11. Reducing security risks by controlling possession and use of civil materials

IAN ANTHONY

I. Introduction

In recent years the need to complement the traditional framework for arms control with other measures in order to adapt it to new security challenges has increasingly been recognized. In a number of cases initiatives have been taken to supplement the multi- and bilateral agreements that have traditionally been perceived as the core of arms control efforts.

The existing arms control agreements were designed to help manage the risk of attacks being mounted by the armed forces of states. As part of the effort to address that problem, bi- and multilateral arms control agreements referred to state behaviour when defining what would be subject to control. In a number of cases these agreements went further by identifying parts of the military establishment of states when defining the scope of controls and by developing detailed lists of objects to which restraint measures or reductions would apply.

Since the 11 September 2001 terrorist attacks on the United States there has been a much greater focus on how to block access to weapons by non-state actors and in particular by groups planning acts of mass-impact terrorism.[1] The effort to supplement the arms control framework to take into account the risks that non-state actors present has been stimulated by assessments that emphasize the potential threat that is posed by the possibility that such groups could succeed in acquiring weapons. In a 2006 speech the Director General of the United Kingdom's Security Service speculated that 'today we see the use of home-made improvised explosive devices; tomorrow's threat may include the use of chemicals, bacteriological agents, radioactive materials and even nuclear technology'.[2]

Efforts are needed to augment arms control with new measures tailored to current conditions. However, a number of observers have pointed out that in future, given the changing nature of the threats perceived in a number of countries and regions, it will be necessary to look even wider to identify the full range of threat-reduction tools that will be required. Soon after the 11 September attacks Jayantha Dhanapala, then the Undersecretary-General for Disarmament Affairs at the United Nations, noted that there are extremist groups in all regions that are prepared to use 'unthinkable methods to bring about the crash

[1] See appendix 11A.

[2] Manningham-Buller, E., 'The international terrorist threat to the UK', Speech at Queen Mary's College, London, 9 Nov. 2006, URL <http://www.mi5.gov.uk/output/Page568.html>.

of civilization in its entirety' and pointed to the need for a multidimensional response, including 'diverse, synergistic contributions'.[3] The focus on new, non-state groups is one key element of this multidimensional response. Another is the attempt to develop new and advanced international standards to manage and control a range of potentially dangerous materials that go beyond the lists of items traditionally associated with nuclear, biological and chemical weapons.

Section II of this chapter identifies and briefly describes some of the recent initiatives to develop security-related standards for materials not normally thought of as weapons. Section III briefly examines how the European Union (EU) has approached this issue in a region where civil goods move freely within a single market. The development of this approach is particularly complicated in Europe because in the areas discussed in this chapter it can be argued that control measures cut horizontally across the three 'pillars' on which the EU organizes its activities.[4]

Section IV examines efforts to engage with the private sector of industry as part of the overall security-building effort. A key part of this effort to develop and promote control standards is to enlist the support of a different group of non-state actors (in particular the private sector and the specialized research community) that are the custodians of many of the relevant materials, items and technologies. Engagement with these actors is at an early stage and will certainly be a complicated new challenge. The effort will probably include the incorporation of new standards in legislation and regulations that will make the non-governmental sector the target of security controls. However, it is also likely to include efforts to encourage that sector to develop voluntary standards and apply them, perhaps as part of the system of quality management.[5]

Some tentative conclusions are offered in the final section of the chapter. UN Security Council Resolution 1540 is discussed in appendix 11A, and the resolution is reproduced in appendix 11B.

II. Recent developments

Traditionally, arms control has mainly addressed the control of items that are specially designed, developed or adapted for military use, but there have been some efforts to deal with what are usually referred to as dual-use items. This term has been employed to classify items that were not specially designed, developed or adapted for military use but that could nevertheless be used by a state's armed forces in military programmes. One example of such an item is a chemical that has legitimate industrial applications but is also the direct precursor of a chemical weapon. Another example is a lathe that can be equipped

[3] Dhanapala, J., 'The impact of September 11 on multilateral arms control', *Arms Control Today*, Mar. 2002, URL <http://www.armscontrol.org/act/2002_03/dhanapalamarch02.asp>.

[4] On the 3 EU pillars see the glossary in this volume and section III below.

[5] According to the International Organization for Standardization (ISO) definition, total quality management consists of the coordinated activities to direct and control an organization with regard to quality, where quality is the degree to which a set of inherent characteristics fulfil stated requirements.

with numerical controls (software that determines the actions of the machine) and can work in more than two axes that can be coordinated simultaneously.

Such dual-use items are of interest to arms controllers because of their military potential. Interest in such items increased in the 1990s in the light of proof that some countries (notably, Iraq) had made the acquisition of dual-use items a central element of their arms procurement strategy. The dual-use issue remains an important part of the arms control discussion. However, this chapter focuses on items that are purely civil in their origin and technical specifications—but that could be put to harmful use—rather than on items that are dual-use in the sense that they have military applications.

