WMD Insights
Issues and Viewpoints in the International Media

# Minding Our Business: The Role of the Private Sector in Managing the WMD Supply Chain

*February 2009 Issue*

In 1992, Allergan, a small U.S. bio-pharmaceutical company, began exporting a new drug that was hailed as a medical breakthrough because of its ability to relieve the debilitating symptoms associated with a range of muscle ailments. From 1992 to 1994, the company sent the product to thousands of doctors across Asia, Europe, and North and South America, tapping an estimated market of $1.5 billion. [1] One of the company's many clients was the International Federation of the Red Cross and Red Crescent Societies. In several instances, the Red Crescent redirected the drug into Iran, which the United States had accused of bioweapons development and which was operating under rigorous trade embargos. In 1998, the U.S. Department of Commerce fined the U.S. company for export violations. The Government was particularly concerned with the trace amounts of botulinum toxin Type-A contained in the product that could be diverted for nefarious uses, even while it provided relief to patients. As a result, some people inferred that the Red Crescent – and by extension Allergan – had unwittingly been aiding Iran's bioweapon program. Realizing the unique national security implications of its product, the company has since enacted multiple layers of safeguards above and beyond the legal requirements to prevent sales to customers with potentially malign motives.

The market for therapeutic drugs containing botulinum toxin, a so-called Select Agent (pathogens or biological toxins which the U.S. government has determined to have the "potential to pose a severe threat to public health and safety"), will grow to an estimated $2.1 billion by 2010. [2] This has led to an explosion of new industry actors entering the market space, both in the United States and around the globe. Depending upon the integrity of the new entrants, this could have profound implications for national security. For example, recently, and over the objections of U.S. lawmakers, Ipsen Pharmaceuticals, a European company with a competitor product to that of Allergan, began exporting its botulinum toxin product into Iran and has since initiated a series of clinical trials in the country, sharing potentially sensitive dual-use information with Tehran. [3]

These cases, involving two law-abiding pharmaceutical firms, and hundreds of other cases like it, highlight the ease with which states and terrorist organizations could exploit legitimate businesses up and down the supply chain to obtain dual-use knowledge and technologies. They also illustrate the inability of existing control measures to contain this growing threat and the need to modernize the global nonproliferation toolkit. Most importantly, they exemplify the growing size and complexity of the market, and the critical role of private sector collaboration in preventing the proliferation of weapons of mass destruction (WMD) and managing proliferation risks. In today's security environment, a diverse set of forces is gathering, presenting a growing challenge to the practicality of the existing nonproliferation regime and to governments' ability to prevent proliferation without the determined efforts of the private sector. [4]

## The Proliferation Enablers

A commission chartered by the U.S. Congress recently asserted that the world faces a greater than even chance of a nuclear or biological weapon incident within the next five years. [5] This finding is consistent with the near constant warnings from world leaders, intelligence agencies, experts, and the media regarding market opportunities available to determined proliferators. In many ways, these dire predictions are reminiscent of the 1950s and 1960s – an era that led to the development of the existing patchwork of treaties and verification measures designed to curb the spread, and promote the elimination, of nuclear, biological, and chemical weapons. Although the current efficacy of each of these instruments varies dramatically, the common thread connecting them to the WMD nonproliferation regime is a strategy of "technology denial" based on this premise: provided that the components of a weapon can be locked away or otherwise controlled, proliferation is presumed to be manageable.

While the predictions of the last 50 years regarding WMD proliferation and use have not been realized,

evidence suggests that the proliferation challenge in this century will be dramatically different than it was in the last. By the 1990s, an array of powerful economic and political forces converged to revolutionize the global security environment by pushing dual-use knowledge and equipment into more hands in more countries than ever before, expanding and accelerating the pace of trans-shipment and financial transactions. These trends were fostered by:

- *A growth in foreign direct investment:* Although foreign direct investment (FDI) had long been viewed with suspicion by governments around the world, by the 1980s many concluded that it yielded not only short-term financial gains, but also long-term economic benefits. The global development community joined economists and state development agencies in promoting models of export-oriented growth to the governments of less-developed countries. As a result, FDI jumped from $14 billion in 1970 to an astonishing $1.2 trillion by 2007. [6]

- *Increases in global trade:* Greater trade openness emerged with lowered barriers to imports and exports around the world. In 1981, the worldwide average tariff on imports was 29.7 percent; by 2006, that figure had dropped to 9.5 percent. [7] The unprecedented growth in both FDI and trade meant that capital flows and the movement of goods became a regulatory nightmare for governments seeking to prevent the spread of illicit items.

