International Journal of Nuclear Security

Volume 1 | Number 1 Article 6

7-9-2015

Calling All Actors: A holistic framework for tackling supply-side proliferation

Christopher Hobbs
King's College London, United Kingdom

Elisabeth Young
King's College London

Calling All Actors: A holistic framework for tackling supply-side proliferation

Cover Page Footnote

We acknowledge the support of Daniel Salisbury in proof reading and fact checking our manuscript.

International Journal of Nuclear Security, Vol.1, No. 1, 2015

Calling All Actors: A holistic framework for tackling supply-side proliferation

Dr. Christopher Hobbs
King's College, London, United Kingdom

Elisabeth Young
King's College, London, United Kingdom

Abstract
This article proposes a new holistic framework for tackling supply-side proliferation, based on a mix of punishments, incentives, and new normative standards (PIN) that could be taken by industry. After outlining a brief history of illicit nuclear trade, highlighting the increasingly sophisticated strategies adopted by proliferators, we explore in detail the PIN framework. We argue that to meet this challenge, industry must adopt behavior that goes beyond compliance with current regulations, particularly in the area of due diligence and information sharing.

I. Introduction
Since the dawn of the atomic age, the spread of nuclear weapons and their associated delivery systems has been at the forefront of the international security agenda. Originally perceived as a state-level issue, the exposure of the A.Q. Khan procurement network in 2004 vividly highlighted the role that non-state actors, the private sector, and in particular dual-use industries can play in facilitating nuclear proliferation. Here there have been multiple examples where states lacking indigenous resources or expertise have sought to obtain materials and equipment from the global marketplace in order to advance weapons programs. In response to this challenge, the international community has developed a system of supply-side controls, aimed at restricting the transnational movement of such goods. While these state-enforced measures have, arguably, served to slow the rate of proliferation, they are far from watertight, with their provisions varying from country to country and with determined actors employing ever more elaborate schemes to circumvent them.

As a consequence, attention has turned to whether the private sector could play a more proactive role in helping curb proliferation activities. This article aims to contribute to this discussion by outlining a new holistic framework of punitive actions, incentives, and new normative standards (PIN) for industry engagement in non-proliferation efforts, drawing on interviews with practitioners, theories of corporate social responsibility, and lessons from other industries

After providing a brief history of illicit nuclear trade, intended to highlight evolving challenges to the export control regime, we will explore in detail the proposed PIN framework. Here we will argue that in order to tackle increasingly sophisticated proliferation efforts, firms must adopt measures for due diligence and information sharing that go further than what is required under existing national legislation. This beyond-compliance behavior, currently exhibited by only a small number of firms, should be promulgated across relevant industries. Here a bottom-up

approach is likely to be most effective, in which industry champions and other relevant bodies promote the non-proliferation benefits of "beyond compliance" in tandem with its economic advantages.

II. A brief history of illicit nuclear trade and export controls

International efforts to reduce the risk of imported nuclear materials and technologies being used in weapons programs can be traced back to the establishment in 1971 of the Zangger Committee, a small group of states tasked with exploring the implementation of Article III.2 of the recently ratified Non-Proliferation Treaty (NPT), which had entered into force in 1970. In 1974 the Zangger Committee published the first "trigger" list of sensitive materials and equipment, whose export to nuclear weapons states not party to the NPT would require the application of IAEA safeguards **[*1*]**. That same year, India conducted its first nuclear weapons tests, using plutonium diverted from a Canadian-supplied research reactor, dramatically demonstrating how imported civil nuclear technology could be misused **[*2*]**. In reaction to this, the most prominent nuclear supplier states came together to form the Nuclear Suppliers Group (NSG), an informal body focused on reducing proliferation by controlling the export and re-transfer of nuclear materials and technologies, who published their first guidelines in 1978 **[*3*]**. Similar in spirit to the Zangger Committee, the NSG crucially included a number of states that – at the time – were non-NPT member states and required the application of controls on transfers to all non-nuclear weapons states, including parties to the NPT.

