



Stockholm International Peace Research Institute
Non-proliferation and Export Control Project
Signalistgatan 9, 169 70 Solna, Stockholm

Export control in the context of the contemporary threat environment

Seventh Annual International Export Control Conference

Stockholm, 20-22 September 2005

Ian Anthony, SIPRI

1. The changing nature of the proliferation threat

The term proliferation has been taken to mean the process by which the armed forces of states come into possession of or gain the ability to use chemical, biological, radiological or nuclear weapons. This understanding reflected the concern was the use of weapons in conflicts between states or between alliances of states.

A more modern and sophisticated view of what proliferation is and how it needs to be fought has begun to become widely accepted. This new understanding places as much emphasis on the threats posed by proliferation to non-state actors as it does on the more traditional threat from proliferation by states. As an example, in its threat assessments the EU not only takes into account the threat from weapons but explicitly points to the risk associated with acquisition of chemical, biological, radiological and nuclear (CBRN) goods and materials by non-state actors intending to use them in acts of mass impact terrorism.

In June 2004 Guy de Vries, the EU counter-terrorism coordinator, observed that ‘the risk of small scale, low tech and relatively simple CBRN terrorist attacks causing social disruption is to be considered more likely than large scale, high tech and complicated CBRN attacks causing mass destruction. It would certainly be wrong, however, to rule out the risk of such large scale attacks.’

In regard to Weapons of Mass Destruction (WMD), there has also been a change in view. A Weapon of Mass Destruction has traditionally been thought of as one capable of causing high lethality and massive physical destruction in an attack involving the use of a relatively few munitions. The special character of nuclear weapons has been linked to the fact that this level of destruction can be achieved with just one device. Under certain conditions biological weapons might have the same effect.

In spite of the fact that there have been a number of mass *impact* terrorist attacks, thus far there has not been any use of CBRN weapons that have led to mass *destruction*. Nevertheless, in particular after the attacks in the United States in September 2001 attention has been focused on the threat of mass disruption caused by the use of materials that are not weapons as traditionally defined. Repeated, coordinated attacks using materials that cause low levels of lethality and physical destruction could lead to extreme

economic damage. Depending on the response, such attacks might represent a threat to the democratic system of the states where targets are located.

There is a convincing body of evidence that a small number of states have made a dedicated attempt to acquire weapons of mass destruction. In addition to the countries that appear to be developing nuclear weapons, there are also countries that seem intent on holding open the option to develop nuclear weapons in the future by putting in place the research, technology and industrial base that would allow the fairly rapid development of a weapons programme should a political decision be taken.

The local roots of these weapon programmes are to be found in the security environment in areas of conflict and tension (and in particular in the Middle East and Northeast Asia). During the Cold War the risk that any conflict would escalate into a superpower confrontation meant a very heavy emphasis on war avoidance. Where major powers became engaged in conflicts around the world it was usually in order to assure the appropriate degree of restraint and control, to minimize any risk of escalation. This conservative and cautious approach has given way to increased attention to how force might be applied in various ways to achieve what are considered desirable political outcomes. These changes have probably raised uncertainties in the minds of strategic planners about the kind of security environment they might anticipate in the future and might, therefore, contribute to a tendency to hold open a wide range of force planning options.

2. From export control to trade control

A number of conclusions flow from the above observations.

First, the number of locations where there are state proliferation programmes of concern is small. The problem facing export controllers in regard to state proliferation is how to prevent proliferation-sensitive items from flowing to these specific locations, rather than being a general and global problem.

Second, one of the main security threats is now posed by the presence of non-state actors with malicious intent in the countries where they intend to carry out acts of mass impact terrorism. It would be of particular concern if there was clear evidence of an “insider threat” within branches of industry or research where materials are available that can be directly applied in such attacks.

Third, there have been changes in the international marketplace and in the way that technology transfer takes place that challenge traditional export controls. The greater availability of a much wider class of dual-use items and technologies has required that the traditional approach of licensing items on lists compiled according to the technical characteristics of the given listed products has been supplemented by the growing use of end-use (or “catch-all”) controls. At the same time, the tendency for industry to work in international teams to develop, manufacture and market dual-use but proliferation-sensitive items, combined with the worldwide availability of wide-area computer networks (including the internet) have created a need for effective controls over “intangible” technology transfers.

Taken together, these developments suggest the need to move away from a system of export control to a system of trade control. This would respond to the need for any proliferation-sensitive transaction to be assessed against agreed security criteria regardless of the location of the end-user.

3. New ways of working with industry

Efforts to respond to these new threats are changing the approach to regulation by putting pressure on states to introduce controls not only on their own behaviour but also on the behaviour of the companies and enterprises operating within their jurisdiction.

Whereas arms control treaties have largely left it to the discretion of States Parties to decide how to implement their obligations at the national level, UN Security Council Resolution 1540 takes the step of prescribing at least some elements of national implementation that would have a direct impact on industry.

UNSC Resolution 1540 introduces obligations on states to introduce effective export controls and border security management. The resolution requires the criminalization of any WMD-related acts carried out by individuals (including legal or physical persons) that would contribute to proliferation or mass impact terrorism. Moreover, the resolution requires states to put in place effective measures to account for, secure and physically protect proliferation-sensitive materials.