A topical example can be used by way of illustration. Liquefied natural gas (LNG) is not a material of interest to any organized military force for battlefield use, nor can it be turned into a battlefield weapon.[6] However, if released, LNG will evaporate and the resulting vapour cloud can explode and burn when combined with air. In 2003 the US Government drew attention to the potential risk of a successful terrorist attack on the energy infrastructure of a country, including on LNG during storage or transport.[7] In future the quantity of LNG being produced and transported as well as the number and frequency of cargo movements are expected to rise significantly as this fuel plays an increasingly important part in energy strategy. Although in this case it was the USA that highlighted the issue, there is no Western monopoly of concern over security risks associated with LNG: the most important producers and exporters include several non-Western countries with a recent history of attacks that were carried out by non-state groups (including Algeria, Egypt, Indonesia, Nigeria, Qatar, Russia and the United Arab Emirates).[8]

The example of LNG illustrates another feature of the discussion about risks that emanate from the civil sector—the relationship between safety and security. In January 2004 an accident involving a train carrying LNG caused a major explosion and fire at the Sonatrach LNG facility at Skikda, Algeria.[9] Where there are inherent dangers associated with particular materials or processes there is a need to reduce the risk that lack of competence, negligence or the use of inappropriate or outdated equipment and methods will cause damaging accidents. The process of reducing this risk is normally referred to in different sectors as safety. Safety measures do not usually assume that individuals or groups with malicious intent are taking deliberate actions to cause damage.

[6] On additional security-related issues surrounding the use of LNG see chapter 6 in this volume.

[7] US Department of Homeland Security, 'The national strategy for the physical protection of critical infrastructure and key assets', Feb. 2003, URL <http://www.dhs.gov/xprevprot/publications/publication_0017.shtm>, p. 52.

[8] US Department of Energy, Energy Information Administration, 'The global liquefied natural gas market: status and outlook', Report no. DOE/EIA-0637, Dec. 2003, URL <http://www.eia.doe.gov/oiaf/analysispaper/global/>.

[9] Hightower, M. et al., Sandia National Laboratories, 'Guidance on risk analysis and safety implications of a large liquefied natural gas (LNG) spill over water', Sandia report SAND2004-6258, Dec. 2004, URL <http://www.fossil.energy.gov/programs/oilgas/storage/lng/sandia_lng_1204.pdf>, pp. 159–60.

In relation to bio-safety and bio-security, good safety practices create a sound platform for enhanced security. With bio-safety as a basis, additional measures that have been adapted to meet particular security threats can be identified and implemented so that bio-safety and bio-security measures are managed together. The World Health Organization (WHO) produced a laboratory bio-security guidance document in September 2006 in which bio-safety is defined as 'the containment principles, technologies and practices that are implemented to prevent the *unintentional* exposure to pathogens and toxins, or their accidental release'. Laboratory bio-security is defined as 'the protection, control and accountability for valuable biological materials . . . within laboratories, in order to prevent *their unauthorized access, loss, theft, misuse, diversion or intentional release*'.[10]

Other analyses have pointed to potential conflicts between security measures and safety measures in particular conditions. In the field of nuclear safety and security Igor Khripunov has taken note of the argument that 'Proponents of safety typically call for building increased redundancy into at-risk systems, while proponents of security point out that greater redundancy might . . . create a situation in which there are more components and equipment than can affordably be secured against malicious acts—making security costlier and more elusive than it already is.'[11] However, after analysing the relationship between safety and security Khripunov concludes that 'Notwithstanding the tension between the two concepts, the characteristics of a good security culture would likely result in improved safety, quality, and productivity within the organization, since closer attention to personnel performance tends to produce better results in every area.'[12]

The discussion of how to enhance security by controlling civil materials has taken place against the background of transnational interdependence, including in the economic sphere.[13] In this context a number of recent intergovernmental discussions have pointed to the fact that any major disruption in the global supply chain could have serious consequences for the sustainable growth and development of many economies. For example, at the 2006 Symposium on Total Supply Chain Security, organized under the auspices of the Asia–Pacific Economic Cooperation (APEC) group, delegates pointed to the need for an approach to supply-chain security based on 'greater consistency of

[10] World Health Organization (WHO), 'Biorisk management: laboratory biosecurity guidance', WHO document WHO/CDS/EPR/2006.6, Sep. 2006, URL <http://www.who.int/csr/resources/publications/biosafety/WHO_CDS_EPR_2006_6/en/> (emphasis added). Issues related to bio-security are addressed in greater detail in chapter 13 in this volume. See also Roffey, R. and Kuhlau, F., 'Enhancing bio-security: the need for a global strategy', *SIPRI Yearbook 2006: Armaments, Disarmament and International Security* (Oxford University Press: Oxford, 2006), pp. 732–48.

[11] Khripunov, I., 'Nuclear security: attitude check', *Bulletin of the Atomic Scientists*, vol. 61, no. 1 (Jan./Feb. 2005), pp. 58–64. The need to account for and secure nuclear material is discussed further in appendix 12C in this volume.

[12] Khripunov (note 11), p. 62.

[13] See also the Introduction and chapter 7 in this volume.

principles, guidelines and standards of security across and between the various nodes in the supply chain'.[14]

As a further example, in the maritime parts of the supply chain, the International Maritime Organization (IMO) has been trying to establish a comprehensive set of standards through a combination of legal and political agreements among states. The political momentum generated in the immediate aftermath of the terrorist attacks on the USA meant that by December 2002 'a comprehensive series of measures designed to prevent and suppress acts of terrorism against shipping and in port facilities had been developed'.[15]

These enhanced security standards were formalized in the Code of Conduct for International Ship and Port Facility Security (ISPS Code), which amended the 1974 International Convention for the Safety of Life at Sea (SOLAS Convention).[16] Under the ISPS Code the relevant authorities are required to draw up security plans for ports and other land facilities as well as for ships. The ship and port security plans, which must receive formal government approval, define security measures for a range of conditions. The authorities are required to appoint dedicated security officers to implement these plans on ships, in shipping companies and at ports.