Broader in scope than the Zangger Committee, the NSG was not without weaknesses. Focusing initially on nuclear-specific items, its guidelines did not cover "dual-use" materials and technologies that, although not necessarily directly nuclear-relevant could be used in a weapons program. This gap was recognized by proliferators, with states seeking nuclear weapons now trying to buy nuclear-related technologies piecemeal – targeting dual-use items that were not addressed by the NPT or NSG at the time, and whose ultimate use was ambiguous. In the case of South Africa, materials and technology sourced from multiple states were used to produce seven nuclear weapons in the 1980s, which were ultimately dismantled **[*4*]**. However, it was the discovery of a covert nuclear weapons program in Iraq in the early 1990s, which used imported technology, that galvanized international action. In an effort to close this gap, the NSG developed and published in 1992 a new list of guidelines for the transfer of dual-use materials, equipment, software, and other technologies **[*5*]**.

The NSG, while it has adapted somewhat to a changing security environment, remains hamstrung by its status as a voluntary group, with states retaining the ultimate say in how its guidelines and control lists are implemented within their national laws. For example, evidence suggests that export control measures vary significantly from state to state in terms of punitive actions, enforcement, and level of regulation **[*6*][*7*]**. This enables proliferators to selectively choose procurement targets and pathways where they are less likely to get caught. Furthermore, while NSG control lists are typically updated every few years to take into account technological progress, proliferators have sought to target materials and equipment before they appear on the lists, and also to seek those sub-threshold items with properties that fall just outside of documented specifications. These weaknesses were highlighted by the activities of A.Q. Khan, an eminent scientist within Pakistan's nuclear weapons program. In the 1990s and 2000s, Khan established an international black market through which states—including Libya, Iran, and North Korea—bought a wide range of nuclear technology **[*2*]**. These were sourced from multiple companies, operating in more than ten states, with Khan using a system of front companies and transhipment hubs to obscure the ultimate destination of the various items.**[*2*]** The extent of this

black market became apparent in the early 2000s, culminating in Khan's 2004 confession to selling nuclear secrets to the three aforementioned states **[*2*][*8*]**.

In the wake of the exposure of Khan's network — and a post-9/11 increase in fears of nuclear terrorism — the UN Security Council unanimously adopted Resolution 1540 **[*9*]** in April 2004. This resolution, which focuses on minimizing the potential role that non-state actors are able to play in WMD proliferation, calls on "all States to take additional effective measures to prevent the proliferation of nuclear, chemical or biological weapons and their means of delivery"**[*9*]**. In contrast to the NSG and the other WMD-related multilateral export control regimes, such as the Missile Technology Control Regime (MTCR) and Australia Group, UNSCR 1540, passed under Chapter VII of the UN Charter, is legally binding. Consequently it requires, alongside other security measures, that governments put in place appropriate border, export, and transhipment controls. This universality was a crucial step in putting the international export control regime on a more formal and—hopefully with time—a more level footing, although the implementation of 1540 remains hindered due to a number of factors, primarily because there is no mechanism for gauging and ensuring states' compliance. While legally binding, the mandate of the 1540 Committee, established to oversee the Resolution's implementation, is weak. It contains no provisions for verification or for enforcement. Instead, the Committee has to rely on voluntary self-reporting by states, which is often conducted inconsistently.

III. Export control challenges: Widening gaps and sophisticated procurement strategies

Although UNSCR 1540 requires that states put export controls in place, and other initiatives such as the NSG have helped improve harmonization across states, national regulations, control lists, licensing criteria, and enforcement activities remain far from uniform. As was the case during the time of A.Q. Khan's network, proliferators continue seeking to exploit weak points in this web, trying to get items directly from, or to tranship them through, states with weaker export controls, where they are less likely to get caught **[*10*]**. Unfortunately, the vulnerability posed by these gaps is liable to increase in the near future due to the ever-growing internationalization of supply chains and the wider availability of dual-use goods. At present, developed nuclear states with relatively strong export controls harbor the bulk of higher-quality nuclear and missile-related manufacturing capabilities. However, this situation is changing as manufacturing sectors in developing countries grow and increase in sophistication **[*11*]**. A prime concern here is the explosion of the dual-use manufacturing sector in China, increasingly capable of manufacturing commodities, which were previously the preserve of the state-owned enterprise. UNSCR 1540 recognizes this challenge, calling on well-resourced states to assist others—although deference to state sovereignty means that this is provided only to those that ask for it.

