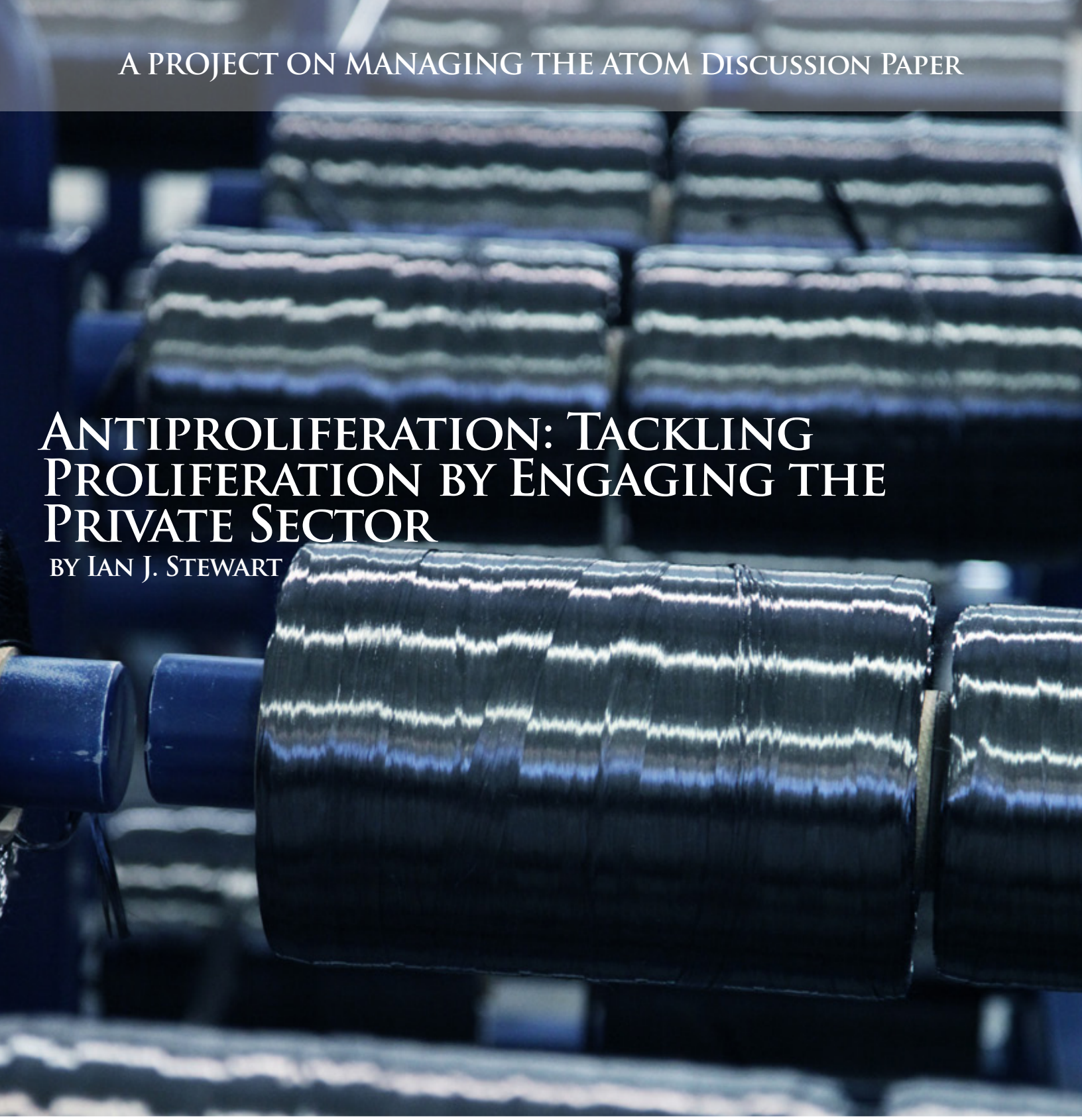
A PROJECT ON MANAGING THE ATOM DISCUSSION PAPER

ANTIPROLIFERATION: TACKLING PROLIFERATION BY ENGAGING THE PRIVATE SECTOR

BY IAN J. STEWART



HARVARD Kennedy School
BELFER CENTER for Science and International Affairs

NOVEMBER 2012

Discussion Paper #2012-15

About the Author

Ian J. Stewart is a research fellow with the International Security Program and the Project on Managing the Atom at Harvard's Belfer Center for Science and International Affairs. He is also lead researcher on Project Alpha in the Center for Science and Security Studies at King's College London, a project that works to engage the private sector in countering proliferation.

Acknowledgements

The author would like to thank the British Foreign and Commonwealth Office for their support of Project Alpha. He also would like to thank the staff of the Project on Managing the Atom at Harvard's Belfer Center and the staff of Project Alpha of King's College London for feedback on earlier drafts of this paper – in particular, the author would like to thank Professor Matthew Bunn and Professor Wyn Q. Bowen.

The Project on Managing the Atom would like to thank the John D. and Catherine T. MacArthur Foundation for its generous support.

Cover Image: Spools of carbon fiber, usable for lightweight, high-performance car parts, or high performance centrifuges for uranium enrichment.

A PROJECT ON MANAGING THE ATOM DISCUSSION PAPER

ANTIPROLIFERATION: TACKLING PROLIFERATION BY ENGAGING THE PRIVATE SECTOR

BY IAN J. STEWART

HARVARD Kennedy School
BELFER CENTER for Science and International Affairs

NOVEMBER 2012

Abstract

This paper exploits the concept of antiproliferation[1] to analyze the potential for mobilizing the private sector in countering the proliferation of weapons of mass destruction. Illicit trade from the international marketplace plays a direct role in sustaining the nuclear and missile programs of several countries, including Iran, in defiance of UN sanctions. These programs also profit indirectly from trade-enabling services, such as insurance, financing, and shipping. It is argued that almost all firms will work to avoid direct involvement with proliferation for a variety of reasons, but that firms often lack the systems, expertise, and information required to identify illicit proliferation-related trade.

This paper sets out what measures the private sector should take in order to manage the legal, financial and reputational risks associated with involvement in proliferation-related trade, and makes recommendations to national authorities for how to support antiproliferation. These recommendations center on the creation of partnerships between national authorities and the private sector. Strategically engaging the private sector requires partnerships to be developed between governments and businesses and, at the practical level, that a range of tools, services, and guidance materials also be developed. The potential contribution of third-party facilitators in developing and deploying antiproliferation is also examined.

1 In the 1990's Dr Bradley Roberts introduced antiproliferation as a notion capturing the spirit of opposition to proliferation while encompassing a growing array of policy tools. See B. Roberts, "From Nonproliferation to Antiproliferation," *International Security* Vol. 18, No. 1 (Summer, 1993), pp. 139-173. The use of the term in this paper refocuses this same spirit of opposition, but in reference to all measures that the private sector should take in order to prevent proliferation.

