed on the United Nations Convention Against Corruption, opened for signature at Mérida, Mexico, on 9–11 Dec. 2003. See the Internet site of the United Nations Office

parallel, it may be noted that such recent business scandals as those involving the Enron Corporation and WorldCom Incorporated in the USA, and Vivendi Universal and others in Europe, have also involved issues about the quality of information made available to the public and about conspiratorial behaviour leading to the subversion of normal control mechanisms.[54] In both contexts, leaders have been blamed for building high-risk patterns of behaviour on shaky or non-existent foundations of fact. The sternness with which the US Administration, in particular, has striven to punish and control Enron-type excesses has in turn become a new source of transatlantic tension: European companies and governments have raised concerns about the extraterritorial application of new US boardroom disciplines to their own US-linked or US-registered operations.

For all this multiple evidence of the interplay and interdependence of public- and private-sector security concerns, it cannot be said that 2002 and 2003 have witnessed any breakthrough in the way in which these two constituencies talk and work together. To take the example of terrorism, the irritation felt by many businesses over the impact of perhaps insufficiently thought-through countermeasures on their operations has been compounded by frustration that government seems uninterested in benefiting from their expertise, notably in risk assessment and management, or the huge amount of information on international processes and individuals that they gather in their own operations.[55] (Of course, any new system which might be developed for exploiting such expertise would run into delicate problems of data privacy and 'end-use', just as has happened in the case of disclosures relevant to money laundering and to travel safety.) On the other hand, the insurance industry is still calling for more serious governmental attention to be given to the problem of its vulnerability should even one further terrorist incident with large loss of life occur in the near future.[56]

Part of the problem is the continuing lack of any single clear institutional framework or process where the two sectors could review the whole security agenda together. The problem is far from being one of a total vacuum. Numerous initiatives have been taken, especially since the 1990s, to set up: (*a*) groupings or networks of business people to address security issues in individual countries; (*b*) international private-sector initiatives in association with the United Nations, such as the Global Compact;[57] (*c*) consultation mechanisms between governments and their national business communities on

on Drugs and Crime (UNODC) at URL <http://www.unodc.org/unodc/en/crime_convention_corruption.html>.

[54] On Enron see URL <http://www.enron.com>, on WorldCom (now MCI) URL <http://www.mci.com>, and on Vivendi URL <http://www.vivendiuniversal.com>.

[55] In Aug. 2003 the US Defense Advanced Projects Research Agency (DARPA) had to abandon, amid widespread derision, a planned scheme for a 'terrorism futures' market where companies' inside information could be reflected in collective 'betting' on likely future attacks. As pointed out at the time, however, the premise of harvesting companies' know-how was far less foolish than the particular method proposed. Harford, T., 'All bets are off at the Pentagon', *Financial Times,* 2 Sep. 2003, p. 8.

[56] See chapter 19 in this volume.

[57] See note 11.

specific issues of policy framing and implementation;[58] and (*d*) some corresponding international mechanisms, between a specific intergovernmental community or agency and private sector representatives from the countries involved. The difficulty is that all these approaches—except (*d*) in a very few cases—are voluntary, not formalized, and have thus resulted in an extremely varied (and not necessarily well-prioritized) pattern of coverage.

Very broadly speaking, business has tended to organize itself most systematically in the field of conflict prevention/management/reconstruction and 'conflict commodities';[59] to some extent on issues of critical infrastructure protection; vis-à-vis the security issues related to 'globalization', such as the environment; and for national coordination purposes in countries with a high consciousness of threat (and/or of international security responsibility).[60] Governments have most often sought dialogue with business on matters where their dependence on the private sector for policy execution is most obvious: export control and technology transfer issues,[61] infrastructure protection, national emergency planning in general, and of course their own requirements for private-sector services in the defence operational as well as equipment field. The control of WMD-relevant and other strategically sensitive exports is an area of rather well-developed consultation mechanisms and it needs to be, given the complexity of the balances that need to be struck and the need for constant adaptation to new possibilities of both equipment and technology 'leakage'.[62] The fact remains that there is no truly comprehensive process allowing *all* relevant businesses to consult regularly with *all* relevant governments on the spectrum of currently urgent issues, even within the narrower

[58] As an example, the US National Strategy for Homeland Security of 2002 calls for government to work with business on developing protection strategies for 14 critical sectors. See URL <http://www.whitehouse.gov/homeland/book/>.