Proliferators have also tried to get around export control regimes by targeting non-listed items, for which export control obligations are far less straightforward. In order to combat this, states have put in place systems of end-use controls, requiring firms to contact the relevant export licensing organization if they know or suspect that their export would be used in a WMD program (NSG 1). Although this is a logical step in tackling an undefined set of potentially relevant items, to be effective it requires that industry be able to distinguish a proliferation-related activity from a legitimate request. This is especially necessary when considering goods that fall below the control threshold, but could be of use in a weapons program. In this situation, companies are not obliged to apply for an export license if they do not believe the goods are destined for a WMD program, meaning that government authorities are not always afforded the opportunity to assess the risk of the license application. Distinguishing these suspicious enquiries from bonafide trade is a far from simple task, with evidence suggesting that proliferators are becoming increasingly deceptive

in their procurement efforts, making it harder to identify such actions. Consider for example the recent case of Chinese proliferator Li Fang Wei, who dealt in dual use missile-related goods, and who is believed to have used at least 13 company names and eight aliases in his procurement efforts **[*12*]**.

IV. Efforts to engage industry

With international action in this area limited by state sovereignty, and with proliferators adopting sophisticated procurement strategies that are challenging to identify even by complying with the most robust of national export controls, it is necessary to consider what additional measures could be undertaken by industry to combat this threat. Studies in this area can be traced back to the early 1990s, in reaction to the unveiling of Iraq's nuclear weapons program **[*13*]**. The need for industry engagement is also captured by UNSCR 1540, which requires states to "develop appropriate ways to work with and inform industry and the public regarding the obligations"**[*14*]**. Industry outreach has been taken up in the context of UNSCR 1540 via the so-called Wiesbaden process, which in 2012 held the first international industry-focused conference on the resolution's implementation **[*15*]**. Other sub-regional events targeted at different sectors have followed this, initiated by countries including the US, Japan, Germany, and the UK **[*16*]**. While in 2013, the NSG published a code of good practice for industry outlining eight non-proliferation-related internal actions that firms could employ **[*17*]**.

These international, regional, and national activities have served to improve awareness within industry of proliferation issues, although studies indicate that there is still considerable work to be done, particularly in engaging small medium enterprises (SMEs) **[*18*]**. A study by the UK's Department for Business, Innovation & Skills **[*19*]** of more than 500 industry firms found that the general understanding of export controls was significantly lower within SMEs than within larger firms **[*19*]**. Anecdotal evidence indicates that the majority of these smaller firms are not active members of major trade associations, through which non-proliferation guidelines and events are propagated **[*20*, *21*]**. Efforts are further complicated by a lack of understanding about what categories of firms in different sectors manufacture dual-use items. Mapping the dual-use industry would enable more targeted outreach, which at present can be implemented only at the sector level.

V. A holistic PIN framework for tackling supply-side proliferation

Studies into combating supply-side proliferation have tended to focus on individual initiatives or particular approaches, but without considering them in combination. But we must consider a range of strategies and their linkages, and discuss how it is necessary to employ them together in order to shift firms' behavior in this area towards ownership of non-proliferation. Here it is instructive to consider the "ladder of involvement" developed by Roper *et al*. for categorizing the engagement of employees in security programs **[*22*]**. This ladder has "rungs" of behavior, which from bottom to top are: subversion; avoidance; apathy; compliance; participation; and ownership. In this formulation, compliance can be reached through top-down measures including a combination of punishments and incentives, provided in this context by national authorities. However, to reach participation and ultimately ownership, it is necessary to consider how best to grow, within industry itself, broader normative standards—which go beyond what is required under national legislation.

In exploring how firms might climb Roper's ladder to reach ownership of supply-side proliferation, we use concepts from theories of corporate social responsibility (CSR), stakeholder

engagement, and industry regulation. Because self-regulation approaches to supply-side proliferation are still at their early stages of implementation, we draw parallels with initiatives in other sectors in order to demonstrate how these might apply in practice.

Punitive actions to ensure compliance

When exploring punishments that can serve to influence behavior it is important to include both "formal" and "informal" penalties, the former of which might include fines or imprisonment levied by states, and the latter reputational damage. In the commercial context, these must be considered alongside other relevant drivers, in particular the desire to maximize profits. The effects of these on the decision-making calculus of firms would constitute a cost-benefit conception of compliance drivers.