Table of Contents

Foreword

Traditionally, nation-states have taken the lead in implementing the main elements of supply-side nonproliferation measures, namely export controls and technology sanctions. During the Cold War the ideological conflict between the western and eastern camps dominated strategic trade controls with, for example, COCOM established to control western trade with communist countries. At this time, nuclear technology, and the advanced manufacturing capabilities involved in its development, were largely concentrated in the military-industrial base maintained by each bloc. With the end of the Cold War, the privatization of the defense industry and the globalization of advanced manufacturing capabilities, the ability of nation states to control strategic trade has now been somewhat constrained. The spread of the high-technology manufacturing base has also seen the opening of new proliferation pathways, as demonstrated by A.Q Khan's proliferation activities and the diversification of trade routes used by proliferators to sustain their programs by seeking technologies from the international marketplace.[1]

The response of the international community to these evolving strategic and commercial realities was to reinforce the state-centric approach through United Nations Security Council Resolution 1540 (2004), which sets out what supply-side controls national authorities must adopt to prevent the proliferation of non-conventional weapons. To date 168 of 193 countries have submitted implementation reports to the committee established to oversee the implementation of 1540, and many countries have since qualitatively improved the implementation of their supply-side controls. However, the risk remains that the globalized marketplace may be used as a source of technology to support the proliferation of non-conventional weapons.[2] Iran is a key case in point: despite several UN Security Council Resolutions imposing sanctions that are binding on all member states, Iran continues to illicitly acquire the sanctioned technologies it needs to sustain and expand its nuclear program.[3]

In a globalized marketplace the implementation of supply-side controls is increasingly difficult: the manufacturing base is increasingly dispersed; shipping routes are increasingly complex; and businesses are increasingly multinational in both ownership and operation. Proliferation-sensitive dual-use technologies may also now be more commonly used in commercial and consumer applications than has previously been the case.

Despite these challenges, sanctions continue to be the tool of choice for the international community in responding to states that present proliferation concerns. Sanctions may be an attractive option for supplier states because they have a degree of control over their adoption. For example, as a result of diplomatic action within the UN Security Council or through domestic legislation, laws may be passed that prevent the private sector from conducting certain types of trade even in circumstances

1 On A.Q. Khan's proliferant activities using export networks, see foremost: Sanger, D. E., "The Khan Network," Conference on South Asia and the Nuclear Future (Stanford, 2004), http://iis-db.stanford.edu/evnts/3889/Khan_network-paper.pdf, accessed April 9, 2012. For a more recent example of attempts by Iran to procure maraging steel, aluminum 7075, vacuum systems and more in breach of sanctions, see 'District of Columbia Incitement 12-cr-00061', July 12, 2012.

2 Letter dated February 1, 2012 from the Chair of the Security Council Committee established pursuant to resolution 1540 (2004) addressed to the President of the Security Council, available online at http://www.un.org/ga/search/view_doc.asp?symbol=S/2012/79.

3 Letter dated June 4, 2012 from the Panel of Experts established pursuant to resolution 1929 (2010) addressed to the President of the Security Council, available online at http://www.un.org/ga/search/view_doc.asp?symbol=S/2012/395.

when the use of force would not be acceptable. Such laws may be enforced through border inspections and by delivering threats of punitive sanctions against deviant exporters. However, the same supplier states may only be able to exert influence over the target state through diplomatic pressure because of the lack of an international body tasked with enforcing those commitments that are binding upon states.

Nevertheless, supply-side controls include a range of measures which operate in different ways and place different obligations on certain business sectors. While economic sanctions may prevent nearly all trade with a target state, or more specifically oil and gas-related trade and investment for example, targeted sanctions place restrictions on trade that could directly stimulate activities of concern or enable services to develop which could facilitate the evasion of sanctions. For example, by some estimates targeted sanctions imposed on Iran have delayed its nuclear program for up to six years.[4]

Of course, the implementation and enforcement of laws can never be perfect, and the national authority is often not in a position to control all activities within its jurisdiction because of practical and systemic limitations. These limitations include the limited resources available to the national authority to promote awareness, outreach, and enforcement; the difficulty in detecting illicit trade when the proliferating state actively attempts to hide the true end use of illicit materials; and the imperative for legitimate trade not to be disproportionately burdened by prohibitive controls. Moreover, individual companies – with an in-depth knowledge of their own market sector, technologies, and customer base – are often better placed than the national authority to identify instances of illicit activity, although often they will lack the information and expertise required to do so.[5]

The purpose of this paper is to set out measures that national authorities and the private sector should take in order to improve implementation of trade controls and how they can be delivered in practice. The measures are based upon the principle of partnership between national authorities and the private sector, a subject which Project Alpha based in the Centre for Science and Security Studies, King's College London, has been examining with the sponsorship of the British government.

4 C. Hope, "MI6 chief Sir John Sawers: 'We foiled Iranian nuclear weapons bid,'" the Telegraph, July 12, 2012. Available online at http://www.telegraph.co.uk/news/uknews/terrorism-in-the-uk/9396360/MI6-chief-Sir-John-Sawers-We-foiled-Iranian-nuclear-weapons-bid.html.

5 Illicit activity as described here includes the acquisition of proliferation-sensitive goods using clandestine techniques and the use of services such as finance, banking, and insurance to support programs of concern.

Preventing Proliferation through Supply-side Controls

Supply-side controls are measures used by sanction-sending states to control the trade in goods or services with other countries in order to effect a policy goal. This umbrella term includes both export controls and technology sanctions, where export controls are proactive and nominally non-discriminatory in that they control a defined list of technologies and services regardless of recipient, and sanctions are reactive and discriminatory in that they are designed to affect policies within a specific country.

While sanctions may be invoked by sender states simply to be seen to "do something", a number of specific goals can be attributed to supply-side controls more generally.[6] These goals may include:

- Slowing proliferation by making prerequisite technologies more difficult and costly to acquire
- Detecting proliferation attempts by highlighting proliferation-related procurement trends
- Deterring proliferators, which may occur at two levels:
    - Where the fear of being detected can in fact deter a country from pursuing the acquisition of proliferation sensitive technology
    - Where the fear of designation deters a company from conducting trade that contributes to proliferation (or that defies sanctions)
- Dissuading proliferation by reinforcing the nonproliferation norm

Sanctions and export controls impose restrictions on a variety of activities ranging from trade in certain sensitive goods to the prohibition of trade with designated entities. These tools can contribute to nonproliferation both directly and indirectly. A direct contribution would include preventing an export of a material that was destined for use in an enrichment centrifuge in Iran, for example, whereas an indirect contribution would involve disrupting the financing or shipping of the material to Iran. For the purposes of this paper, such indirect services are termed "enabling services."

In free-market economies it is usually the private sector that conducts trade and, as such, the ability of supply-side controls to deliver the goals set out above is partly linked to the effectiveness of the implementation of these measures by the private sector, and partly linked to the ability of the national authority to enforce controls on private sector activity.

The aim of the international community and of national authorities should be two-fold. First, to ensure that potential proliferators cannot directly access the prerequisite technology from the international market place either illicitly or legitimately, thus slowing breakout. Second, sanctioned activity must not be allowed to benefit from access to trade-related enabling services.