The ISPS Code and the associated SOLAS amendments that were adopted in 2002 entered into force in 2004, and port authorities and operators, shipowners and operators as well as relevant national authorities now face the task of implementing them. This process of implementation depends for its success on cooperation from many actors in the private sector and the approach to engaging with the private sector is discussed further below. However, it is broadly true that the benefits of strengthened security can only be achieved if established standards are translated into practical measures that are applied by the relevant actors at relevant facilities. As an example of this synergy between standards and practical measures, the International Organization for Standardization (ISO) published a publicly available standard (PAS), ISO/PAS 20858, at the same time as the ISPS Code came into force to help

[14] Asia–Pacific Economic Cooperation (APEC), Symposium on Total Supply Chain Security, 'Factsheet on total supply chain security', Singapore, 6–7 July 2006, URL <http://app.mot.gov.sg/data/fs_06_07_03c.htm>. The APEC members are listed in the glossary in this volume.

[15] Mitropoulos, E. E., Secretary-General of the International Maritime Organization, 'Security of the international container supply chain: threats, challenges and solutions', Speech to the Ministry of Foreign Affairs, Berlin, 18 Jan. 2005, URL <http://www.imo.org/InfoResource/mainframe.asp?topic_id=1028&doc_id=4650 >.

[16] International Maritime Organization (IMO), 'IMO adopts comprehensive maritime security measures', Conference of Contracting Governments to the International Convention for the Safety of Life at Sea, 1974, 9–13 Dec. 2002. The International Convention for the Safety of Life at Sea opened for signature on 1 Nov. 1974 and entered into force on 25 May 1980. It is reproduced at URL <http://www.imo.org/Conventions/contents.asp?topic_id=257&doc_id=647>. On SOLAS see Ahlström, C., 'The Proliferation Security Initiative: international laws aspects of the Statement of Interdiction Principles', *SIPRI Yearbook 2005: Armaments, Disarmament and International Security* (Oxford University Press: Oxford, 2005), p. 764. The ISPS Code is available on the IMO website at URL <http://www.imo.org>.

with its implementation.[17] This coordinated response was possible because of the long-standing cooperation between the IMO and the ISO.

The recent efforts to strengthen nuclear security illustrate another approach to implementing agreed standards, namely the important role that a specialized agency—the International Atomic Energy Agency (IAEA)—can play in providing both a framework in which to agree standards and a technical resource to help states implement them. The fact that fissile materials are indispensable elements of a nuclear weapon has led to the development of elaborate security provisions to safeguard against the diversion of such material to military use. After analysing the potential utility of radiological (as opposed to nuclear) weapons, military forces concluded long ago that there was no operational reason for developing such weapons. However, a number of other nuclear activities contain potential safety and security risks, although they have no military component.

On 11 September 2001 the IAEA Board of Governors, which was meeting in Vienna, considered the question of whether additional measures were needed to improve the security of nuclear materials and other radioactive materials. The board had before it the report of an expert group that had previously discussed whether there was a need to revise the 1980 Convention on the Physical Protection of Nuclear Material (CPPNM) which was, at that time, the only international legally binding undertaking in the area of physical protection of nuclear material.[18] The CPPNM was developed in the 1970s, when the main concern of the drafters was to ensure the safe and secure transport of nuclear material given environmental concerns about the performance of the nuclear power industry and the growing activism of groups and individuals opposed to international nuclear shipments. However, the CPPNM did not address the security and protection of nuclear facilities, although the IAEA did develop technical documents and policy guidelines to address this issue.

In 2001 the draft report from a Group of Legal and Technical Experts (Group of Experts) convened by the IAEA Director General to prepare draft amendments to strengthen the CPPNM found that:

> although responsibility for establishing and operating a comprehensive physical protection system for nuclear materials and facilities within a State rests entirely with the Government of that State, the need for international co-operation becomes particularly evident in situations where the effectiveness of physical protection in one State depends on other States taking, as appropriate, adequate measures to deter or defeat

[17] International Organization for Standardization (ISO), 'ISO/PAS 20858:2004, Ships and marine technology: maritime port facility security assessments and security plan development', 7 July 2004, URL <http://www.iso.org/>.

[18] The Convention on the Physical Protection of Nuclear Material opened for signature on 3 Mar. 1980 and entered into force on 8 Feb. 1987. The text of the amended CPPNM is available at URL <http://www.iaea.org/NewsCenter/Features/PhysicalProtection/>. For a brief summary and a list of signatories and parties to the convention see annex A in this volume. See also Kile, S. N., 'Nuclear arms control and non-proliferation', *SIPRI Yearbook 2006* (note 10), pp. 636–37.

hostile actions against nuclear facilities and materials when such materials are transported across national frontiers.[19]

In March 2003 the Group of Experts adopted its final report setting out possible amendments to the CPPNM. Following discussion by IAEA member states amendments to strengthen the security provisions of the convention were adopted in July 2005 and the name of the convention was changed to the Convention on the Physical Protection of Nuclear Material and Nuclear Facilities. The amended convention obliges states parties to protect nuclear facilities and material in peaceful domestic use, storage and transport. The amended CPPNM establishes measures related to the prevention, detection and punishment of domestic offences linked to nuclear material. The revised convention also envisages expanded international cooperation in order to speed up the location and recovery of stolen or smuggled nuclear material and to reduce the impact of acts of sabotage.[20]