- *Cold War demobilization:* The end of the Cold War touched off an unprecedented transfer of a growing menu of sophisticated – and potentially dangerous – technologies from government to private hands. Former Soviet bioweaponeers, for instance, left their cloistered institutes to open legitimate biotech companies, taking with them their dual-use knowledge. In the United States and other Western countries, defense conversion efforts in the 1990s sought to remake the defense industrial base into a national technology and industrial base with a high degree of civil-military integration that would continue to serve an ongoing, albeit presumably diminished, security need. [8] The result would effectively transition critical dual-use WMD knowledge and capacity from state-governed institutions and a limited number of highly regulated partners to a broader swath of private sector entities.

- *Globalized business practices:* As private companies, initially in the developed world, gained access to new technologies, they sought to maximize profit and efficiency through outsourcing, off-shoring, supply-chaining, and other activities that drove intellectual and manufacturing capacity beyond Western shores. The corresponding transfer of information, processes, and technology led to the generation of new local enterprises, including subsidiary operations, that collaborated with or competed for global market share. Soon, states that were thought to have lacked the indigenous expertise to perform complex R&D and manufacturing operations began to develop competitive industrial sectors. [9]

- *Spread of innovative and manufacturing capacities:* The Global Innovation Index 2008 notes that while knowledge creation, competitiveness, and wealth creation all continue to be dominated by the United States, Germany, the United Kingdom, and Japan, leading indicators also suggest an emerging innovation capacity among newly industrialized and even developing world economies. The biological sciences are particularly telling. Cuba, for example, was one of the first countries to have developed a vaccine against the group B meningococcus. Egypt has developed several innovative diagnostic and therapeutic products for hepatitis C. India developed and now produces a recombinant hepatitis B vaccine and is one of several developing countries, including Brazil, that has launched a major nanotechnology initiative. [10]

- *Accelerated movement of goods and services:* Advanced transportation technologies have enhanced the capacity of companies – including dual-use technology manufacturers – to ship products around the globe in an unhampered, undetected manner. Larger and more efficient boats, roll-on/roll-off cargo container vessels, new loading and unloading tools, more efficient port management, improved logistics, and satellite navigation and tracking have accelerated the pace at which goods flow around the world. [11] The United Arab Emirates (UAE) alone invested billions of dollars during the 1990s to become a global trading hub. By 2007, more than $12 billion worth of U.S. goods were flowing through the UAE annually. [12] *(For more information on the sensitivities surrounding UAE as a global trading hub, see "Export Controls in the United Arab Emirates: A Practical Manifestation of a Strategic Dilemma" in this issue of* WMD Insights.) The sheer volume

of trade through many of these ports imposes practical limitations to oversight, regulation, and the strategy of technology denial.

## Examples of the Private Sector's Role in the Proliferation Supply Chain

Given these political and economic realities, the potential for proliferation has gone global. [13] Today, not only do more countries have access to critical know-how, materials, and capacities to develop, build, and ultimately use weapons of mass destruction than ever before, but more importantly, the number of private companies servicing this global market has also expanded. The techniques involved in WMD development – harnessing the atom, synthesizing chemical production, and using biological organisms or substances – have an overwhelmingly legitimate and absolutely necessary role in the civilian economy. Thus, the environment in which proliferation risks occur is shaped largely by the private sector. Privately-owned companies not only produce and operate nuclear, chemical, and biological industrial equipment, but they also carry out, by far, the greatest share of the basic R&D for the relevant technologies, goods, and methods of application. In addition, university research is often commercially funded, and governments have expanded public-private partnerships even in some of the most sensitive areas of technology in order to take advantage of cost reductions and innovation. [14]