Most countries have export control legislation in place that authorizes the application of punitive measures against non-compliant firms. Some of these approaches to potential punitive measures are more stringent than others. The US implements by far the most severe penalties, and has in the past fined companies millions of dollars for felonies related to export control **[*23*]**. The US has also imposed significant financial penalty on non-US companies through extra-territorial sanctions, which prevent firms from accessing US markets. In other countries— such as the UK—penalties are seen less frequently and when they occur are of much lower severity.

However, in broad terms, and across the world, it would appear that the scope of these measures is far from well understood within the commercial sector (besides those firms already subject to penalties), particularly by small medium enterprises (SMEs). Relevant trade industries and government departments have undertaken some scoping work in this area, which in turn has served to highlight the extent of this problem. In a 2013 survey carried out by ADS Group—a leading trade association for the UK's aerospace, defense, security, and space sectors—responders from SMEs clearly indicated that they did not appreciate the costs of non-compliance with export control. In the previously cited BIS study, more than half the surveyed firms claimed that the key barrier to understanding dual-use controls was a perceived lack of relevance **[*19*]**. Other accounts indicate that firms have tended to consider export control issues only retrospectively, once an incident had occurred **[*21*, *24*]**.

Consequently, there is a need to more widely publicize export controls issues with a particular focus on formal punishments levied on non-compliant firms and on the wider informal costs. Here there are a number of case studies that could be used. One such high-profile example is Oerlikon Leybold, a German supplier of dual-use vacuum machinery, whose technology was found by IAEA inspectors at Iraq's nuclear sites in the early 1990s. As a consequence, Leybold suffered massive reputation damage and the loss of major contracts in both Japan and the US **[*4*]**.

It is also important that punishments be perceived as credible—i.e. they will be enforced—and severe enough to deter non-compliance. Otherwise a firm may understand what the law states, but may believe that they will get away with not adhering to it, or after carrying out a cost-benefit analysis may decide, for example, that it would be cheaper to pay a small fine for first-time noncompliance than to establish an internal compliance program. Here studies focused on the UK have indicated that firms themselves perceive the penalties for non-compliance as too low **[*19*]**. Other evidence suggests that serious punishments such as imprisonment are not regularly enforced **[*11*]**. On the flip side of the coin, costs of running compliance programs for SMEs may run into the thousands of pounds per year and result in lost business through rejection of suspicious orders **[*25*]**.

Consequently, there is a general need for stronger, more costly punitive measures and their greater enforcement. It is also important that these be applied proportionally, based on the nature of the offence and the behavior of the firm in question. To use Roper et al.'s ladder: we must punish offending members of industry proportionally, based upon whether they are subversive, avoidant, or apathetic. Fines, confiscation of assets, and loss of export privileges could be employed to tackle negligence-driven non-compliance, while imprisonment might serve to deter firms thinking about bypassing export controls. These penalties should also contain an element of flexibility, with leniency displayed to firms that voluntarily disclose instances of non-compliance.

Incentives used to encourage ownership

While punishments can change behavior, studies across a range of fields have shown that in isolation they are at best likely to achieve mere compliance **[*22*]**. To encourage participation and ownership, it is necessary also to consider incentives as part of a broader carrot-and-stick strategy. As was the case with punishments, these can be either formal or informal in nature, ranging from "performance-conditioned obligations" to reputational benefits **[*26*]**. To date, relatively little consideration has been given to incentives, both by governments and industry, with most firms viewing export controls as a hoop that must be jumped through—and compliance an activity that will likely stunt business growth and profit as opposed to one that could have wider beneficial effects. That said, there are a small number of cases where firms have identified clear financial benefits resulting from their non-proliferation efforts.

In terms of formal approaches, export licensing is one area where incentives could be offered. Here the Wassenaar Arrangement in its 2011 "Best Practice Guidelines on Internal Compliance Programs for Dual-Use Goods and Technologies" have suggested that states should consider taking into account a firm's internal compliance programs when adjudicating export licenses, potentially making it a requirement for receiving a general license **[*27*]**. This is the case in France, where national legislation includes codified criteria for effective internal compliance programs against which firms are judged when applying for a license **[*28*]**. Related approaches might include a simplification and speeding up of the licensing process for firms judged to have effective internal compliance systems. This type of approach has been used in other sectors, for example in healthcare, where under the US Occupational Health and Safety Administration's (OSHA) Voluntary Protection Program (VPP), practices judged to maintain lower-than-average injury and illness rates have their OSHA inspections reduced **[*29*]**. However, streamlined procedures such as these bring with them the inherent risk that it may become easier for firms to cheat the system, making it essential that national authorities retain their ability to detect and punish incidences of non-compliance in such a setup.