The amended CPPNM forms one part of a nuclear security framework that also includes published technical standards that can be used by operators on a voluntary basis and non-legally binding codes and guidelines that have been endorsed by states. The fact that certain sources of radioactivity need to be shielded because there may be harmful effects if they are exposed raises both a safety issue (because of evidence of shortfalls in the procedures for accounting for, storing and disposing of such sources) and a security issue (because such sources may be open to malicious use). As the IAEA has expressed this, 'the continuing incidents and accidents involving radiation sources and the new concern about the possible malicious use of radioactive sources indicate a clear need for a comprehensive set of standards and guidance documents to support States in their effort to ensure an adequate level of both safety and security of radioactive sources'.[21]

The Code of Conduct on the Safety and Security of Radioactive Sources was approved by the IAEA Board of Governors on 8 September 2003.[22] It contains safety and security standards as well as guidelines that indicate how to meet some of these standards. Any state may apply the standards contained

[19] International Atomic Energy Agency, 'Measures to improve the security of nuclear materials and other radioactive materials', IAEA document GC(45)/INF/14, 14 Sep. 2001, URL <http://www.iaea.org/About/Policy/GC/GC45/Documents/gc45inf-14.pdf>.

[20] At the conference to consider amending the CPPNM, 89 states agreed to a set of amendments that will enter into force when two-thirds of those 89 states deposit their ratification of the amended treaty. As of 18 Sep. 2006, 6 states (Austria, Bulgaria, Croatia, Libya, Seychelles and Turkmenistan) had ratified the amended CPPNM. For the text of the amendment see 'Nuclear security measures to protect against nuclear terrorism: amendment to the Convention on the Physical Protection of Nuclear Material', Report by the Director General to the Board of Governors General Conference, GOV/INF/2005/10-GC(49)/INF/6, Vienna, 6 Sep. 2005, URL <http://www.iaea.org/About/Policy/GC/GC49/Documents/gc49inf-6.pdf>. See also Kile (note 18), pp. 636–37.

[21] International Atomic Energy Agency, 'Developing guidance for the safety and security of radiation sources', URL <http://www-ns.iaea.org/tech-areas/radiation-safety/source.htm>.

[22] See International Atomic Energy Agency, 'Code of Conduct on the Safety and Security of Radioactive Sources, and supplementary guidance on the import and export of radioactive sources', URL <http://www-ns.iaea.org/tech-areas/radiation-safety/code-of-conduct.htm>.

in the Code of Conduct and its widespread use would promote consistent international approaches to radiation protection, safety and security.

In 2005 the International Convention for the Suppression of Acts of Nuclear Terrorism was adopted by the UN General Assembly and opened for signature. This convention identifies actions by individuals that are to be considered as criminal offences and requires states to develop the measures necessary to establish those offences under its national law and to make them 'punishable by appropriate penalties' that take into account their grave nature. The convention also requires states to ensure that the national authorities needed to investigate the offences exist and to ensure that they have the power and the resources needed to cooperate with one another in investigations and prosecutions.[23]

In addition to the development of the framework of laws, regulations and guidelines to promote nuclear safety and security, the IAEA has recruited a technical secretariat that is able to help (at the request of countries) with the development of national strategies or to advise on dealing with specific technical problems. As part of its work, the IAEA has also developed a number of action plans on different aspects of nuclear safety and security through which technical assistance financed by donors can be delivered.

III. The efforts of the European Union

The structure of the EU is often illustrated by three 'pillars'. The first pillar includes the single market—within which there should be free movement of people, goods, services and capital—and matters related to the environment and trade policy. In this pillar the institutions of the EU have the right to draw up legal instruments and introduce legislation. In the two other pillars the EU has agreed to strengthen cooperation between member states: in the second pillar external cooperation is coordinated within the scope of the Common Foreign and Security Policy; and in the third pillar cooperation on police matters and criminal law is organized in the areas of justice, liberty and security. In the third pillar the Council of the European Union can take framework decisions that harmonize national rules. The 1997 Treaty of Amsterdam

[23] The International Convention for the Suppression of Acts of Nuclear Terrorism is reproduced as an annex to United Nations, Measures to eliminate international terrorism: Report of the Ad Hoc Committee established by General Assembly Resolution 51/210 of 17 December 1996, UN General Assembly document A/59/766, 4 Apr. 2005. The convention was opened for signature on 14 Sep. 2005 and will enter into force 30 days after it is signed and ratified by at least 22 states. See also Kile (note 18), p. 637. The need to redouble efforts to prevent nuclear terrorism was underlined by the disclosure, in Feb. 2006, by Georgian authorities of the seizure of around 80 grams of uranium enriched to 89% in uranium-235. IAEA Staff Report, 'Georgian authorities report seized illicit nuclear material', 25 Jan. 2007, URL <http://www.iaea.org/NewsCenter/News/2007/georgia_material.html>. This material was seized from an alleged Russian citizen, who claimed that he could acquire additional quantities against payment. Georgian authorities were unable to verify this information because of alleged lack of cooperation by Russian authorities. Butler, D., 'Georgian sting seizes bomb grade uranium', ABC News online, 25 Jan. 2007, URL <http://abcnews.go.com/Politics/wireStory?id=2820902&page=1>.

strengthened the authority of the Court of Justice over matters belonging to this pillar.[24]

This structure means that the EU is necessarily deeply engaged in discussing measures that control the movement of civil goods because of the potential impact on the single market. The administrative structure of the EU and the various divisions of legal competence contain the risk that separate activities to address essentially the same common problem will be carried out in different EU pillars simultaneously. In a functional area that has both internal and external aspects and where the division of legal competence between the EU and its member states is unclear or where the areas of legal competence overlap, there may be separate proposals for internal action and external assistance from different parts of the EU as well as multiple member state initiatives. These various initiatives may or may not be coordinated with one another, and any given actor may simply be unaware of the actions being taken in a different part of the EU. In addition, the European Commission has drawn attention to the fact that in a changing international environment the internal and external policies of the EU are inextricably linked.[25] New policies for external action are now being debated in Europe, which could allow the EU to play a greater role in ensuring that vital transnational and trans-regional flows of goods and supplies are unimpeded by deliberate or accidental disruption. New instruments, such as the Stability Instrument, have been adopted to help finance activities that can help safeguard against such disruptions.[26] The external projection of internal policies is likely to become an important element of future EU external action in this functional area.