Of course, the array of private entities that could aid – either deliberately or unwittingly – the activities of a terrorist or committed state proliferator goes far beyond those firms that operate fuel enrichment facilities, experiment with select biological agents, or produce toxic chemicals. A broad swath of dual-use technology innovators and manufacturers is also involved in information security, telecommunications, sensors, lasers, and many other sectors that could have direct applications in proliferation efforts. Foreign trading companies, brokers, middlemen, shipping companies, and freight forwarders are critical actors in moving materials and fabricated products. The global financial system has attracted an especially substantial degree of government attention for its role in facilitating proliferation networks. Companies in each of these sectors could either contribute to the proliferation supply chain or become a useful partner in its dismantlement.

### *The Technology Innovators*

Identifying the breadth of technologies that could be diverted for weapons purposes is a massive task. The emphasis of developed world governments has been to erect barriers to the outflow and transfer of potentially dangerous technologies, particularly since the 1990s. As damaging as the lack of regulation is, the uneven global application of existing restrictions is also problematic.In the wake of revelations regarding the activities of the Japanese doomsday cult Aum Shinrikyo, and the anthrax attacks in the United States six years later, governments became increasingly concerned with an array of potentially deadly pathogens and toxins that could be exploited by a committed bioterrorist. Meanwhile, the global pharmaceutical industry was exploring conotoxins, botulinum toxin, ricin, tetrodotoxin, and a host of other toxic substances for their therapeutic benefit. As evidenced by the opening anecdote, governments have been unable to manage the movement of fabricated products.

Nor, however, has the international community developed common standards that would curb potentially dangerous research. The patchwork of national laws that has emerged has created an uneven regulatory environment that encourages multinational firms to "forum shop" for the country of least resistance, driving sensitive activities abroad. U.S. regulations, for example, prevent biotech companies operating in the United States from undertaking research using recombinant DNA technology to generate functional forms of these dangerous toxins. A South Korean firm called Medy-Tox, however, is doing so in order to develop a toxin of longer duration – a beneficial property for a therapeutic product, but a critical element of a bioterrorist's weapon. [15] Although the company's plan has raised significant concern at the U.S. Centers for Disease Control and within the National Science Advisory Board for Biosecurity (NSABB), the company is operating legitimately under current South Korean law. Furthermore, once a fabricated product is developed, the firm will be able to enter the massive U.S. market given the FDA's inability to screen products with an eye to national security. Similar challenges can be seen across a host of dual-use technology sectors. The net result is the shift of sensitive technology development activities to locations of least resistance.

### *Manufacturing Sector*

The producers of dual-use items have been particularly susceptible to unwitting exploitation by committed proliferators. The A.Q. Khan network most infamously exposed the degree to which legitimate companies could be exploited, but the case of the network's activities is far from the only example of this exploitation. A host of criminal enterprises involving business activities are routinely exposed as they

attempt to exploit the weaknesses in the global control regimes governing both WMD and conventional armaments. [16] It is well known that Saddam Hussein had taken advantage of illicit networks to circumvent the embargo imposed on Iraq and acquire goods from other countries for use in prohibited programs. In 1991, for example, while scouring an outpost in the desert of Iraq, UN weapons inspectors stumbled upon a small number of vacuum pumps made by the German manufacturing firm, Oerlikon Leybold Vacuum. At the time, none of the pumps were found on any export control or dual-use item list. On closer study, the inspectors realized that one of the vacuum pumps was attached to a cyclotron, which can be used to enrich uranium. Thus, Oerlikon and its competitors had knowingly – though innocently – supplied the pumps to the Iraq government and thereby helped to advance its nuclear weapons program. As news of the case spread, the damage to the Oerlikon brand prompted the company to re-think the fulfillment of a growing number of suspicious requests for technology and develop an internal charter that, as with Allergan, would extend sales restrictions beyond those required by national laws.