The informal benefits of adhering to export controls have also been recognized by an increasing number of companies that have experienced increased trade and revenue as a result of their growing reputation in this area. According to Strong, firms with robust compliance programs often receive more orders, and can increase their prices to cover the costs of a compliance system because many customers are willing to pay more in exchange for the guarantee of a quick turnaround, trusting that their order won't be detained due to non-compliance with regulations **[*24*]**. That said, these benefits are likely to become significant only in the mid- to long-term and may result in a business downturn in the short term. In the case of Westcon Group, a multinational telecommunications distributor, the implementation of a new export control system at first resulted in the cancelling of millions of pounds worth of orders **[*30*]**. However, the new customers attracted as a result of the firm's increased reputation in this area gradually offset this. Over the past six years since its compliance program was implemented, the Westcon Group

estimates that it has attracted significantly more new business than it has had to turn away due to export control concerns **[*30*]**.

Beyond Compliance Behavior

With proliferators becoming increasingly deceptive in their efforts to acquire technology relevant to nuclear weapons, it is necessary to consider what additional steps firms might take to combat this threat, above what is currently required under national regulations. Kurzrok and Hund suggest seven possible options including: corporate governance statements; participation in an industry-wide code of conduct; preferential choosing of business partners; sharing suspicious trade requests; participating in government export control rulemaking; non-proliferation training for employees; and acknowledging incidences of noncompliance **[*31*]**. In what follows, we explore the potential benefits of some of these approaches with a focus on the utility of due diligence and information sharing.

In performing due diligence on potential transactions, industry must be on the alert for a range of warning signs that might indicate a suspicious order **[*32*]**. These can be related to customer, end-use, or destination and may include the following: a customer declines routine installation, maintenance and training; the product's capabilities and order size does not match its stated end-use; or the destination is a major transhipment hub. A combination of these and other indicators should trigger a further investigation to establish the legitimacy of a particular order, through the use of open sources or other means **[*33*]**. Due diligence processes can be enhanced through establishing an internal database of suspicious enquires, enabling firms to analyze historical trends and establish whether a particular order might be part of a broader proliferation strategy.

Rakon UK, a UK subsidiary of a New Zealand-owned electronics firm, manufactures frequency control products, e.g. quartz crystal oscillators, which can be applied in both GPS systems and for missile guidance. It has carried out due diligence checks for nearly a decade. Following an incident in 2005 where a Rakon product was believed to have been diverted from Switzerland to Iran's ballistic missile program, the company decided to establish a system for identifying red flags and storing information regarding possible suspicious orders **[*33*]**. Rakon's efforts include training for staff on export control regulations as well as on past cases of suspicious enquiries and how they have been identified. Potential customers are checked against national entity lists and vetted using open-source methods. Thanks to these processes, Rakon UK identified and rejected about 30 suspicious enquiries from 2005 to 2011 **[*34*]**.

The power of due diligence can be significantly enhanced through wider sharing of information. Here firms could pass data on suspicious enquiries to their competitors, supply-chains, and national governments. This would help establish a more comprehensive understanding of the proliferation threat, with analysts able to draw on information from multiple firms. Sharing of security-relevant data between companies is carried out in other industries—for example, in banking, where UK firms pass on incidences of fraud through the Fraud Intelligence Sharing System (FISS) **[*35*]**. When it comes to sharing procurement data, this can be as simple as forwarding an email inquiry. Unfortunately, at present this is not commonly done by the dual-use industry, with firms typically discarding information on an order they deem too suspicious to fill **[*12*]**. This can be partly attributed to a perceived risk that sharing such information would associate firms with illicit procurement, making them more likely to be investigated and potentially prosecuted for non-compliance **[*36*]**. In order to alleviate this barrier, a third-party facilitator, comparable to the FISS, could act to sanitize this information before it is shared with other companies and the authorities **[*12*]**. The importance of sharing information related to due diligence has been recognised by the NSG, who published a set of corporate guidelines for dual-

use exporters in 2013 **[*17*]**. These encourage firms to establish internal compliance systems incorporating due diligence and vetting, sharing information with relevant state authorities and with their supply chain.