The EU is aware of the risk that a piecemeal approach might be adopted in a new and rapidly evolving security situation. In its ‘Hague Programme’ on freedom, security and justice the EU noted that ‘in the field of security, the coordination and coherence between the internal and the external dimension has been growing in importance and needs to continue to be vigorously pursued’.[27] In an effort to produce this coherence, in May 2005 the European Commission published its five-year Action Plan for Freedom, Justice and Security containing detailed proposals on, among other things, terrorism. One element of the anti-terrorism component of the Action Plan was the protection

[24] The Treaty of Amsterdam amending the Treaty on European Union, the Treaties Establishing the European Communities and Certain Related Acts was opened for signature on 2 Oct. 1997 and entered into force on 1 May 1999. It is available at URL <http://europa.eu.int/eur-lex/en/treaties/dat/amsterdam.html>.

[25] Commission of the European Communities, ‘Europe in the world: some practical proposals for greater coherence, effectiveness and visibility’, Communication from the Commission to the European Council of June 2006, COM(2006) 278 final, Brussels, 8 June 2006, p. 4, URL <http://www.ec.europa.eu/comm/external_relations/euw_com06_278_en.pdf>.

[26] ‘Regulation (EC) No. 1717/2006 of the European Parliament and of the Council of 15 November 2006 establishing an Instrument for Stability’, *Official Journal of the European Union*, L327 (24 Nov. 2006), pp. 1–11. On the Instrument for Stability see International Security Information Service (ISIS), Europe, ‘The Stability Instrument: defining the Commission’s role in crisis response’, ISIS Briefing, Brussels, 27 June 2005, available at URL <http://www.isis-europe.org/>.

[27] Council of the European Union, ‘The Hague Programme: strengthening freedom, security and justice in the European Union’, document 16054/04, Brussels, 13 Dec. 2004, URL <http://www.ec.europa.eu/justice_home/doc_centre/doc/hague_programme_en.pdf>.

of critical infrastructure, which was defined to include both transport (airports, sea ports, intermodal facilities where cargo or passengers can move between transport modes, railway and mass transit networks, and traffic control systems) and the production, storage and transport of dangerous goods (e.g. chemical, biological, radiological and nuclear materials).[28] To achieve its counterterrorism objectives in these areas the EU has engaged in a number of activities intended to produce the following outcomes: (*a*) ensure that the various actors have the proper skills and competences to perform essential security tasks; (*b*) make certain that items being stored or moved are screened and evaluated against security criteria; (*c*) increase the time available for screening items during transport by requiring advance notification of the contents of shipments; (*d*) guarantee the physical security of items in storage or in transit; and (*e*) inspect stored items or items in transit.

To bring about the necessary changes the EU has taken a mixed approach by combining regulations and directives in some areas with efforts to encourage or stimulate voluntary action in others. For example, the Commission has proposed measures to ensure greater security of explosives, detonators, bomb-making equipment and firearms aimed at improving the security of the storage and transport of explosives as well as at ensuring the traceability of industrial and chemical precursors. The proposed measures include legislation to bring elements from international agreements (such as the UN 2001 Protocol against the Illicit Manufacturing of and Trafficking in Firearms, their Parts and Components and Ammunition) into Community legislation as well as the elaboration of voluntary measures through a 'structured dialogue' with industry and other non-governmental bodies.[29] A somewhat similar approach is being adopted in regard to preventive and responsive measures such as bio-security, preparedness and response. [30]

Legal and administrative decisions have also been used on other occasions to translate emerging international standards into law and practice in a uniform way across the EU. For example, in April 2005 security amendments were made to the Customs Code contained in EC Regulation 648/2005, which establishes the legal basis for customs procedures in all EU member states. The elements introduced in the Customs Code were based on the 2005 Frame-

[28] Commission of the European Communities, 'Critical infrastructure protection in the fight against terrorism', Communication from the Commission to the Council and the European Parliament, COM(2004) 702 final, Brussels, 20 Oct. 2004.

[29] The Protocol against the Illicit Manufacturing of and Trafficking in Firearms, their Parts and Components and Ammunition, supplementing the United Nations Convention against Transnational Organized Crime was opened for signature on 31 May 2001 and entered into force on 3 July 2005, URL <http://www.unodc.org/pdf/crime/a_res_55/255e.pdf>. The approach and its elements are described in Commission of the European Communities, 'Communication from the Commission on measures to ensure greater security in explosives, detonators, bomb-making equipment and firearms', COM(2005) 329 final, Brussels, 18 July 2005, URL <http://www.eur-lex.europa.eu/LexUriServ/site/en/com/2005/com2005_0329en01.pdf>.

[30] The EU measures related to these activities are described in chapter 13 in this volume.

work of Standards to Secure and Facilitate Global Trade developed under the umbrella of the World Customs Organization (WCO).[31]

Voluntary standards, which are discussed further below, can support policy and regulatory initiatives of this kind. For example, technical standards are currently being developed for mechanical and electronic seals for freight containers. These standards will help manufacturers understand and incorporate security practices when making their products to ensure that the seals are suitable for securing freight containers for international commerce in the light of the anticipated future regulatory environment. The development of these standards is therefore being followed closely by the WCO, the EU and the United Nations Economic Commission for Europe.