Illicit Procurement

Supply-side controls have been effective in slowing most instances of proliferation. The response of proliferators to the international system of supply-side controls, however, has been to use deception,

6 Adapted from the framework presented in Neta C. Crawford and Audie Klotz, eds., *How Sanctions Work: Lessons from South Africa* (London: Palgrave Macmillan, 1999)

smuggling, and illicit procurement practices to evade controls. These practices usually involve the acquisition of components, materials, and equipment in isolation, often with only small, tell-tale signs indicating that ostensibly innocent trade is in fact linked to proliferation.[7] The use of such techniques by proliferators means that compliance with legal requirements is not sufficient to prevent a company's products from being used to enhance WMD programs, and so the adoption of antiproliferation principles by affected industries becomes central.

The number of firms actually affected by proliferation is relatively small; there are, in fact, few firms that manufacture key choke-point technologies which programs of concern could not be advanced without access to. Consequently, the engagement of such firms and the mobilization of the supply chain can help to counter even the clandestine acquisition of WMD-related materials. The following section explores measures that firms in affected sectors should implement in order to prevent their products from aiding proliferation.

7 Project Alpha at King's College London has been working to highlight the scope of illicit procurement in relation to WMD programs. See http://kcl.ac.uk/alpha for more information.

Antiproliferation: The Role of the Private Sector

It is the responsibility of the private sector to operationalize the requirements of nonproliferation measures as they relate to trade. While the ability of national authorities to control trade in strategic technologies is constantly challenged by the effects of globalization and other dynamic factors, the supply chains of the private sector do have the potential to act as nonproliferation assets. As mentioned above, firms are always better placed than the national authority to know their industry sector, customer base, and technology, and there are only a finite number of firms that manufacture the items of highest proliferation concern.

At present, the responsibilities of national authorities relate to the regulation of the private sector: national authorities adopt as law lists of controlled technologies, and companies are required to seek export licenses prior to exporting the controlled goods. This system is enforced by customs and border protection officials who inspect shipments to identify exports of controlled goods that do not have a license. However, this relationship requires a fundamental reconsideration. In order to effectively respond to the challenges posed by proliferant activities, there must be a shift toward sustaining partnerships between national authorities and the private sector so that antiproliferation compliance measures can be more easily adopted by industry. Both national authorities and the private sector must implement such measures above the minimum standards of compliance if involvement in proliferation is to be prevented; and, let us be clear, it is in the interests of both to do so.

Recommendation

R1: National authorities should facilitate the development of partnerships with the private sector

Private Sector Implementation

The requirements of supply-side controls vary from industry to industry and from sector to sector. The obligations of each specific sector are explored below. Nonetheless, regardless of business sector, if requirements and obligations for managing proliferation risks are to be effective, the private sector must implement a trade compliance system. As Brewer highlights, the private sector has no excuse for failing to adhere to export compliance laws.[8] For proliferators to be denied access to solicited services and technologies, firms in the sectors set out below must do the following:

1) **Adhere to the legal requirements of the jurisdictions within which they operate;**
2) **Undertake to implement the following measures (adapted from Brewer):**
    - **Implement a compliance system based on sector-specific best practices and integrate this system with the company's Corporate Social Responsibility Framework;**
    - **Develop and implement a corporate monitoring and detection system to identify illicit procurement attempts for proliferation-sensitive goods;**

8 Jonathan Brewer, "The private sector plays an important role in delaying the development of the Iranian nuclear program", *The Bulletin of the Atomic Scientists*, November 30, 2012.Available online at http://www.thebulletin.org/web-edition/roundtables/iran-and-the-west-next-steps.

- **Conduct background checks on customers and business partners using open-source material and, in consultation with relevant government departments, terminate business deals with entities of proliferation concern;**

All firms, regardless of sector or location, are prohibited by UN sanctions from conducting business with some entities. The requirement for background checks on potential business partners does not stop here, however, with many national authorities also imposing additional restrictions when trading with entities known to be of concern. Some national authorities go as far as to adopt extraterritorial measures that can apply even to firms outside the national jurisdiction. Finally, since not all entities of proliferation concern have been designated (or indeed even identified), firms should also conduct due diligence to verify the *bona fides* of an end user and end use when engaging in the trade of proliferation-sensitive technology or enabling services, in order to minimize the risk that the trade will support proliferation.

3) **Share suspicious inquiries and counter actions with government agencies, departments, and the private sector (using third party intermediaries if necessary);**

Diligent sales or compliance officials working in industry can often identify illicit procurement attempts even when the national authority is unable to do so. The detection and sharing of such efforts can allow national authorities and others in the business sector to detect future attempts by highlighting the latest entities and methodologies used by proliferators.

Such information is of intelligence value to governments and organizations with responsibilities related to nonproliferation, such as the International Atomic Energy Agency. Failure to collect and share such information can result in new procurement networks, front companies, and methods going undetected.

4) **Commit to training staff against a compliance competence framework or accreditation standard endorsed by the national authority;**

Implementing compliance in the private sector requires staff with knowledge and experience of the conceptual and practical requirements of the field, and training is the primary means by which such knowledge can be accumulated. Firms should undertake to train their staff against a compliance competence framework to ensure that the required skill-set is developed. Such training might be developed with the assistance of private-sector consultancies and incorporate simulation exercises designed to highlight the challenges faced by target entities.

5) **Require subsidiaries and agents, including those overseas, to implement equivalent systems;**

6) **Ensure business partners, brokers, and distributors, including those overseas, implement equivalent trade compliance systems;**

In working to evade export controls, proliferators often target the overseas representatives of firms engaged in the manufacture of the most proliferation-sensitive goods. Only by ensuring that such overseas business partners employ equivalent systems can a firm be certain that their goods will not be diverted to a program of concern.

7) **Adopt measures to protect the intangible technology (such as design and production information) associated with proliferation-sensitive goods or processes;**

Lack of "know how" or expertise – both types of tacit knowledge – is one factor that prevents proliferators from developing indigenous capabilities and capacity to produce proliferation-sensitive goods. It is almost always in a firm's own interests to protect intangible technologies as such information is commercially valuable.

8) **Encourage relevant professional bodies to adopt and disseminate the standards and emphasize adherence to these measures via the company's website.**

Regardless of how well any one firm implements export compliance, if others in the business sector fail to do likewise then proliferation attempts could still succeed. Trade associations and third parties can, therefore, provide a forum to build confidence between competing organizations that compliance obligations are being adhered to by all parties.

Project Alpha has seen this in practice: at the project's sector-specific outreach events for the carbon fiber and alloys industries, for example, firms were reassured to discover that others in their business sector shared experiences regarding the implementation of compliance.