New normative standards

The above sections have attempted to illustrate some of the steps that can be taken to combat supply-side proliferation, drawing on a small number of firms' existing actions in this area and highlighting the importance of beyond-compliance actions. Given the variation in national export controls, and the propensity of proliferators to target the weak points in the international system, these measures will be effective only if widely promulgated across the dual-use industry. At present it seems that levels of adoption are low, particularly among SMEs, where there may be little if any awareness of proliferation issues. Consequently, this section will consider how a non-proliferation norm of behavior might be developed within the dual-use community.

According to theories of corporate social responsibility (CSR), firms frequently take voluntary measures, which go beyond their legal obligations, superseding their immediate economic interests. These might be due to a mix of ethical, philanthropic, or other reasons, with actions strengthened if the firms also expect longer-term economic gain **[*37*][*38*]**. In the proliferation context, it is clear that some large firms are already exhibiting CSR, having embraced supply-side control issues, perceiving it to be part of their role as a responsible stakeholder and a mechanism to grow business in the longer term. However, for others, in particular SMEs, the situation is less clear. This is not surprising, as studies have shown that while CSR can strongly influence the behavior of large firms, its effect is not as significant in decision making of SMEs. For example, in a 2005 survey of Danish SMEs, only just over a third believed CSR had a positive impact **[*39*][*40*]**.

Consequently, it would seem that the onus is on larger firms to develop industry-wide standards, by encouraging or even requiring involvement from their supply-chain partners as a condition of doing business. This approach has proven effective in other industries. For example, in 1990 the three major tuna canners demanded that their suppliers adopt dolphin-safe technology, measures which have been linked to a significant drop in dolphin mortality **[*41*]**. In the proliferation context, this approach has been suggested by Bhandarkar and Alvarez-Rivero, who encourage multinational corporations (MNCs) to take the lead in encouraging CSR in supply chains, recommending that MNCs should assess the specific needs of their suppliers and offer training and other support accordingly **[*40*]**.

Civil society can also play an important role in establishing new normative standards in this area. Appropriate actions include monitoring, assessing, and publicizing firms' activities relevant to non-proliferation. This is already done in the area of nuclear safety by the Institute of Nuclear Power Operations, which ranks power plants on their performance and shares these with the public as a means of motivating managers to adhere to relevant standards **[*40*]**. Civil society can also help facilitate the sharing of best practice and information, offer training and expertise, and undertake awareness-raising efforts **[*42*]**. Here Gunningham and Rees argue that "a commitment to dialogue, persuasion and cooperative problem solving" is likely the most effective strategy for fostering CSR, provided that it is a lack of capability to understand and follow the norms—and not subversiveness—that underlies unsatisfactory performance **[*43*]**. As has been acknowledged in the literature and at the 2012 Wiesbaden Conference, firms, especially smaller ones, struggle significantly with a lack of resources when it comes to proliferation issues. An example of a cooperative approach for civil society is Project Alpha, a UK-government-funded, university-based group, that provides openly available compliance guidance and threat briefs on its website

[*44*]. Alpha also runs sector-specific seminars on export control compliance. Additionally, the project has created a "Partners Against Proliferation" initiative, in which firms that have committed to implement a compliance program receive access to training and other resources.

VI. Conclusions and future work

This paper has argued that supply-side controls enforced by states alone are insufficient to counter nuclear proliferation, and it has suggested a range of actions that industry might take to help close this gap. Weaknesses in the current export control regime stem from the uneven national implementation of UNSCR 1540 and other relevant guidance. This is compounded by the dynamic nature of illicit procurement, with proliferators adopting ever-more-sophisticated strategies to circumvent existing measures. In order to combat this, the private sector will need to take actions that go beyond what is required under existing national regulations, including due diligence and the sharing of this information within their communities. Although this is already happening to some extent, much more effort in this area is required. Large multi-national companies should take the lead, supporting SMEs and propagating best practices for non-proliferation throughout their supply chains. Civil society also has a role to play. It should publicize firms' actions (and inactions) in this area, provide expert guidance and training, and carry out broader activities to raise awareness of the risks posed by supply-side proliferation.