Although the Hague Programme in effect set the objective of securing the entire supply chain for goods and services in the EU, the supply chain is not entirely contained within the boundaries of the European single market. The supply chain includes all of the actors associated with a particular transaction: the suppliers of unprocessed raw materials, all the intermediate actors engaged in processing and manufacturing, the service providers and the final customer. The supply chain links many companies, including those operating in the European single market.

The modifications to the Customs Code are part of an EU effort to promote integrated border management at the external perimeter of the single market. The new code creates the legal status of authorized economic operator (AEO), which enables companies to earn the right to use simplified customs procedures by putting in place and certifying internal procedures that enhance security in the supply chain. However, goods and services as well as people and capital move freely within the single market and are not subject to customs controls. These transactions can also pose a security risk.

In February 2006 the Commission Directorate-General for Energy and Transport (DG TREN) presented a proposal for a regulation on enhancing supply-chain security.[32] The draft regulation, which was discussed in advance with the officials who developed the modifications to the Customs Code, contains a voluntary scheme based on creating 'secure operators'. The characteristics of a secure operator are similar to those of an AEO in the customs area, and it is intended that a company which meets the minimum requirements to be an AEO will automatically qualify to be a secure operator. The secure-operator status is expected to be relevant mainly to specific groups such as coastal shippers, transport companies, freight forwarders, warehouse and storage operators, and inland terminal operators whose operations take place exclusively within the single market even if they work with goods that

[31] The changes to the Customs Code are described in Anthony, I. and Bauer, S., 'Transfer controls', *SIPRI Yearbook 2006* (note 10), pp. 775–97. Their implementation is discussed further in chapter 15 in this volume.

[32] Commission of the European Communities, Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions on enhancing supply chain security, COM(2006), 79, Brussels, 27 Feb. 2006, URL <http://www.ec.europa.eu/dgs/energy_transport/security/intermodal/doc/com_2006_0079_en.pdf>.

originate elsewhere or are later designated for export. The expectation is that the market will reward the secure operators by giving them certain advantages. It might be expected, for example, that companies elsewhere in the supply chain that are AEOs or secure operators would prefer to work with partners that hold the same or similar status, because this could strengthen their own security measures. It is also possible that there might be benefits in reduced insurance premiums for secure operators.

The European Commission has proposed that EU member states set up secure-operator schemes covering all types of packaging and all transport modes. It has proposed that these schemes be made compatible with the systems that are already being set up to designate AEOs for customs purposes. The Commission has also proposed that there should be mutual recognition between the AEO and secure-operator certification processes.[33]

The development of greater supply-chain security is inevitably a long-term process. The initiative is primarily aimed at actors in the supply chain that could be potential targets for mass-impact terrorism attacks, which narrows the scope of application somewhat. Nevertheless, the Commission estimates that this might include almost 1 million operators across the EU. Moreover, these are companies that work with purely civil items and whose personnel are familiar with the need for safety measures but generally have a low level of security awareness.

Not surprisingly, the initial reaction of industry to this proposal by the European Commission was somewhat negative, although the Commission had tried to anticipate the most likely criticisms during drafting. The European Small Business Alliance (ESBA) argued that the scheme would disadvantage small companies that are unable to meet the requirements of a secure operator 'without any clear benefits'.[34] The British Federation of Small Businesses estimated that introducing the secure-operator requirements might cost a small business an initial fee of €135 000 (*c.* $243 000) and an annual fee of €131 000 (*c.* $250 000).[35]

The complaint by industry that the EU was creating a 'forest of regulations' was a response to the fact that the EU made changes to the Customs Code and proposed the regulation on supply-chain security shortly after security regulations related to civil aviation and port security came into effect. After civil aircraft were used to mount attacks in the USA in September 2001, the EU rapidly developed EC Regulation 2320/2002 to lay down new aviation security provisions. The regulation was adopted on 16 December 2002 and entered

[33] Commission of the European Communities (note 32), p. 8.

[34] Sommer, T., President of the ESBA, quoted in 'Transport security proposal could "cripple" small businesses', Euractiv.com, 4 Sep. 2006, URL <http://www.euractiv.com/en/transport/transport-security-proposal-cripple-small-businesses/article-157458>.

[35] Cave, A., Federation of Small Businesses, 'Briefing note: European Commission's proposal on enhancing supply chain security', 9 Aug. 2006, URL <http://www.fsb.org.uk/data/default.asp?id=409&loc=policy>.

into force in January 2003.[36] It contains provisions related to many aspects of aviation security, including some that have a direct impact on the movement of air cargo. As well as establishing certain common minimum security standards, every EU member state is required to establish a national civil aviation security programme with corresponding quality-control and training programmes within three months of entry into force of the regulation. Member states are permitted to apply more stringent security measures at the national level according to need. Reviewing the implementation of the regulation after two years of operation, the Commission expressed the view that errors in drafting (owing largely to the speed of the process) needed to be corrected because the 25 national systems that had been put in place had created a potential distortion of competition that could undermine the single market. The Commission has argued for the greatest possible harmonization of security measures and procedures to facilitate the work of industry (including airlines, cargo shippers and freight forwarders as well as manufacturers of security equipment).[37]