Sectors Affected

The prerequisite to the implementation of these antiproliferation measures is the provision of guidance on what firms should do to limit instances of proliferation. While the additional measures may not be required by statute or criminal law, they could nonetheless be promoted by embedding them into commercial or civil contracts and, in doing so, bind the parties to implementing them. However, antiproliferation measures vary from sector to sector with, for example, those required in the financial sector varying greatly from those needed in technology exporting industries. Antiproliferation measures are relevant to the following sectors:

- Exporters: This category includes the manufacturers and distributors of physical goods and associated intangible technologies. The specific circumstances in which a license must be sought varies between states, but typically includes the following three situations:
    - The goods are controlled and the destination is an entity outside the customs zone;
    - The entity is designated or otherwise known to be involved in activities of concern;
    - The exporter knows or has been informed that the goods are designated for a WMD program or for a military program in a country that is subject to an arms embargo.
- Shippers: This category includes fast-freight forwarding companies and freight-based shipping firms. Typically, such firms are obliged to act only when a party to the shipment is a designated entity. However, such firms may also be asked to ship controlled goods without a license.
- Insurance firms: These include those that insure individual firms or insure other insurance firms. In addition to identifying whether a prospective client is a designated entity, insurance firms should also ensure that their clients have a compliance system in place and have ceased handling illegal business, including in relation to sanctioned activities.
- Financial services firms: Banks and other financial institutions are obliged not to conduct business with designated entities and destinations. U.S. and U.K. sanctions, in particular, designate

the whole Iranian financial system, meaning that banks operating in these territories (or those operating elsewhere that wish to comply with U.S. extraterritorial measures) must ensure that no transactions take place with any Iranian financial institution unless a license has been granted.

- Academia / researchers: Export controls and sanctions apply as much to academia as to other business sectors, although a balance must be struck with academic freedom. Researchers in academia or elsewhere are likely to possess intangible information that could be of use to proliferators. Academia and professional bodies have a responsibility to ensure that appropriate controls are in place to manage these proliferation risks, even when no legal obligation exists. In practice, this may be addressed through "codes of practice" rather than through laws and legislation.
- Export compliance consultants: Numerous consultants provide compliance-related guidance to individual firms. It is the responsibility of such consultants to provide guidance that is well informed.

Businesses operating in each of these sectors must take measures to avoid direct or indirect involvement in proliferation.

Recommendation

R2: National authorities should set out for the insurance, exporting, and finance industries the measures that should be implemented in order to counter proliferation, including defining the scope of WMD programs as relevant for the industry sector.

Private Sector Support for Antiproliferation

Firms are clearly willing to adopt best practice trade compliance measures. In a survey conducted by Project Alpha of 50 British firms in 2012, 53 percent of respondents indicated that they would advocate that their firm adopt best practice compliance driven by a commitment to corporate responsibility, with a further 32 percent advocating adoption driven by a need to manage risks more effectively. Only 9 percent of respondents would advocate adoption driven by a desire to secure incentives such as access to discretionary license types. Overall, the survey results clearly indicate that most private sector firms are prepared to work with national authorities to counter proliferation-related trade. [9]

The same survey found that 52 percent of respondents would do more than is legally required in relation to compliance.

These findings are reinforced by interviews. Project Alpha has directly engaged with more than 300 firms, most of which have taken measures beyond those strictly required by law.

By applying an analytical framework to the drivers for compliance, a hypothesis could be put forward that firms will comply only when the potential costs of not doing so outweigh the costs of doing so, but this hypothesis was not supported by the research. Research conducted by Project Alpha has identified that the costs associated with not doing so could include:

9 Project Alpha. (November 2011). Survey Results. Not yet published . London.

- Legal: Deliberate non-compliance is illegal and can result in imprisonment. In the U.K., for example, failing to comply with proliferation financing obligations can result in a prison sentence of up to 7 years.
- Financial: Non-compliant firms regularly face significant fines.
- Reputational: Being linked to proliferation-related trade, whether legal or otherwise, damages the reputation of the company. The U.S. government maintains a list of denied entities that are suspected of noncompliance, and such firms can often neither compete for U.S. government contracts nor import goods or services from the United States. More generally, many leading firms also opt not to do business with firms that have been linked to non-compliance or proliferation as part of a risk-management strategy.
- Normative: Involvement in proliferation is morally wrong.

Additionally, it should be recognized that there can be costs to the private sector for both compliance and non-compliance. Costs of compliance include staffing and resourcing costs associated with recruiting, training, and paying export compliance professionals, a less responsive sales force, and lost sales. Costs of non-compliance can include fines and other financial penalties.

In the U.K., only 18 firms have been fined and fewer still (eight) have been prosecuted in the last three years.[10] This would appear to suggest that the detection and prosecution rate may have only a weak deterrent effect, and that other factors drive compliance with normative and reputational issues dominating.[11]

Supply Chains and Antiproliferation

Another potential driver for the adoption of antiproliferation practices relates to the supply chain itself. The primary markets for many of the proliferation-sensitive technologies are the defense, nuclear, and aerospace sectors. These sectors can thus play a leading role in securing the support of their supply chains in relation to implementing nonproliferation measures. Firms in these sectors should be pressed to implement best-practice compliance systems given the high level of proliferation risk associated with their products. Such firms should also encourage adherence to these same high standards in their supply chain.

Extraterritoriality

A final driver for antiproliferation principles relates to exclusion from the international marketplace. In the case of additional measures adopted by the United States, many have an extraterritorial element, pressuring non-U.S. firms to comply with U.S. law.

---

10 http://www.bis.gov.uk/policies/export-control-organisation/eco-press-prosecutions and http://www.bis.gov.uk/policies/export-control-organisation/eco-press-prosecutions/compound-penalties

11 It should be noted, however, that this analysis is based on a heavily-skewed dataset. Respondents to the survey were typically compliance officials employed by large defense and consumer electronics firms.

U.S. extraterritorial measures are backed by the threat and use of sanctions against entities operating in third countries that fail to adhere to U.S. controls. These include:

- Being cut off from the U.S. financial system;
- Being precluded from consideration for U.S. government contracts; and
- Being listed as a denied entity for the purposes of U.S. trade control measures, where U.S. firms are prohibited from conducting business with denied entities without a license.

To achieve the effective implementation of a control system, firms may opt to use a range of services that contribute to effectiveness. These services can be sourced internally or externally, with the former including commercial, non-commercial, and government sources. Services that are a prerequisite to obtaining some desirable public goal are public goods, and authorities should seek to ensure that public goods are available even in the event of a market failure.

The Role of National Authorities

The UN Security Council has become the preeminent rule-making body with regards to preventing illicit trade. Through Resolution 1540 the Security Council has set out measures that all states must implement with regards to nuclear, chemical, and biological weapons and, with 168 countries submitting implementation reports, the scope of coverage goes beyond that of the voluntary export control regimes, such as the Nuclear Suppliers Group. Nonetheless, national authorities must implement trade control systems and facilitate compliance, and it is the private sector, at least in free-market economies, that must render operable the requirements of trade controls.

Current Obligations

The UN Security Council is the body to which individual national authorities are responsible. The UNSC requires all states to:

Measure	Source
Implement a system of export controls	1540
Enforce export and transshipment controls at the country's border	1540
Implement UN sanctions through domestic legislation	UN country-specific sanctions resolutions
Engage the private sector	1540

The passage of 1540 has resulted in the spread of the coverage of national legislation related to export controls, which is a vital prerequisite to increasing resilience to proliferation in additional countries.[12] 1540 also calls upon all states to "develop appropriate ways to work with and inform industry and the public regarding their obligations [with regards to countering proliferation]."[13]

Most national authorities have undertaken to establish a range of voluntary commitments in support of nonproliferation norms and goals, either as members of export control regimes or as subscribers to the principles of the export control regimes, which commit the state to:

- Incorporate the regime's export control list into national legislation;
- Set licensing criteria for certain sensitive goods; and
- Share denial notifications with partner countries.