VII. Work Cited

1. Zangger Committee (ZAC) | NTI. *NTI: Nuclear Threat Initiative*, (available at http://www.nti.org/treaties-and-regimes/zangger-committee-zac/).

2. W. Langewiesche, *The Atomic Bazaar: The Rise of the Nuclear Poor* (Penguin Books, New York, 2007).

3. Nuclear Suppliers Group - History, (available at http://www.nuclearsuppliersgroup.org/en/history1).

4. D. Albright, *Peddling Peril: How the secret nuclear trade arms America's enemies* (Free Press: Institute for Science and International Security, New York, 2010).

5. The Nuclear Suppliers Group, NSG-AtAGlance.indd - NSG.pdf (2006), (available at http://www.armscontrol.org/system/files/NSG.pdf).

6. M. Hibbs, The Future of the Nuclear Suppliers Group (2011), (available at http://carnegieendowment.org/files/future_nsg.pdf).

7. A. Wetter, *Enforcing European Union Law on Exports of Dual-use Goods* (Oxford UP, Oxford, 2009).

8. B. A. R. in L. and A. L. Guardia, I've sold nuclear secrets to Libya, Iran and N Korea (2004), (available at http://www.telegraph.co.uk/news/worldnews/asia/pakistan/1453353/Ive-sold-nuclear-secrets-to-Libya-Iran-and-N-Korea.html).

9. 1540 Committee, (available at http://www.un.org/en/sc/1540/).

10. P. Litavrin, The way forward for UNSCR 1540 | 1540 Compass | Publications | CITS. *1540 Compass 6*, 24 (2014).

11. D. Albright, P. Brannan, A. S. Stricker, Detecting and Disrupting Illicit Nuclear Trade after A.Q. Khan. *The Washington Quarterly*. **33**, 85–106 (2010).

12. D. Salisbury, in *Open Source Intelligence in the Twenty-first Century, ed. Christopher Hobbs, Matthew Moran and Daniel Salisbury* (Palgrave Macmillan, London, 2014), pp. 86, 89–91, 95.

13. D. Albright, P. Gray, Building a Corporate Nonproliferation Ethic. *ISIS Reports* (1993) (available at http://isis-online.org/isis-reports/detail/building-a-corporate-nonproliferation-ethic/).

14. U.N. Security Council Committee, United Nations Security Council Resolution 1540 (2004), (available at http://www.un.org/en/sc/1540/committee/composition.shtml).

15. UNODA Update - First Industry Conference on Security Council Resolution 1540 (2012), (available at http://www.un.org/disarmament/update/20120425/).

16. I. Khripunov, A Work in Progress: UN Security Resolution 1540 After 10 Years | Arms Control Association. *Arms Control Association* (2004) (available at

https://www.armscontrol.org/act/2014_05/A-Work-in-Progress-UN-Security-Resolution-1540-After-10-Years).

17. Nuclear Suppliers Group, Good Practices for Corporate Standards to Support the Efforts of the International Community in the Non-Proliferation of Weapons of mass Destruction (2013), (available at http://www.nuclearsuppliersgroup.org/images/Files/National_Practices/NSG_Measures_for_industry_update_revised_v3.0.pdf).

18. European Commission, What is an SME? - Small and medium sized enterprises (SME) - Enterprise and Industry, (available at http://ec.europa.eu/enterprise/policies/sme/facts-figures-analysis/sme-definition/index_en.htm).

19. I. and S. Department for Business with Export Control Organisation (Great Britain), Great Britain, *Export Control Organisation dual-use compliance study: summary of results and key findings.* (Department for Business, Innovation & Skills, London, 2009; http://www.berr.gov.uk/files/file53872.pdf).

20. N. Boland, Interview with Amber Road Director of EMEA Solutions Consulting (2014).

21. J. Larkin, Interview with Larkin Trade international President (2014).

22. C. A. Roper, J. Grau, L. Fischer, *Security Education, Awareness, and Training* (Elsevier, Inc., Burlington, MA, 2006).

23. U.S. Department of Commerce, Don't Let This Happen To You! (2014), (available at http://www.bis.doc.gov/index.php/forms-documents/doc_view/1005-don-t-let-this-happen-to-you-071814).