[59] For a definition of these commodities and discussion of policy options see Pauwels, N., *Conflict Commodities: Addressing the Role of Natural Resources in Conflict*, ISIS Briefing Paper no. 27 (International Security Information Service, ISIS Europe: Brussels, Mar. 2003), URL <http://www.isis-europe.org/isiseu/brieflist/No.27_Conflict_Commodities.pdf>.

[60] *Vide* the Business Executives for National Security (BENS) network in the USA; see URL <http://www.bens.org>.

[61] See chapter 6 in this volume.

[62] Concerns about dangerous transfers have to be matched in this field against legitimate commercial and technology-development objectives, especially given that many of the commodities in question are of dual (military and civilian) use. The increasing interest in controlling intangible 'knowledge assets' relevant to proliferation, as well as hardware and software, will pose quandaries given the international character of many modern private-sector research teams. The way ahead may lie in more targeted controls, focusing on blocking leakage to the most dangerous destinations (state and non-state) rather than using generic export and transfer bans. As regards consultation mechanisms, in 1991 the USA established the Business Executive Enforcement Team (BEET) in the form of a secure electronic network linking over 3000 individuals in dual-use exporting firms with the Office of Export Enforcement in the Bureau of Industry and Security of the US Department of Commerce. See URL <http://www.bxa.doc.gov/enforcement/beets.htm>. The network is used both to inform business people of, and to let them pass comment on, official concerns and developments. In an alternative model, in 1994 the Swedish Chamber of Commerce established the Swedish Export Control Society (ECS; in Swedish, Sveriges Exportkontrollförening) to inform companies' export licensing specialists of developments in Swedish, EU and US policies and to coordinate the expression of these constituents' views back to the government. See URL <http://www.chamber.se/exportcontrol> (in Swedish). The ECS holds an annual meeting with all its members, can summon ad hoc meetings, issues a newsletter and operates otherwise through a secure electronic network.

sphere of military security—let alone the whole variety of security challenges reviewed above.

To some extent the gap is filled—and the worst kind of policy incoherence avoided—by discussions and personal networking between public and private sector leaders in wholly unofficial contexts such as the annual meetings of the World Economic Forum, which apart from anything else have a valuable educational effect (allowing each side at least to hear what the other is thinking and doing).[63] Any attempts to improve intra-sectoral dialogue would need to take the benefits of such non-constrained intercourse into account, and perhaps start from the premise that 'good' and 'comprehensive' in this context does not necessarily equate to 'formal' or 'obligatory'. The expressions of need voiced from the business side are strikingly often couched in terms of *information* and *early warning*—in essence: 'tell us what you're planning in good time and we might be able to help you with it more than you think, as well as adjusting better to the consequences for ourselves'. Voluntary information exchange and consultation mechanisms could meet quite a lot of these requirements, while leaving flexibility for subsequent operational cooperation to take the form most appropriate for the case in hand.

There are, in fact, at least two pitfalls to be avoided in any more formal attempt at reinforced dialogue and collaboration. Across the field as a whole, at both the national and international level, the latest evolution of the security agenda offers a clear temptation to 're-nationalize' (or the equivalent): that is, to resume executive and/or juridical control of functions essential for security which have passed into private-sector hands in the course of free-market developments (or perhaps have always lain there). The lesson cited above of the Warsaw Pact command economies should signal some of the dangers along this path. The more recent evidence of hastily conceived security measures damaging the 'good' economy more than the 'bad guys' underlines the danger even of indirect regulatory approaches when they are divorced from economic reality. This is not to say that everything can and should be left to voluntary actions from the private-sector side. Many of the issues at stake are ones where consistent universal coverage and a 'level playing field' are the very essence of an appropriate security solution. The free play of voluntarism and market forces not only cannot guarantee these requisites but also may lead to distortions (e.g., solutions disproportionately favouring the larger northern hemisphere companies which take most of the initiatives, or *excessive* philanthropy leading to clientage and aid dependence) which in the long run make things worse. This leads on to the second consideration: the all-too-real risk—illustrated by the airline insurance issue—that actions apparently constituting rational steps in mutual support between government and business may have (intended or accidental) anti-competitive effects, damaging both to the overall health of the economy and the environment for international cooperation. At

[63] On the World Economic Forum see URL <http://www.weforum.org>.

present, the world's strongest defence and security institutions are not those most sensitive to such risks or best seasoned in avoiding them.