National authorities are the lead actors in implementing supply-side controls, and the international community holds the governments of each jurisdiction to account for activities that occur within their territory. Nonetheless, this approach to implementing supply-side controls is based upon two potential fallacies. First, that national authorities can control their private sector; in reality, national authorities can often only influence the action of entities operating within their territories. The

12 Douglas M. Stinnett, Bryan R. Early, Cale Horne and Johannes Karreth, "Complying by Denying: Explaining Why States Develop Nonproliferation Export Controls," *International Studies Perspectives,* Vol. 12 No. 3 (August 2011), pp. 308-326.

13 UN Security Council, Security Council Resolution 1540 (2004)available at: http://www.un.org/Docs/journal/asp/ws.asp?m=S/RES/1540%282004%29

second potential fallacy is that compliance alone can limit proliferation; in reality, even if all firms remained compliant with the requirements of export control laws and sanctions, proliferation could continue through illicit procurement routes. Therefore, legal compliance with export controls and sanctions should be viewed primarily as a backstop for providing a minimum standard of resilience against proliferation.

Making and Enforcing Rules

There are numerous sources of rules that apply across society. In the commercial sphere, the three principal sources are laws adopted by governments and business contracts entered into with other parties and any internal rules set by the company's management team. Rules may also be enforced by multiple bodies with most laws enforced by governments, and most contracts enforced through civil (rather than criminal) enforcement mechanisms.

It is often the case that the rule-making body will also maintain a process to enforce compliance. However, it is also common to find that commercial or non-governmental organizations enable compliance through the provision of some form of service by, for example, setting a standard against which an organization's processes can be tested to demonstrate compliance.

Overall, rules can be set and enforced publically or privately and compliance can be verified via assurance or inspection.

In the context of export controls and sanctions, the UN is a rule-making body with no effective enforcement mandate. Responsibility for administering supply-side controls must instead lie with the licensing authority. Nonetheless, the concept of partnership implies shared responsibility rather than externalization of responsibility from one body to another. While it is right that government should be the licensing authority, many of the recommendations made in this paper could be implemented either by the national authority or third parties. For example, training can be delivered by several parties in line with standards set by governments.

Enabling Implementation

Strategic engagement of the private sector in countering proliferation requires the development of partnerships between governments and businesses. At the practical level such partnerships should be supported by the provision of a range of tools, services, and guidance materials. For example, firms operating in sectors affected by trade controls and sanctions must have in place compliance systems if legal obligations are to be met. Consequently, provision of guidance on compliance can also be considered a prerequisite.

Nonetheless, even when a firm has set up a compliance system, it will still need to be supported by ensuring access to the following:

- Compliance Guidance
- Supporting Services
- Information Exchange
- Certification/kite marking

Each of these services is explored in the sections that follow.

Compliance Guidance

Companies engaging in the trade of strategic goods, or in business that could fall within the scope of multilateral or unilateral sanctions or export controls, should take a systematic approach to compliance. Systems implemented by private sector entities should both ensure compliance with the law and prevent proliferation. One way to achieve this goal is to develop systems based on best-practice compliance standards.

Such an approach is necessary not only for exporters and manufacturers, but also for insurance firms, finance firms, shipping firms, and freight forwarding firms. Many firms build upon the guidance of their national authority. In the U.K., for example, 70 percent of respondents to a survey of British firms in 2011 indicated that they implement the BIS export compliance code of practice.[10]

A particular challenge brought about by the structure of intra-governmental responsibilities is that in most countries trade compliance is a function that is often fragmented and split across government departments. Typically, the treasury or finance department deals with financial sanctions while the trade or business department deals with export controls and technology sanctions. Guidance for the private sector promulgated by one department is often produced in isolation from the requirements set out by other departments. Another challenge is that governments typically produce guidance on compliance using legal requirements rather than requirements based on countering proliferation. As compliance is not sufficient to counter proliferation, implementing the guidance alone is often insufficient for preventing the company's products or services from being used in a program of concern.

Recommendations

R3. National authorities should endorse or adopt a best-practice compliance standard for each affected business sector, and ensure that this standard is linked to compliance-related training.

R4. National authorities should develop or endorse guidance materials on identifying illicit procurement (red flag guidance).

Outreach

While ignorance is no excuse for breaking the law, awareness of export control laws cannot be assumed, particularly where controls extend to dual-use and intangible technologies with no obvious WMD application, or enabling services that would otherwise be benign. National authorities thus have a responsibility to ensure that outreach activities are undertaken on a regular basis. This activity should not be limited to exporting and manufacturing firms and should also focus on firms operating in the finance, insurance, shipping, and fast freight forwarding sectors.

Outreach work conducted by Project Alpha highlights that, where practical, it should be undertaken on a sector-specific basis, with content tailored to suit each business sector. Another lesson is that outreach should not focus solely on export controls but encompass other elements of supply-side controls such as sanctions. It is notable that in many national authorities there are different groups responsible for implementing export controls and sanctions and, therefore, there is often a need to

coordinate outreach in a cross-governmental way. Alpha's proliferation briefs may provide a template for sector-specific outreach events.[14]

Recommendations

R5: National authorities should conduct sector-specific trade compliance outreach

R6: National authorities should develop or endorse a compliance competence framework

R7: National authorities should develop or endorse sector-specific compliance training against a compliance competence framework, taking advantage of E-learning where possible and recognizing that the sharing of experience is invaluable

R8: National authorities should develop or endorse a compliance official's certification program

Compliance Training

Implementation of compliance in the private sector requires a cadre of trained and experienced personnel. Creating this cadre requires a structured approach to training. National authorities should facilitate this approach by creating or recognizing a compliance competence framework against which training can be set and from which certification exam questions could also be derived. Training can be delivered either by the national authority or by a suitably-qualified official in either the public or private sector. The aim should be for all compliance professionals to be certified as practitioners. In Japan, for example, almost 13,000 individuals have been certified in this way.

Supporting Services

Ratings advice

While firms can "self-rate" their technology against control lists, this requires trained and experienced personnel that may not be available in every company. Therefore, exporters should have access to services that can advise them on whether the product or technology is subject to control or is otherwise proliferation-sensitive. Ratings advisory services are offered at present by both national authorities and by some consultancy services. National authority provision is usually free, but this free provision may impede the full development of market-driven advisory services.

Ratings advice often has to combine information on the goods with information on destination or end use, and such services should be able to answer questions both about control status and about end-use sensitivity. National authorities can also do more to define the conditions under which trade could be considered proliferation-related. For example, could the export of structural materials for underground facilities fall within the scope of the controls when the country is known to use such facilities to house clandestine elements of a nuclear program?

A survey of 52 compliance officials in British firms in 2011 revealed that 92 percent of firms would use the BIS ratings service under certain circumstances, with 14 percent using ratings services to

14 See http://kcl.ac.uk/alpha

determine the control status (a further 32 percent use information provided via the BIS website).