In mid-2005 a group of 89 states agreed to amendments to the Convention on Physical Protection of Nuclear Materials that will extend agreed international standards for physical protection, currently applied to international shipments, to any nuclear material used for peaceful purposes and nuclear facilities used for peaceful purposes.

In January 2004 the IAEA Code of Conduct for the Safety and Security of Radioactive Sources was published in final form. The Code, which is focused on sealed source management and control, prescribes legislative frameworks, regulatory programmes, and import/export provisions for IAEA Member States. While it is not a legally binding commitment, a number of states are now working to introduce the provisions of the Code in national legislation and to conduct outreach to try and persuade other states to take the same step.

New types of export licence have been introduced.

General licences (such as the EU Community General Export Authorisation) allow the export of specified controlled items by any exporter to any end-user in specified destinations that the conditions in the licence are met. Global project licences are intended to simplify the arrangements for licensing military goods and technologies between certain countries collaborating in certain specific defence projects.

In Regulation no. 648/2005 of the European Parliament and the Council of 13 April 2005 amendments were introduced to the Council Regulation (EEC) No 2913/92 that established the Community Customs Code. The Regulation creates the status of 'authorised economic operator' that may be awarded to any entity that meets common criteria relating to the operator's internal control systems, financial solvency and record of compliance with existing laws and regulations. An authorised economic operator shall benefit from facilitations with regard to customs controls relating to security and safety and/or from simplifications provided for under the customs rules.

The status of authorised economic operator, once granted by one Member State, should be recognised by the other Member States. Moreover, other EU Member States should allow the use of simplifications by authorised economic operators provided they meet all the specific requirements for use of the particular simplifications. In considering a request to use simplifications, the other Member States need not repeat the evaluation of

the operator that will already have been completed by the Member State that granted the operator the status of authorised economic operator.

Proposals intended to raise the efficiency of export controls have also come forward from industry. Dominique Lamoureux, the Vice-President for Corporate Social Responsibility at the THALES company, has developed a discussion paper describing a general framework that could give companies of whatever size the legal security they require to manage their obligation to control sensitive technologies more efficiently by integrating this obligation into their internal management and control procedures. Lamoureux proposes that certified companies operating in world markets would develop an integrated approach to managing the export control of sensitive goods and technologies.

In essence, the exporter would specifically undertake to enforce control regulations, exercise vigilance with respect to the risk of diversion, and agree to a process of voluntary certification combined with greater transparency.

Following on from an extensive study of the role of the business in helping to build security, SIPRI has drawn attention to the responsibility of private companies for the lawful and responsible handling of their direct and indirect impact on other security processes.

To shoulder this responsibility it is necessary for business to enforce internal security discipline through employee vetting, knowledge control, security routines and their monitoring and enforcement. In addition, the direct impact of business on security requires observance of all relevant (national or international) technology and export controls, embargoes, provisions of humanitarian law and other defined ethical standards. Increasingly this corporate social responsibility extends beyond manufacturing industry to include the provision of a range of different services.

In the nuclear, chemical and bio-industries, companies are likely to be pressed to face up to the responsibility to supplement *safety* controls on substances that can cause harm to employees or public by accident with *security* controls that take into account the risk of malicious acts in regard to substances and technologies that may be ‘weaponised’ or used in acts of mass impact terrorism.

Companies and financial institutions are being reminded of and pressed to observe their expanding responsibilities in regard of international and national rules relating to terrorist financing as well as informed of the universal prohibitions on any actions that facilitate trade and transfer in WMD-relevant materials and knowledge; transportation and travel security.

4. A possible way forward

Over the next few years the implementation of new controls may increase the responsibility of business for public security across a range of different fields. Those mentioned above are in fact only a few of the new responsibilities that companies may have to take on. The imperative on industry and commerce to maintain and increase the volume of trade and investment will continue.

It is desirable to find a form of regulation that minimizes the burden on companies while providing maximum assurance that companies are meeting all of their corporate responsibilities for maintaining security.

One approach that might help to achieve this outcome would be to offer regulators insight into future transactions and activities undertaken by companies while allowing companies to demonstrate their own capacity to control proliferation-sensitive elements of their business practices. Under such a system of control certain minimum requirements would have to be met.

The company would need to provide the authorities with a single document containing a detailed picture of its future activities during an agreed time period. The document would have to include a regulatory impact assessment that would explain all of the different obligations of the company in regard to the reported future transactions and an explanation of how these obligations were being met.

The regulatory authorities would have the opportunity to extract individual activities for further scrutiny and licensing, but for others the company would receive a single 'letter of comfort' or similar document giving assent. This would release the company from seeking the multiple separate authorisations currently needed to satisfy different requirements. This process would involve the regulators in the different jurisdictions in which the company was carrying out the specified activities and the authorisation granted would be valid in all those jurisdictions.

Many aspects of this approach would need to be examined in much greater detail before it could be considered a fully fledged proposal. However, the process of building corporate responsibility for security should be seen as a high priority in risk reduction.