All this suggests that it will be very important, when building any more systematic new framework for public/private interaction on the new agenda, (*a*) to maintain a bias towards the 'lightest' possible means of control for solving any given problem (e.g., regulation rather than executive action, contracting rather than requisitioning), and (*b*) to use or at least involve international forums whose primary competence lies in the economic sphere. The roles played by the World Bank, the World Trade Organization, the Organisation for Economic Co-operation and Development (OECD), and relevant parts of the UN machinery have been entirely appropriate from this point of view. The time could now be ripe for more activism in this field by the EU (and through EU–US dialogue), as well as in the framework of the Group of Eight (G8) major industrialized nations.

IV. Other players, other interests

With all the complexities that increased public/private sector interaction on the new security agenda may imply, it is still too simplistic a model because there is—in reality—a very important third side to the triangle. The *individual citizen* enters into the equation as well, and in a number of guises. First and foremost, he or she may be thought of as the actual and potential *victim* of every kind of security malfunction so far mentioned: the target for terrorism and crime as well as armed warfare, the sufferer from collapse of services or disease or a disintegrating environment. His or her degree of objective vulnerability, in prosperous as well as developing societies, is arguably greater than ever in history before because his/her simplest needs (food, warmth, movement) depend on the operation of complex technical systems far beyond the individual's ability to control—or in many cases, even understand. It is not unreasonable that citizens should look increasingly to their governments to ensure, nationally or collectively, that these support systems of modern society are protected as a high priority and that 'normal service is restored' as fast as possible after any breakdown. As soon as things go wrong, as they did in the spate of urban power breakdowns in the autumn of 2003, it becomes clear that these expectations are among the strongest ones invested by the ordinary people of many nations in their ruling structures and in the international groupings they belong to. For different reasons in different parts of the world, as noted above, citizens are also increasingly aware of the impact of the private sector's activities on many of these issues and are prepared to use their own purchasing strength and consumer choice to signify their judgement on its performance.

When governments and/or companies make less than optimal choices in pursuit of their 'duty to protect', however, citizens can be hurt in other ways than through simple lack of protection. They will ultimately receive the bill for

any material measures taken, whether by the state (through paying taxes) or by the private sector (through higher prices). Their political and human rights, access to information and education, freedom of economic activity and freedom to travel could be hit by many different types of 'corrective' measures tending to tighten central controls and disciplines. The atmosphere and efficiency of the multi-ethnic, multi-sectarian societies in which an increasing proportion of the world's citizens live will be damaged if the effect of security measures is to stigmatize and discriminate between elements with different ethnic and religious backgrounds. A safe society does demand individual alertness, but it may tip into paranoia and probably become more prone to violence if the culture of 'snooping' and denunciation of fellow citizens gets out of hand. The economic conditions for ordinary people's activity may be skewed in more subtle ways if government and industry organize their collaboration in the style of a mutually beneficial 'cartel' while leaving the impact on individuals out of account. All this is just one dimension of a much more general and permanent quandary for security policy (referred to in section I): the risk of crushing by inappropriate protection the very assets and values that the policy sets out to protect.

The citizen is not only the object of security solutions, but may also be a *part of the problem*. Individuals cause or aggravate emergencies through initial error and negligence (including neglect of preventative measures), failure to respond appropriately to the strings of abnormal events which lie behind so many large emergencies, failure to follow security instructions after the alarm is given, and so forth. It is striking to note how many security experts in the business world identify their own employees, in this sense, as their primary security risk.[64] Moreover, in a free-market environment where much security equipment and advice is for sale at a price, individuals can make the rational handling of emergencies more difficult by inappropriate preparation (e.g., purchasing the wrong equipment, panic buying and hoarding) as well as by inappropriate responses. It is very difficult to blame people for this given the general lack of control and understanding of complex new security processes, which makes it often virtually impossible for them to work out independently what would be the 'right' thing to do in the face of a given threat or emergency. The key point which emerges is that many solutions for countering the new-style threats to society will lie as much in the *behavioural* field—requiring change in the role of citizens themselves—as in the regulatory sphere proper to government, or the technical sphere where business is supreme.