Recommendations

R9: National authorities should make available a ratings service through which exporters can check both the control status of their products and whether the technologies, even if uncontrolled, could contribute to programs of concern.

R10: National authorities should develop or endorse category listings of goods that, even if uncontrolled, could pose proliferation concerns so that firms can apply additional vigilance.

R11. National authorities should set out the scope of WMD programs for the purposes of export licensing. (Could the scope include ancillary services in a building used to house WMD, for example?)

Information Exchange

In addition to the provision of compliance guidance, firms also need to be kept up-to-date on proliferation risks in order to counter illicit procurement. Information on the following is essential:

- Which countries currently pose a proliferation risk?
- What technologies are currently being sought by proliferators?
- What entities are currently involved in illicit procurement?
- What red flags should firms look for when conducting due diligence?

National authorities may find it difficult to provide such information to the private sector for fear of causing offense to another country's government or compromising valuable intelligence. Solutions to these challenges include confidential briefings to industry and the use of independent, but informed, third parties.

The private sector is well-placed to identify illicit procurement attempts because of its knowledge both of the market and of the technology. National authorities must capitalize on this information by making it possible for the private sector to share such information either with the government itself or with others in the private sector.[15]

Recommendations

R12: National authorities should create or develop routes through which suspicious enquiries may be shared.

There are numerous routes through which suspicious enquires can be collated by the national authority, including through the licensing authority, through enforcement authorities, through intelligence services or through independent third parties.

R13: National authorities should provide to their private sector consolidated lists of all entities with which trade requires special consideration, including entities

15 The role of the private sector in sharing such information is discussed in the sections that follow.

designated by international or unilateral sanctions together with sector-specific guidance on how to ensure compliance.

R14: National authorities should publish export licensing statistics and outcomes.

R15: National authorities should develop or endorse mechanisms through which the private sector can share suspicious enquiries, tips, and concerns with both national authorities and others in the business sector, using third parties as necessary.

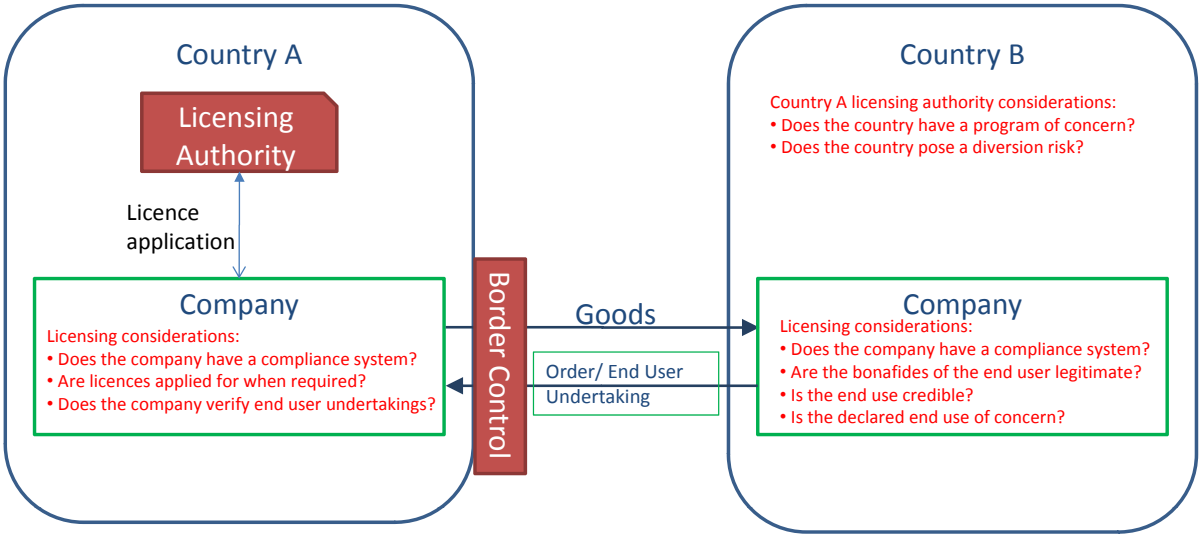
Compliance Certification

Trade can aid proliferation in the following circumstances: 1) when the end user is involved with activities of concern directly, or 2) when the end user will assist an entity involved with activities of concern, either by re-transferring goods or by providing enabling services. Differentiating risk in this way highlights the possible uses of compliance certification. Verification of a business's credentials and/or compliance system by a third party could increase the confidence that the goods would not be either misused or diverted provided that:

- Driven by a compliance system exporters submit licenses when appropriate and do not attempt to deceive the national authority;
- The party verifying the end user's credentials is credible
- The end user's country is not of direct proliferation concern;
- The end user's country has in place an effective export control system; and
- The end user has in place a compliance system that would prevent the further export of the goods without first referring to the national authority's export controls.

A survey of 52 British firms in 2011 revealed that 48 percent of respondents would advocate accreditation of the company's compliance system if it eased the licensing requirement when

Figure 1. Showing the role of certification in supporting export licensing decisions



shipping to known customers. A further 23 percent were motivated by quicker licenses and 15 percent if exports to overseas subsidiaries did not require licenses. Moreover, 60 percent of the respondents conduct internal audits of their compliance systems and 21 percent use both internal and external compliance audits.

The introduction of end user certification of any kind would require both an international agreement regarding the objectives of such a system and a sustained investment by firms wishing to trade in strategic technologies.

Recommendations

R16: All parties should work collaboratively to develop international standards for trade compliance.

R17: National authorities should include an optional provision for certification in licensing assessments and with regards to open licensing.

R18: Firms should encourage business partners to undergo certification when trading in proliferation-sensitive technology or services.

Accreditation of Consultants and Trainers

Market provision of compliance accreditation, training, and outreach is a credible option that can be facilitated by national authorities. Market-based providers of public goods, however, may operate with an explicit or implicit delegated authority from the national authority, regardless of legal liability, and it may be desirable for providers to be trained to the standards endorsed by the national authority.

Recommendations

R19: National authorities should implement a certification program targeted at compliance consultancies and training providers. If a national authority does not itself intend to carry out accreditation, this responsibility may be delegated to an appropriate independent agency.

Toward Integrated Compliance

Based upon the a recognition that compliance is not sufficient to prevent proliferation, this paper has set out the measures required to prevent the internationally-dispersed private sector from being used to sustain proliferation. The recommendations set out in the paper are neither overly-burdensome nor impractical. Nevertheless, those setting and enforcing controls have an obligation to make adherence as simple as possible.

Recognizing that economic globalization poses a challenge to the effectiveness of supply-side controls, this section investigates whether another aspect of globalization, namely the availability of ever more integrated information, can aid nonproliferation efforts.

Information Fusion

Spotting illicit trade requires a detailed review of a proposed transaction both against pre-set nonproliferation criteria and the confirmation of the *bona fides* of the parties involved. While the national authority is legally responsible for both, businesses already conduct elements of both as part of an internal due-diligence process.

When conducting due diligence it is necessary to know *who* wants *which* goods and *why*. Guidance on implementing due diligence is available on the Alpha webpage - kcl.ac.uk/alpha).