In September 2005 the European Commission presented a new proposal that would require member states to undertake an assessment of the risk to aviation security and to justify national actions and security measures more stringent than those laid down in the January 2003 regulation if requested to do so by the Commission. This proposal was intended to address concerns that industry might be burdened with unnecessary security requirements, while preserving the right of member states to respond to threats with heightened security requirements. Particular attention was drawn to the security of air cargo, and the Commission suggested interlinking the security requirements for regulated agents and known shippers with the AEO concept developed in the Customs Code.[38]

The EU has taken a somewhat similar approach in regard to port security. The international standards developed in the SOLAS Convention and the ISPS Code have been incorporated in EU law through a regulation.[39] A subsequent directive establishes implementing measures to be taken by member states to try to ensure uniform implementation that does not distort the single market.[40]

[36] 'Regulation (EC) No. 2320/2002 of the European Parliament and of the Council of 16 December 2002 establishing common rules in the field of civil aviation security', *Official Journal of the European Communities*, L355 (30 Dec. 2002), pp. 1–21.

[37] European Commission, 'Proposal for a Regulation of the European Parliament and of the Council on common rules in the field of civil aviation security', COM(2005) 429 final, Brussels, 22 Sep. 2005, URL <http://eur-lex.europa.eu/en/dossier/dossier_06.htm>, p. 2.

[38] European Commission (note 37).

[39] 'Regulation (EC) No. 725/2004 of the European Parliament and of the Council of 31 March 2004 on enhancing ship and port facility security', *Official Journal of the European Union*, L129 (29 Apr. 2004), pp. 1–86.

[40] 'Directive 2005/65/EC of the European Parliament and of the Council of 26 October 2005 on enhancing port security', *Official Journal of the European Union*, no. L310 (25 Nov. 2005), pp. 1–12.

IV. The role of business and the private sector in securing sensitive civil items

The previous sections underline that the need to combat mass-impact terrorism is creating new sets of security regulations that apply directly to business. Business can readily share the objective of preventing mass-impact terrorism. Apart from protecting themselves from direct attack, the business community should recognize three other compelling reasons to put in place effective security systems. First, businesses have a legal duty to comply with the law and face the risk of punishment if they do not. Second, they have a moral obligation to their employees and to the societies that support their activities not to contribute to activities that undermine security. Third, they have a self-interest that stems from the potentially devastating economic consequences for their companies if they are connected in the public mind with mass-impact terrorism. Industry recognizes the need for regulation—on the condition that rules are clearly drafted, well publicized, do not disrupt day-to-day business practice, include checks on enforcement, and provided that punishments for non-compliance 'fit the crime'.

When multiple regulators take an interest in solving the same basic problem, however, it is understandable that business would become nervous. To take the European example, in the worst case (from the perspective of business), a business might face five sets of requirements under anti-terrorist legislation: a European supply-chain security regulation, European customs regulations, aviation security regulations, port security regulations and security regulations specific to the particular product. Even if the regulations offer the opportunity to earn the right to use simplified procedures, the detailed requirements to achieve the status of trusted partner might differ in each case. Moreover, this would be the situation for European regulations, but additional or different requirements could apply in other jurisdictions such as the USA.

This view was summarized in 2003 by a Swedish business association, which requested that new systems should avoid creating the need for new information technology systems that would require heavy investments. A concern was expressed that 'too many new initiatives are under way, at the same time, which will make coordination of the different projects more difficult and lead to fragmentation and non-compatible solutions'.[41] More recently, responding to the proposed EU regulation on the security of supply chains, the International Road Transport Union pointed to the risk that too many security initiatives would create confusion for operators.[42]

[41] Confederation of Swedish Enterprise and Swedish Chamber of Commerce, 'Reformation of the Community Customs Code: position paper on the Swedish business community's response to the European Commission's latest initiatives', Interinstitutional file 2003/167(COD), 2003, URL <http://www.swedfreight.se/sidor/transppol/EU%20_ccr_sw_com.pdf>.

[42] Dahlin, B., President of the International Road Transport Union Goods Transport Liaison Committee, quoted in 'Transport security proposal could "cripple" small businesses' (note 34).

The idea of forming a closer partnership between regulators and industry is being explored and an informal bargain seems to be emerging: a business that can demonstrate that it has internal mechanisms in place to ensure that its actions do not undermine security will be relieved of some regulatory requirements. What is now needed is common understanding of what business must do in order to take advantage of simplified procedures related to security regulations, and detailed work to elaborate the agreed elements. Particular attention is required in two areas—the need to understand the potential uses of civil items and knowledge about the background of persons with access to them.

To simplify and harmonize the task of industry, several initiatives are exploring the development of certified standards for business security systems that would become part of a company's quality-management system. A growing number of companies use a management approach based on documenting policies and procedures to improve and control the various processes that will ultimately lead to improved business performance.[43]

Although designing a management system probably has to be approached on a company-by-company basis, if there are too many variations and differences in approach by companies there may be less confidence in the effectiveness of such measures. In general, a set of standards will have to establish company policy at the highest level and must put in place an organizational structure to determine the authority and responsibility of different officers of the company. The system should offer guidance to partners along the supply chain and to subsidiaries of the company and affiliates, and it should create obligations on staff to carry out established duties with real and serious consequences for non-compliance. The standard would need to address issues of physical security, access controls, personnel security, documentation procedures, information security, and issues related to staff education, training and awareness. Several groups are exploring the development of voluntary security standards together with accreditation systems for them.[44]

Creating standards is a complicated process that requires administration, which can be provided by dedicated standards organizations, such as the ISO, a global body, and the European Committee for Standardization (Comité Europèen de Normalisation, CEN), a European organization.[45] Where possible, standards should be developed at the international level to promote harmonization and to avoid creating technical barriers to trade.