The right approach to developing such multi-faceted answers cannot be to marginalize and disenfranchise the ordinary person even further. Ignorance, passivity, and the 'dumbing down' of security judgement in individuals can only lessen the resources available both to the state and business for their mutual support, and reduce the resilience and adaptability of society as a whole. Rather, the emphasis should be on finding ways to increase the general

[64] See chapter 15 in this volume.

public level of understanding, confidence, preparedness, self-reliance (within reason), and—not least—the consciousness of responsibility to help even weaker and more vulnerable members of the community. It should go without saying that simply lecturing people on the nature and seriousness of the challenges is not enough, and can merely make things worse when it amounts to frightening them without offering clear remedy. Panic is a deliberate weapon of all kinds of 'bad guys', and is the enemy of good security policy both short- and long-term.[65] Conversely, it is a bad mistake for government to belittle and simplify actual threats or to claim that it can provide a simple executive solution, when this is not only untrue but liable to be exposed as such sooner rather than later. The question of how to build more genuine and lasting forms of partnership between government, business and the citizen—whether through education, information, consultations, media actions,[66] exercises, new forms of citizen's service,[67] and/or the mobilization of civil society's own groups and structures—would provide material for another major publication in itself.

Practically all the analysis in this chapter suffers another major limitation in that it reflects an essentially Western-inspired and West-centric agenda, leaving the interests of *other regions of the world* out of account. It is important here not to fall into simplistic assumptions about opposing 'Northern' and 'Southern' agendas. The threats of terrorism, proliferation and rogue-state behaviour hurt even more people and often hurt them more directly in the developing countries than they have done (at least so far) in the world's richer societies. Globalization has made the security challenges for different regions more comparable overall and has increased inter-regional dependence in a way that should banish any 'zero-sum' notion of Northern and Southern security. All players' interests are best served by freedom to trade and communicate in peaceful, predictable surroundings, so all have a prima facie interest in working together to eliminate the various saboteurs and parasites of the global security system. These are not only idealistic statements but may be shown to have some reflection in reality, if one considers (for instance) the role of oil-producing countries in bringing the world through the period after September

[65] Zanders (note 15).

[66] Since the massacres in Rwanda and the conflicts of the 1990s in South-Eastern Europe in particular, awareness has grown that the media have a dynamic effect not just in reporting conflicts to the outside world but in influencing opinion and action within the conflict area. There is a growing consensus that the international community's task in such cases should include providing its own sources of unbiased (especially radio) broadcasting, and if possible, suppressing any local media which by projecting a 'hate' message de facto become parties to the conflict. During the 2003 conflict in Iraq, major innovations were made in techniques of outwards-directed reporting ('embedded' journalists, etc.), but the actual and potential *local* role of democratic media is an aspect that has hitherto been somewhat under-discussed.

[67] Since the end of the cold war the clear trend among countries in the wider European area has been to move away from national defence systems based on conscription towards the greater use of professional forces, often linked with changes in the role of reservists. Even in countries still making extensive use of conscription (e.g., states in Northern Europe), the proportion of young men in each generation called up for service is dropping because of overall force cuts. In countries which are reluctant to lose the notion of citizens' service altogether (e.g., because of its perceived bonding and democratizing effect), one solution would be to devise new forms of non-military service devoted to internal and functional security needs, as well as to social and humanitarian ones.

2001 without a major price shock, or the very wide range of countries who have cooperated with the UN Counter-Terrorism Committee.

Nevertheless, there are both in theory and actuality several ways in which the pursuit of Western public–private sector security agendas since 11 September 2001 could create difficulties vis-à-vis other world regions, generally with greatest cost to the interests of the latter. The first problem is that Western analysts may not consider carefully enough the need for extending their corrective policies to other regions, and/or may underestimate the help the latter could provide. Several regional organizations outside Europe have in fact discussed their own anti-terrorism, anti-proliferation measures since September 2001,[68] but these developments have tended to be underreported and the EU, for example, still needs to do much more to achieve practical synergy with such groups (inspired as they often are by the EU's own model). The critical infrastructure and energy supply issue is one for which, patently, solutions will only be as good as the weakest link in the chain. Attention should be given as a priority to the standards of protection in both neighbouring and more distant supplier countries. Again, the new understanding of the terrorism/proliferation nexus and the importance of emerging security dimensions such as infrastructure, migration control or disease control will need to be factored far more carefully than they are at present into developed-world policies for crisis prevention, management and post-crisis reconstruction in other parts of the globe. Events in Iraq up to the present have provided an almost perfect negative model of what happens when these aspects are not properly understood or planned for at the time of intervention and when the right capacities are lacking for addressing them afterwards.