Information fusion allows each of these questions to be addressed automatically or semi-automatically. Data supplied by a potential customer such as a firm's name, address, telephone number and business sector can be cross-referenced and verified through web 2.0 services when interlinked with information held in the deep web, such as telephone and business directories, maps, and business intelligence.

Project Alpha is investigating the use of information fusion techniques for use in due diligence with the aim of launching a test application by early 2013. National authorities should embrace such innovation: much of the information currently required for due diligence is either not made available by national authorities or is not released in suitable formats. By making such information available in suitable formats for anytime, anywhere access by business users, the efficiency of compliance frameworks will be greatly enhanced.

Recommendations

R20: National authorities should embrace information fusion and share licensing refusals or outcomes (including recipient name, country, control entry/type of trade, and grounds for refusal) in a suitable format for anytime, anywhere user access.

Partnerships in Practice: Third-party Facilitators

This report has highlighted the need for partnerships between national authorities and the private sector to combat proliferation and it has set out recommendations for specific measures that both governments and firms should implement in order to ensure that illicit trade is prevented. This final substantive section of the report explores whether there is a role for third parties in facilitating such partnerships by delivering upon the recommendations set out elsewhere in this report.

As export licensing decisions must take account of both a state's foreign policy priorities and sensitive

information on potential end uses, they are, rightly, available only to governments. Therefore, national authorities must continue to be the ultimate competent authority to issue licenses for the export of military and dual use technologies.

But there is a range of services associated with the export licensing process that could be implemented either by the national authority or by competent designated entities operating under the accreditation of the national authority. These services are outlined in the table below, where current / possible service providers are also identified.

	Government provision (U.K.)	Market provision	Private-sector self-provision	Possible NGO-provision?	Comment
Licensing decisions	All	None	None	None	Sole competence of national authority
Technical ratings	Most	Some	Some	Yes	Only government has legal authority
Exportability meetings	Rarely undertaken	Nil	Nil	Yes	Constrained by resources
End-use verification	None	None	None	Yes	Constrained by resources
Development of compliance systems	Ni	Few	Most	Yes	No set standards
Compliance auditing (and access to discretionary licensing)	All	Some	Some	Yes	No systematic approach other than for access to discretionary licensing
Compliance accreditation / kite-marking	None	None	None	Yes	No standards set
Training / outreach	Some	Some	Some	Yes	Several providers, but no standards
Accreditation of consultants and trainers	None	None	None	Yes	No standards set

In addition to consultancies and other commercially-driven suppliers of compliance-related services, there are two notable examples of projects that could be considered as third-party facilitators: CISTEC in Japan and Project Alpha in the U.K. While both were established to engage the private sector in countering proliferation, they are funded differently; Project Alpha is funded by government whereas CISTEC is funded by contributions from its members. Both of these projects are described below.

The CISTEC and Project Alpha case studies demonstrate that there is a credible role for third parties in facilitating the implementation of nonproliferation in the private sector. In particular, such organizations have the freedom to conduct activities that governments cannot: be it highlighting the proliferation risks posed by certain countries or representing the views of participating companies in relation to trade control issues.

Center for Information on Security Trade Control (CISTEC)

CISTEC was created in 1989 as a non-profit, non-governmental organisation to work with the private sector in implementing export controls. CISTEC has evolved to become a champion and partner for industry, but this has corresponded with a decrease in closeness to government. The organization has an annual budget of $6m per year which is entirely covered by industries contributions. This budget covers a staff of around 40 people, offers a full suite of ancillary services for export licensing, including ratings, training, certification, and consultancy.

CISTEC's establishment was driven by the recognized need to develop a compliance culture in Japanese industry following the Toshiba export of machine tools Russia, tools that subsequently were used to improve Russia's submarine propeller production capabilities. The organisation was originally heavily staffed by government (METI) personnel, and grew to be funded almost entirely be industry.

CISTEC has two primary roles: 1) promote export compliance, and 2) representing industry

1. Promoting export compliance
    - Individual consultations, including on control status and similar
    - Compliance programs, including maintain guidance and advising individual firms on its implementation
    - Seminars, training, etc
    - Publication of goods' control status at company's behest.
    - Other knowledge transfer services, such as journal publications, articles on current issues etc.

    The organization has no official status as a provider of export licensing information, and advice given by CISTEC could, in theory at least, differ from that given by METI.

    CISTEC focuses solely on strategic export controls for dual-use goods, but this role may expand to cover military goods following the decision by the Japanese government to allow military-related exports.
2. Representing industry
    - Seek harmonization of export controls worldwide and promoting Japanese firm's export interests to METI and the international community.

As a not-for-profit organisation, CISTEC is also able to conduct outreach activities both within Japan and internationally to spread best practice and promote CISTEC's values. This includes holding regional export compliance workshops and conducting outreach to SMEs within Japan.

Membership: With around 370 member-companies, CISTEC representatives claim their membership includes all major Japanese exporters of dual-use technologies. Nonetheless, one identified "challenge" of CISTEC is to engage SME's, suggesting that coverage is not complete. Expansion of SME membership would likely result in an increased use of CISTEC's services, however, as the current membership, which consists mainly of large firms with well-established compliance system, rarely need to consult with CISTEC.

CISTEC is also working to expand its relationships with academia and SMEs. While university membership of CISTEC has expanded in recent years, it is not yet clear what universities desire or will gain from membership.

Seminar series: 34 seminars per year (25 general export compliance seminars per year, 9 events on laws and regulations)

Professionals training and certification program: 12,483 holders of "associate" status, 147 of "legal expert" status, and 285 of "expert" status.

Relationship with Government: METI, the Japanese equivalent of BIS, continues to have an export controls staff of around 80 people and collectively process some 18,000 licences. CISTEC holds no official position in the Japanese compliance system, but does provide a forum through which to government and industry can share views and information on export controls

Project Alpha

Project Alpha was created in 2011 in the Centre for Science and Security Studies of King's College London for the purpose of proactively engaging the private sector in countering proliferation. The project works to improve and inform implementation of export compliance in individual firms and to make supply chains more resilient to illicit trade. The project acts as an independent third party facilitator, providing a route through which firms can be informed about proliferation risks and compliance requirements and through which the governments can access information from the private sector on suspicious enquires and technologies. The project is funded by the British government but operates independently.

Guidance Materials & Training: Project Alpha works to provide information on countering proliferation to industry. This is achieved through the project's website (kcl.ac.uk/alpha), which contains compliance guidance, proliferation briefs, country briefs, and other materials. The project also runs sector-specific compliance seminars for those sectors that can be affected by trade controls.

Partners Against Proliferation: Project Alpha launched a "Partners Against Proliferation" initiative in summer 2012 through which firms undertake to implement compliance systems that could counter proliferation risk. Firms receive a range of benefits for doing so, including the support of the Project Alpha project team, training, and access to certain tools. The main benefit for firms, however, is the ability to demonstrate to pontifical customers and suppliers that they take compliance responsibilities seriously; this is particularly important for the manufacturers of high-tech materials and equipment, which often wish to supply these technologies to the defense, aerospace, or government sectors.