For dual-use manufacturers, this case illustrates the serious consequences that illicit networks may have on legitimate business operations. For government regulators, it points to the additional measures that industry could take – if given the incentive to do so – to support proliferation prevention. The case of Oerlikon has prompted an awakening, particularly among European companies and governments who have begun collaborative efforts to extend voluntary charters across a broad cross-section of dual-use industries. [17] For example Oerlikon is leading an effort to extend the so-called “Leybold Charter” across European dual-use industries. The Charter consists of a stringent set of voluntary self-restraint mechanisms related to export matters and in support of nonproliferation objectives.

***Shipping Industry***

In 1993, a highly trained and now redundant officer of the Soviet military named Victor Bout founded a private shipping company called Transavia Export Cargo. Over the next two years, his fortunes grew to an estimated $50 million, aided in large measure by the delivery of weapons to the Northern Alliance in Afghanistan. Supported by multiple military aircraft obtained from Moscow, Bout’s empire and profits grew as he moved his business operations from Belgium, where authorities had launched an investigation into his questionable activities, to the UAE. Using Sharjah International Airport as well as airfields in the neighboring emirates of Ajman and Ras Al Khaimah as trans-shipment points, Bout built a global network of front companies and clients. UN officials say that Bout smuggled untold numbers of small arms, narcotics, and other contraband fueling African conflicts in Angola, Cameroon, Central African Republic, Democratic Republic of the Congo, Equatorial Guinea, Kenya, Liberia, Libya, Republic of the Congo, Rwanda, Sierra Leone, South Africa, Sudan, Swaziland and Uganda. Bout’s operation exemplifies the complexities of regulating the global shipping industry. Even the United States government became an unwitting client of Victor Bout when a freight forwarder under contract to the State Department subcontracted to his firm. [18]

*Victor Bout*

Because of his continued ties to the Russian military, Western intelligence agencies were particularly concerned with Bout’s potential to move contraband nuclear material into Afghanistan. While the CIA never received credible evidence of WMD material shipped on Bout’s planes, a senior Afghan official alleged that Ariana Airlines shipped cyanide, ricin, and other toxic substances for al Qaeda from Sharjah to Kandahar. [19] Although it would appear that Bout was not an integral part of the WMD supply chain, his network illustrates that the global shipping industry extends well beyond the much publicized sea-based cargo container market around which extensive government outreach at targeted “megaports” is occurring. Without the willingness of this industry not only to know their customer, but also to know their cargo, preventing the diffusion of materials and weapons of mass destruction will become increasingly challenging. These companies have been urged, therefore, to develop a more stringent code of conduct while governments appropriately encourage such behavior through market-based access.

***Financial Sector***

On March 3, 2008, the UN Security Council approved a new round of sanctions against Iran for refusing to suspend uranium enrichment and heavy-water-related projects. In doing so, it

called upon all states to exercise vigilance over the activities of financial institutions in their territories with all banks domiciled in Iran, in particular with Bank Melli and Bank Saderat, and their branches and subsidiaries abroad. According to the sanctions resolution, both banks were complicit in activities contributing to proliferation-sensitive nuclear activities, or to facilitate the purchase of sensitive materials. But even as America's closest allies in Europe seek to curb Iran's pursuit of an offensive nuclear capability and terrorist financing, branches of Saderat continue to operate in the UK, France, Germany, and Greece. [20] Like domestic regulations governing the biosciences, in a globalized world, the uneven enforcement of financial regulations provides unique opportunities to circumvent global mandates. As governments reassess the regulation of this sector in the wake of the global financial crisis, the moment is ripe not only to incorporate nonproliferation as a central tenet of regulation, but to reaffirm the responsibility of the financial sector to become a partner in proliferation prevention by sharing critical information and developing industry-wide best practices.

Bank Saderat and Bank Melli Logos

## Getting the Relationship Right

At a time when global economic and political forces require tighter collaboration between governments and industry, the relationship between the public and private sector in most countries around the world, including the United States, can only be characterized as poor and tainted with mutual suspicion and animosity. Making this relationship more functional will be a difficult process, but doing so is paramount to preventing WMD proliferation in the 21st century.