Iraq also illustrates the next set of problems: those which arise when the remedies chosen by the West for its own perceived security problems are based on mistaken or inadequate theories about the rest of the world's role in creating them; or when methods are used which are counterproductive when applied in the real extra-European environment; or when there is a tendency more generally to discriminate against non-Westerners both in practice and in terms of perception. The biggest debate that has already taken place under this heading is the familiar one about the need to tackle the causes of terrorism, not just its manifestations. The wrong kind of forceful action against the latter, and the use of wrong methods to coerce or buy developing countries' support, may

[68] E.g., the members of the Asia–Pacific Economic Cooperation (APEC) forum agreed in Oct. 2003 on a number of joint measures to tackle aspects of the 'new security agenda' such as the dismantling of terrorist organizations, imposition of controls on shoulder-launched anti-aircraft missiles, enhancement of security at seaports, cutting off of terrorist finance, and measures against WMD proliferation. See 'Bangkok Declaration on Partnership for the Future', 21 Oct. 2003, URL <http://www.apecsec.org.sg/content/apec/leaders_declarations/2003.html>. Similar measures had previously been discussed by the Association of South-East Asian Nations (ASEAN) (see 'ASEAN efforts to counter terrorism', URL <http://www.aseansec.org/14396.htm>) and the African Union (see 'Decision on terrorism in Africa', Assembly/AU/Dec.15(II) 2003, URL <http://www.africa-union.org/Official_documents/Decisions_Declarations/Assembly%20AU%20Dec%2015%20II.pdf>). These issues were also raised at the Special Conference on Security of the Organization of American States (OAS), meeting at Mexico City on 27–28 Oct. 2003. See OAS, 'Declaration on security in the Americas', URL <http://www.oas.org/csh/ces/en>.

carry a wide range of costs. They may create new enemies for the West (and new terrorists, criminals, mercenaries, arms traffickers, etc.); worsen regional divisions and antagonisms; create new local arms races and actual incentives to proliferate WMD (if the proven possession of WMD is perceived as a defence against superpower attack); and blur the messages which the West wishes to project about the need for reform, democracy and legality worldwide.[69] They may also cause concrete damage to the security and stability of individual non-European states. The element of discrimination or differential damage to the interests of developing countries may arise from new security-related obstacles to travel and trade, the creation of new operating costs which only more prosperous operators can bear, the disproportionate burden placed by new international norms on smaller states,[70] and so on. On top of all this comes the risk that non-Westerners in general and their religions and political–social–economic practices will be stamped in general terms as 'the enemy' or at least become a source of mistrust and apprehension. It should go without saying that the interests of Western business and the conditions for its mutually beneficial operation in non-Western areas can only suffer from the compound effect of all such mistakes, even if—inevitably—some niches are created in the process for wrongful and disproportionate gains.

The third type of problem arises when Western-led policies leave out of account the other important challenges affecting the rest of the world, both in the traditional security sphere and more widely, or exalt the currently fashionable 'rich man's agenda' over these other issues to an unjustified extent. The whole point about 'asymmetrical' threats is that they buck the trend: most security processes in the world still favour the stronger over the weaker players and the richer over the poorer. As the UN Secretary-General pointed out in his report in 2003 on progress under the UN's Millennium Declaration,[71] the bulk of mankind is still struggling with security challenges as basic as finding food, water and fuel, keeping their children alive, and avoiding death at the hands of fellow citizens or abusive rulers. Climate change is yet another factor which will hit the developing world harder than the developed: a recent World Health Organization (WHO) report suggests that the bulk of the 300 000 projected deaths per annum from climate-related disease and natural disasters in 2030 will affect the poorest countries.[72] The majority of armed conflicts are

[69] The United Nations Development Programme argued that US and other Western policies since 11 Sep. 2001 had made it easier for less-than-democratic regimes in the Arab world to restrict citizens' freedoms further and to resist reform, as well as hampering human contacts between these countries and the West itself. See United Nations Development Programme (UNDP), *Arab Human Development Report 2003: Building a Knowledge Society* (UNDP: New York, Oct. 2003), summary available at URL <http://www.undp.org/rbas/ahdr/englishpresskit2003.html>.

[70] Leahy, J., 'South Pacific islands hit by wave of regulation after terrorist attacks', *Financial Times,* 8 Jan. 2003, p. 3.