Project Alpha Screening System: Looking to the future, Project Alpha is developing a system that will allow firms to screen potential customers for proliferation concerns. Current commercially-available systems are available to screen entities against the various designated entity lists, but the costs of accessing these systems can be prohibitive. To encourage use, the PASS system will be available for free.

Conclusion

National authorities are responsible to the international community for implementing export controls and sanctions, and they must adopt measures and enforce laws to do so. While often overlooked, it is the private sector that must make operable the requirements of export controls and sanctions. To enable the private sector to do this, national authorities should make a range of information and services available, in the absence of which the private sector cannot reasonably be expected to comply.

National authorities should:

1. **Facilitate the development of partnerships with the private sector;**
2. **Set out for the insurance, exporting, finance, and insurance industries what measures should be implemented in order to counter proliferation, including defining the scope of WMD programs as relevant for the industry sector.;**
3. **Endorse or adopt best-practice compliance standards for each affected business sector, and to ensure that it links to compliance-related training;**
4. **Develop or endorse guidance materials on identifying illicit procurement (red-flag guidance);**
5. **Conduct sector-specific trade compliance outreach;**

6. **Develop or endorse a compliance competence framework;**
7. **Develop or endorse sector-specific compliance training against a compliance competence framework, taking advantage or E-learning where possible and recognizing that the sharing of experience is invaluable;**
8. **Develop or endorse a compliance official's certification program;**
9. **Make available a ratings service through which exporters can check both the control status of their products and whether the technologies, even if uncontrolled, could contribute to programs of concern;**
10. **Develop or endorse category listings of goods that, even if uncontrolled, could pose proliferation concerns so that firms can apply additional vigilance;**
11. **Set out the scope of WMD programs for the purposes of export licensing (could the scope include ancillary services in a building used to house WMD, for example?);**
12. **Create or develop routes through which suspicious enquiries may be shared;**
13. **Provide to the private sector consolidated lists of all entities with which trade requires special consideration, including entities designated by international or unilateral sanctions together with sector-specific guidance on how to ensure compliance;**
14. **Publish export licensing statistics and outcomes;**
15. **Develop or endorse mechanisms through which the private sector can share suspicious enquiries, tips, and concerns with both national authorities and others in the business sector, using third parties as necessary;**
16. **Support the development of international standards for trade compliance;**
17. **Include an optional provision for certification in licensing assessments and with regards to open licensing;**
18. **Encourage business partners to undergo certification when trading in proliferation-sensitive technology or services**
19. **Implement a certification program targeted at compliance consultants and trainers.**
20. **Embrace information fusion and share licensing refusals or outcomes (including recipient name, country, control entry/type of trade, and grounds for refusal) in a suitable format; and**
21. **Facilitate the creation of third-party facilitators to convey proliferation risks to take forward the partnership model espoused in this paper.**

The private sector also has a role to play in countering proliferation that goes beyond compliance with the law. The necessary measures are summarized in Appendix 1. For a variety of reasons, it can be expected that firms will adopt many of these anti-proliferation measures, but national authorities or third parties have a role to play in promoting the adoption and setting of best practices.

KING'S College LONDON

Centre for Science & Security Studies

Appendix: Partners Against Proliferation

Project Alpha

Partners Against Proliferation

alpha@kcl.ac.uk

kcl.ac.uk/alpha

Project Alpha is a government-sponsored project that works to assist the private sector in implementing trade controls and in avoiding involvement with proliferation-related trade. Firms should also refer to Project Alpha's website where sector-specific guidance on implementing export compliance measures can be found. The website also contains the latest information on illicit procurement attempts to aid firms in implementing the measures detailed above.

Background: The private sector has an important role to play in preventing illicit trade in technologies or services that are used to sustain Weapons of Mass Destruction programs in countries. Firms are obliged to comply with the laws of the territories in which they operate – laws that include the requirements of UN Security Council Sanctions imposed on countries such as Iran. But given the illicit routes through which countries like Iran circumvent sanctions to acquire technology and services from the international marketplace, manufacturers, exporters, insurance, finance and shipping firms should take extra measures to ensure they do not inadvertently aid sanctions-busting activity.

Partners Against Proliferation: Partners of Project Alpha are those firms that work to counter proliferation by implementing best-practice trade compliance systems. Partners are asked to assist in steering Project Alpha via the Industry Steering Board, which meets quarterly. Partners undertake to implement the measures that follow and to actively encourage those in their supply chain to do the same.

Partners will:

- Maintain a trade compliance system that initiates appropriate action when:
    - The technology to be exported is controlled;
    - The exporter knows, suspects, or has been informed that the export is destined for a WMD program; or
    - A party to the export is a designated entity.

Partners undertake to:

- Implement a compliance system based on sector-specific best practices that is integrated with the company's Corporate Social Responsibility framework;
- Ensure that key business partners, including distributors, subsidiaries, and agents, implement best-practice compliance systems;
- Conduct background checks on customers using open source material and terminate business deals with entities of proliferation concern;

- Develop and implement corporate monitoring and detection systems to identify illicit procurement attempts for proliferation-sensitive goods;
- Share suspicious enquires and counter actions with government agencies and the private sector (through Project Alpha, if necessary);
- Emphasize adherence to non-proliferation with business partners and through the firm's website;
- Train all relevant staff against a trade compliance competence framework;
- Implement measures to protect the intangible technology (such as design information) associated with proliferation-sensitive goods or processes.

Firms should also refer to Project Alpha's website where sector-specific guidance on implementing export compliance can be found. The website also contains the latest information on illicit procurement attempts to aid firms in implementing the measures detailed above.

About Project Alpha

Project Alpha at King's College London acts to build supply chains that are resilient to proliferation. Alpha provides information, guidance, and training on proliferation and export controls issues for industry. Alpha recently launched a "Partners Against Proliferation" initiative in which Project Alpha helps firms adopt the measures set out in the appendix. Interested parties can find out more about Project Alpha by visiting the project's webpage: www.kcl.ac.uk/alpha

About the Project on Managing the Atom

The Project on Managing the Atom (MTA) is the Harvard Kennedy School's principal research group on nuclear policy issues. Established in 1996, the purpose of the MTA project is to provide leadership in advancing policy-relevant ideas and analysis for reducing the risks from nuclear and radiological terrorism; stopping nuclear proliferation and reducing nuclear arsenals; lowering the barriers to safe, secure, and peaceful nuclear-energy use; and addressing the connections among these problems. Through its fellows program, the MTA project also helps to prepare the next generation of leaders for work on nuclear policy problems. The MTA project provides its research, analysis, and commentary to policy makers, scholars, journalists, and the public.

Project on Managing the Atom
Belfer Center for Science and International Affairs
Harvard Kennedy School
79 JFK Street; Mailbox 134
Cambridge, MA 02138
Phone: 617-495-4219
E-mail: atom@harvard.edu

Website: http://managingtheatom.org

Project on Managing the Atom
Belfer Center for Science and International Affairs
Harvard Kennedy School
79 JFK Street; Malbox 134
Cambridge, MA 02138
Phone: 617-495-4219
Email: atom@harvard.edu
Website: http://managingtheatom.org