Regulating a growing and increasingly unwieldy set of private actors is one component of prevention, but it is not simply a challenge of lack of regulation. In the past decade alone, the events of September 11, 2001, the breakup of A.Q. Khan's one-stop-shopping network, and many other incidents have shown how bad actors have looked for and exploited market opportunities. The response of lawmakers around the globe has typically been more of the same: state-centric, supply-side controls, including tighter export controls, restrictions on access to technology, new measures to forcibly halt the physical transfer of suspected items, enhanced aviation, port, harbor, and container security, tighter controls on visas and immigration, and rigorous enforcement of domestic regulations. For private companies, complying with these new and sometimes uneven regulations, while paying more for insurance premiums, having to scrutinize their practices, and being confronted by diminished public perceptions in an uncertain world have all had a deleterious effect on their overall business environment. According to many firms, occasionally misguided and excessive government action against terrorism is more often a greater danger to corporate interests than the potential impact of terrorist incidents themselves. [21]

In the era of globalized proliferation, uneven regulation from country to country also poses significant challenges to prevention. Activities proscribed by one government are welcomed by others. Even recognizing the inherent dangers of permitting potentially dangerous dual-use research has been counterbalanced by domestic economic growth opportunities. Working to convince developing world governments to strengthen nonproliferation standards can have a direct impact on economic growth: tightened screening at ports and border crossing slows commerce and can negatively affect competition; restrictions on the activities of technology companies can drive jobs offshore; and more strict regulation of the financial sector may make that country less attractive to global commerce. Indeed, the perceived unwillingness of some less wealthy governments to embrace stringent nonproliferation standards fully is in many ways a conflict over development itself. Many in the South have viewed the tightening of controls demanded by the North as a gambit to stymie competition and keep the developing world in a perpetual state of underdevelopment. [22] *(For more information on the South's perspective on instruments used by the global community to tighten proliferation controls, see "UN Security Council Resolution 1540: Part II: The Caribbean States: A Case Study" in the August 2008 issue of* WMD Insights.)

Perhaps most importantly, proliferation prevention in the twenty-first century will necessitate a better understanding of the elements that drive supply-side decision making by the array of new links in the proliferation chain. While a rich literature was generated during the Cold War to examine the decisions of principally developed states to go nuclear, no such systematic analysis has been undertaken that evaluates the incentives – or disincentives – for a new array of non-state actors to proliferate or not. Understanding demand, and the motivations to meet that demand, is a critical unmet challenge for the nonproliferation community. An open dialogue between companies has begun at the front end of the

supply chain in Europe to help define what those motivations and incentives look like. This model could be expanded globally and across all sectors of the proliferation supply chain.

*Brian D. Finlay - The Stimson Center*

HOME

## SOURCES AND NOTES

[1] Global Industry Analysts, Inc., *Botulinum Toxin: A Global Strategic Business Report*, MCP-1833 (San Jose: Global Industry Analysts, Inc., 2008), II-I.

[2] Ibid., II-1.

[3] Ipsen, "Information Document dated December 6, 2005," http://w3.cantos.com/06/ipsen-601-ddfey/en/content /Information_document.pdf **[View Article]** and Matt Korade, "Dual-Use Products Available to Iran Pose Threat, Say Lawmakers," Congressional Quarterly Homeland Security, October 29, 2008.

[4] For an overview of WMD proliferation predictions see: Dwight D. Eisenhower, "Address by Dwight D. Eisenhower, President of the United States, to the 470th Plenary Meeting of the United Nations General Assembly," New York, NY, December 8, 1953, http://www.iaea.org/About/history_speech.html; **[View Article]** "Face-to-Face, Nixon-Kennedy: Vice President Richard M. Nixon and Senator John F. Kennedy, Third Joint Television-Radio Broadcast" October 3, 1960; Lewis A. Dunn, *Controlling the Bomb: Nuclear Proliferation in the 1980s* (New Haven, CT: Yale University Press, 1982), 1-94; Leonard S. Spector, *Nuclear Ambitions: The Spread of Nuclear Weapons* (Boulder, CO: Westview Press, 1990), 6-9; Office of the Secretary of Defense, *Proliferation: Threat and Response* (Washington: U.S. Department of Defense, 2001), 1.