[71] United Nations, Implementation of the United Nations Millennium Declaration: Report of the Secretary-General, UN document A/58/323, 2 Sep. 2003, available at URL <http://www.un.org/millenniumgoals/>.

[72] McMichael, A. J. *et al.*, World Health Organization (WHO), *Climate Change and Human Health: Risks and Responses* (WHO: Geneva, 2003); for a summary of the report see URL <http://www.who.int/globalchange/publications/cchhsummary/en>.

internal to developing states and have only limited connections to terrorism, let alone any inherent anti-Western agenda.[73] If new-style Western security policies neglect and shift resources away from such issues, the West's own security is bound to suffer—and probably first of all, through the effects of such regional disorder and decay on interdependent economic processes including raw material supply and migration flows. When issues like the threat to the global environment or the new trends in epidemic disease are considered, the interlocking of 'rich men's' and 'poor men's' security destiny is all the plainer

It is probably safe to guess that major companies and private-sector groupings are less likely than governments to let themselves be distracted from this last agenda, just as they are less likely to get the 'asymmetrical threats' out of proportion. Their jet-setting executives and expatriate operators are among the most genuine 'citizens of the world', more so than many national officials and certainly more so than national politicians. One of the benefits of a closer and more comprehensive public–private sector dialogue on security priorities and remedies would be to enlist these broader business perspectives and to hear business's (often very perceptive) view on the dynamics and needs of other regions. It could not, however, offer a complete remedy for the risks of West-centricity until and unless some way can be found to draw in the representatives of the private sector from all non-Western regions as well.

V. This book

This book is based on the proceedings of the international conference on Business and Security: Protecting the Legitimate and Blocking the Illegitimate, which was held at Vaduz, Liechtenstein, on 5–6 September 2003 by SIPRI and the Liechtenstein-Institut in the framework of the Liechtenstein Government's programme on peace research and conflict prevention. The chapters which follow consist, by and large, of more developed versions of the talks which were delivered at that conference, taking into account also the points made in subsequent discussion. They are grouped in thematic parts, each with a further short introduction by the editors of this volume.

The aim of the SIPRI–Liechtenstein-Institut Conference, aside from the interest of the subject matter, was to bring together an unprecedented mix of private-sector leaders, researchers, NGOs and other independent activists, and public-sector representatives from governments, parliaments and international institutions. UN agencies, NATO, the EU, the OECD, and the Organization for Security and Co-operation in Europe (OSCE) were all represented. The agenda was drawn up with a view to illustrating the broad span of issues relevant to the private–public sector security dialogue and cooperation since

[73] Wiharta, S. and Anthony, I., 'Major armed conflicts', pp. 87–108, and Eriksson, M., Sollenberg, M. and Wallensteen, P., 'Patterns of major armed conflicts 1990–2002', pp. 109–21, *SIPRI Yearbook 2003* (note 2).

11 September 2001, and to examining these challenges from a variety of angles—including the cogent questions of 'Can we afford to be safe?' and 'Is this just a rich man's agenda?'.

The mix of perspectives achieved at the conference is also reflected in this book, in the different styles as well as the substance of the chapters. Individual contributions are not necessarily 'balanced', although their ensemble is designed to be so. It should thus be emphasized that, as always in such cases, the views expressed by the various authors are their own and should not be taken to reflect the views either of SIPRI or of the Liechtenstein Government.

Given the limited time available for the conference at Vaduz, some issues of considerable importance for both government and business had to be left to one side. This volume is, correspondingly, far from being able to offer truly comprehensive coverage. An obvious omission is any discussion of the defence industrial sector itself. At the functional level, much more could have been said, for example, on the corporate ethics agenda (including the security relevance of corruption); the theme of aviation security; the reliability of energy sources (as distinct from energy distribution); and the issue of security of supply in general. It is possible that some of these matters may be addressed in the course of further activities under the Liechtenstein Government's programme.

The book does, however, aim to fulfil a wider function of reference and to provide a platform for further research and activism through its appendices, prepared by Isabel Frommelt. They gather together information not hitherto available in a single place on security institutions (official, academic or non-governmental) and business organizations, respectively, that are active in or interested in the public–private sector interface in this field. These listings, too, inevitably reflect the limits of SIPRI's own knowledge and access to information. If readers are aware of any omissions under the defined categories, and can supply the appropriate references, they are invited to draw them to the editors' attention.[74]

[74] Email address: director@sipri.org.