24. S. Strong, Interview with Strong & Herd Managing Partner (2014).

25. D. Salisbury, Trade controls and non-proliferation: compliance costs, drivers and challenges. *Business and Politics*. **15**, 529–551 (2013).

26. J. Schieffer, S. Y. Wu, Naughty or nice? Punishment and the interaction of formal and informal incentives in long-term contractual relationships (2010), (available at http://mpra.ub.uni-muenchen.de/20891/).

27. Wassenaar, Best Practice Guidelines On Internal Compliance Programmes For Dual-Use Goods And Technologies (2011), (available at http://www.wassenaar.org/guidelines/docs/2%20-%20Internal%20Compliance%20Programmes.pdf).

28. S. Paile, Cahier n°26 - International and European commitments to the export control of nuclear dual-use items: Do the European Union Member States have any room for manoeuvre? *csp*. **26** (2011) (available at http://popups.ulg.ac.be/1784-6390/index.php?id=707).

29. Directorate of Cooperative and State Programs | OSHA, Voluntary Protection Programs (VPP), (available at https://www.osha.gov/dcsp/vpp/).

30. D. Bayley, Interview with Westcon Group EMEA Trade Compliance Manager (2014).

31. A. Kurzrok, G. Hund, Beyond compliance: Integrating nonproliferation into corporate sustainability. *Bulletin of the Atomic Scientists*. **69**, 37–39 (2013).

32. E. L. Hirschhorn, *The Export Control and Embargo Handbook* (Oxford UP, Oxford, 2010).

33. M. Berkemeier, Red Flag Indicators: Detecting Unusual Behaviour in Transactions. *Project Alpha Report*. **9**, 11–12, 15–16 (2013).

34. Lowrie interview.

35. Fraud Intelligence Sharing System - FISS - UK Cards Association, (available at http://www.theukcardsassociation.org.uk/what_we_do/fiss.asp).

36. A. Widl, Non-proliferation: Social Responsiblity in Industry. *1540 Compass*, 34 (2012).

37. A. B. Carroll, A Three-Dimensional Conceptual Model of Corporate Social Performance. *Academy of Management Review*. **4**, 500 (1979).

38. A. B. Carroll, Corporate Social Responsibility: Evolution of a Definitional Construct. *Business Society*. **38**, 284 (1999).

39. M. Kramer, M. Pfitzer, P. Lee, "Competitive Social Responsibility: Uncovering the Economic Rationale for Corporate Social Responsibility among Danish Small- and Medium-Sized Enterprises." (Foundation Strategy Group and Center for Business and Government, John F. Kennedy School of Government, Harvard University, 2005).

40. M. Bhandarkar, T. Alvarez-Rivero, From supply chains to value chains: A spotlight on CSR. *asdf*, 384, 386, 387, 405 (2007).

41. S. M. Maurer, S. von Engelhardt, Industry self-governance: A new way to manage dangerous technologies. *Bulletin of the Atomic Scientists*. **69**, 55.

42. B. Finley, "Meeting the Objectives of UN Security Council Resolution 1540: The Role of Civil Society" (Stimson, Washington, DC, 2012), pp. 8–11.

43. N. Gunningham, J. Rees, Industry Self-Regulation: An Institutional Perspective. *Law & Policy*. **19**, 388 (1997).

44. About Alpha Project, (available at https://www.acsss.info/alpha).

VIII. Authors' Bio and Contact Information

Dr. Christopher Hobbs is Co-Director of the Centre for Science and Security Studies (CSSS) in the Department of War Studies at King's College London. A physicist by background, he carries out research in the area of CBRN proliferation, with a particular focus on nuclear security. He has authored books and articles in this area on topics that include Iran's nuclear development, open-source intelligence, international security issues, and unconventional terrorism. He chairs the International Nuclear Security Education Network (INSEN) and in 2013 received the King's Award for Innovation and Impact for his work in education and training for nuclear security. Contact: Christopher.hobbs@kci.ac.uk

Elisabeth Young Elisabeth Young is a Visiting Research Assistant at the Centre for Science and Security Studies (CSSS) at King's College London. She completed her MA in the Department of War Studies in September 2014. Contact: elisabeth.young@kcl.ac.uk