[43] A number of such approaches have been developed, including SIX-SIGMA, Total Quality Management and the ISO 9000 series of standards.

[44] Standards are the specifications, contained in technical agreements, that provide the framework for compatible technology or a compatible approach to a particular issue or problem worldwide. Standards are voluntary, and businesses adopt them because they see a self-interest in knowing that they are using methods or technologies that are accepted internationally by both their customers and their competitors.

[45] The ISO is a network of the national standards institutes of 157 countries, with a Central Secretariat that coordinates the system. It is a non-governmental organization but many of its member institutes are government agencies or have some official status in their countries. See the ISO website, URL <http://www.iso.org>. The CEN is a committee of the national standards bodies of the EU and European Free Trade Association countries that has set itself the task of contributing to the development of standards in the European Economic Area. See the CEN website, URL <http://www.cen.eu>.

Although a standard can be said to be established once the specifications are agreed and published, it will normally have greater effect if implementation is validated in some way. The most common form of validation is an audit process. The company concerned is likely to conduct its own review of implementation and may publish a report on steps taken, but an audit to verify conformance with agreed criteria may have more credibility if it is carried out by an independent body. This audit can lead to certification—written assurance (the certificate) by the independent external body that has audited the system and verified that it conforms to the requirements specified in the standard.

The certification process could be carried out by a government agency or government-accredited organizations if the standard is related to security or linked to compliance with anti-terrorism laws, and there are precedents for this in other areas of regulation. The responsible government agencies can take advantage of certification guidelines prepared by international bodies.[46] Alternatively, the task of certification might be given to a trusted party that would probably need to be accredited—that is, recognized as competent to carry out certification in the particular business sector of concern.[47]

Standards bodies are now beginning to take security issues into the catalogue of standards being developed. A CEN working group is tasked with developing a standard for Protection and Security of the Citizen.[48] The mandate for the group was created in December 2003 and it has been meeting since March 2004. The working group is a network that brings CEN members together with representatives of relevant directorates-general from the European Commission, the Joint Research Centre within the Commission, the European Police Office (Europol) and a number of industry associations. It has established a number of expert groups that examine different issues to see whether there is an argument for producing a standard in that area. These groups are looking at a number of issues of relevance to the matters discussed in this chapter, including: (*a*) integrated border management, (*b*) critical infrastructure and energy supply, (*c*) security of the supply chain, (*d*) defence against terrorism, and (*e*) reduction of crime risks in products and services.

The ISO is also developing standards for the provision of protection against threats to people, physical assets, and infrastructure and information technology assets, including electronic networks and facilities. The ISO's Strategic Advisory Group on Security is working on initiatives such as a written guide to encourage all technical committees across the ISO system to take security

[46] E.g. the WCO sets guidelines for national customs administrations about how to certify the requirements for supply-chain security programmes that were recently agreed in the WCO framework. This facilitates the mutual recognition of certificates between countries. The EU is developing guidelines for certifying the status of an AEO, which was created in the revised Customs Code.

[47] The European Co-operation for Accreditation (EA) was established in 2000 through the merger of several accreditation bodies to create a network of nationally recognized accreditation bodies. The participants in the EA currently cover accreditation of certification bodies in laboratories, inspection agencies, quality-management systems and environmental-management systems.

[48] European Committee for Standardization, 'CEN BT/WG 161: "protection and security of the citizen"', URL <http://www.cen.eu/cenorm/businessdomains/businessdomains/security+and+defence/security/btwg161.asp>.

into account in a coordinated and logical way. The need for a number of new international standards has also been identified, such as standards for built infrastructure, personal identification, transport of goods and persons, and cyber-security. As part of the ISO's work to support the transport of goods, a specification has been developed for an ISO publicly available standard on security-management systems for the supply chain (ISO/PAS 28001).[49] Work to create ISO/PAS 28001 began at the end of 2005. The specification for ISO/PAS 28001 outlines the requirements to enable an organization to establish, implement, maintain and improve a security-management system, including financing, manufacturing, information management and the facilities for packing, storing and transferring goods between modes of transport and locations. This is part of a series of security standards that are published by the ISO, and others are being developed.

V. Conclusions

Much work is being done to create a framework for controlling items that represent a potential security risk but cannot be brought into the scope of arms control because of their purely civil nature. These efforts involve a wide range of actors that are not traditionally accustomed to thinking about security matters. Developing the process in a coherent manner is a formidable challenge.

It is premature to reach conclusions about the final outcome of efforts to put in place measures to strengthen security by controlling non-military items. There is currently no system for bringing together the different communities that are engaged in the process to exchange information and describe their activities to one another. An effort to coordinate initiatives as diverse as those described in this chapter or to seek a single framework in which to manage them would be unlikely to succeed. However, a regular opportunity for reporting and information exchange could be organized either on a regional basis or under the global umbrella provided by the United Nations.

Several processes already in place involve the business community directly, including some that address supply-chain security. In one way or another, these different processes all require the classification of items in the supply chain against a set of technical risk factors, the screening of transactions against problematic end-user and end-use information, the establishment of a comprehensive, electronic system for document archival and retrieval, the creation of an effective information system for collecting information and reporting it in different formats, and the development of an education and training programme. Moreover, all of these processes promote the idea that a business can be awarded the status of a trusted, secure operator and that certain benefits will flow from possessing that status.

[49] International Organization for Standardization, 'PAS 28001: Ships and marine technology: best practices for implementing supply chain security, assessments and plans', 4 Apr. 2006, URL <http://www.iso.org/>.