[5] Commission on the Prevention of Weapons of Mass Destruction Proliferation and Terrorism, *World at Risk: Report of the Commission on the Prevention of Weapons of Mass Destruction Proliferation and Terrorism* (New York: Vintage Books, 2008), xi.

[6] UNCTAD FDI Online Database, Foreign Investment Database, http://www.unctad.org/Templates /Page.asp?intItemID=1923&lang=1. **[View Article]**

[7] The World Bank, *Table 1: Trends in Average Applied Tariff Rates in Developing and Industrial Countries, 1981-2006 (Unweighted in %)*, http://siteresources.worldbank.org/INTRES/Resources/469232-1107449512766/tar2006.xls. **[View Article]**

[8] Linda Brandt, "Defense Conversion and Dual-Use Technology: The Push Toward Civil-Military Integration," *Policy Studies Journal* 22.2 (1994), 359.

[9] Mark Fitzpatrick, ed., *Nuclear Black Markets: Pakistan, A.Q. Khan and the Rise of Proliferation Networks*, IISS Strategic Dossier, May 2007, p.12.

[10] Committee on Advances in Technology and the Prevention of Their Application to Next Generation Biowarfare Threats, National Research Council, *Globalization, Biosecurity, and the Future of the Life Sciences* (Washington: National Academies Press, 2006), 112-129.

[11] Moisés Naím, *Illicit: How Smugglers, Traffickers and Copycats are Hijacking the Global Economy* (New York: Doubleday, 2005).

[12] Eric Lipton, "U.S. Alarmed as Some Exports Veer Off Course," *New York Times*, April 2, 2008, http://www.nytimes.com /2008/04/02/washington/02UAE.html. **[View Article]**

[13] See Douglas Frantz and Catherine Collins, *The Nuclear Jihadist: The True Story of the Man Who Sold the World's Most Dangerous Secrets...And How We Could Have Stopped Him* (New York: Twelve, 2007) and American Public Media, "The Business of the Bomb: The Modern Nuclear Marketplace," American RadioWorks, http://americanradioworks.publicradio.org /features/nukes/. **[View Article]**

[14] Alyson JK Bailes, "Terrorism and Business," Sciences-Po, Paris, September 5, 2006, http://www.gem.sciences-po.fr/content/news_events/pdf/bailes_Terror050906.pdf. **[View Article]**

[15] Medy-Tox is using recombinant DNA to generate a functional form of botulinum toxin, and using that rDNA technology to generate a longer duration toxin. See: http://www.medy-tox.co.kr/new_site/rnd/rnd.htm. **[View Article]**

[16] Bruno Gruselle, *Proliferation Networks and Financing* (Paris: Fondation pour la Recherché Stratégique, 2007), http://www.frstrategie.org/barreFRS/publications/rd/RD_20070303_eng.pdf; **[View Article]** and Joby Warrick, "Iran Using Fronts to Get Bomb Parts From U.S.," *Washington Post*, January 11, 2009.

[17] See: Ralf Wirtz, "Finding Innovative Ways to Detect and Thwart Illicit Nuclear Trade," Carnegie Nonproliferation Conference, June 26, 2007, http://www.carnegieendowment.org/files/detect_thwart.pdf **[View Article]** and David Albright, "Creation of Leybold's Internal Compliance System," Institute for Science and International Security, March 30, 2002.

[18] Letter from Paul V. Kelly, Assistant Secretary Legislative Affairs to Senator Russ Feingold, United States Senate, June 2, 2004.

[19] Douglas Farah and Stephen Braun, *The Merchant of Death: Money, Guns, Planes and the Man Who Makes War Possible*, New Jersey, 2007, pp. 142-143.

[20] Security Council 5848th Meeting (PM), "Security Council Tightens Restrictions on Iran's Proliferation-Sensitive Nuclear Activities, Increases Vigilance over Iranian Banks, has States Inspect Cargo," March 3, 2008,http://www.un.org/News/Press /docs/2008/sc9268.doc.htm. **[View Article]**

[21] See source in [14].

[22] See, "The Next 100 Project: Responding to UN Resolution 1540 with Development and Capacity Building Assistance in the Caribbean," http://stimson.org/cnp/pdf/DR_summary.pdf **[View Article]**