STIMSON

MARKET POWER

Adapting Public and Private Roles for Transnational Commerce and Transnational Threats

By Nate Olson & Brian Finlay

Stimson.org

Managing Across Boundaries Initiative

The authors are grateful to all those from industry and government who provided observations, assessments and recommendations to inform this report and our ongoing work with the private sector. Our industry interlocutors, in particular, deserve special thanks for being exceptionally generous with their time and ideas.

We sincerely appreciate the research and editing assistance provided by our Stimson Center colleagues Esha Mufti and Alex Georgieff. We also thank our Center colleague Debra Decker for her valuable input on insurance and risk management topics.

In addition, we are most grateful for financial support from the Project on Advanced Systems and Concepts for Countering Weapons of Mass Destruction (PASCC), Center on Contemporary Conflict, Naval Postgraduate School. This report builds on an earlier product submitted to PASCC.

Finally, we are indebted to Emma Belcher and the John D. and Catherine T. MacArthur Foundation, as well as Carl Robichaud and the Carnegie Corporation of New York, for their keystone support of the wider industry engagement efforts of the Managing Across Boundaries Initiative at the Center.

The Stimson Center
September 2013

A NOTE ON SOURCES

The project team conducted its interviews on a not-for-attribution basis.

This material is made possible in part by support from the Project on Advanced Systems and Concepts for Countering Weapons of Mass Destruction (PASCC), Center on Contemporary Conflict, Naval Postgraduate School, under Grant No. N00244-12-1-0034. PASCC is supported by the Defense Threat Reduction Agency (DTRA).

Governments never will act at the speed of 21st-century innovation and commerce. Achieving genuine security amid a range of complex transnational threats therefore will require new partners, new models for engaging those partners and new ways of thinking to tackle problems that border on intractable.

Privatization, outsourcing, global industrial development and the migration of many business activities to an electronic medium are pushing sensitive items into more hands. These same trends are eroding the capacity of even well-resourced governments to regulate cross-border trade, travel and communication. A wide array of private sector interests – from dual-use technology innovators to shipping companies, investment funds and insurance providers – play a role in the movement of potentially dangerous materials, limiting the control of governments and increasing potential for the proliferation of weapons of mass destruction and other forms of illicit trafficking.

Government regulation will remain central to preventing transnational crime for the foreseeable future. But it will not suffice. Regrettably, neither government nor the expert community has developed practical, sustainable industry collaborations that evolve the public-private relationship beyond a static focus on compliance and into the realm of mutual interest. To address this need, the Stimson Center's Managing Across Boundaries Initiative has been engaged in extensive conversations with dual-use technology manufacturers, radiopharmaceutical companies, supply chain and logistics firms, and insurance providers.

The common thread in these dialogues has been how to better align industry profitability and public security as mutually reinforcing goals in global business operations – principally through nonregulatory means. Exploring how government might accommodate these ideas does not imply that the private sector has a monopoly on wisdom, or that it deserves a platform to advocate for its priorities without critical evaluation. Rather, the aim has been to engage industry with "eyes wide open" and shed greater light on the many variables that shape its priorities, so that ultimately, there emerge new areas where public and private incentives align and support counter-trafficking and nonproliferation more sustainably.

The project team has found that the core challenges to public-private cooperation can be broken down into three categories: gaps in knowledge, gaps in communication and gaps related to structural or institutional context. The US government's (USG) priorities for improving public-private relationships should track largely along the same lines. Those priorities ought to include:

- **Enhancing knowledge of industry's economic and political landscape**
- **Understanding the full range of industry's value drivers**
- **Diversifying the USG's "portfolio" of interagency and public-private coordination tools**

Industry feedback has highlighted several areas of potential near-term action. As just one example, an emerging coalition – including dual-use technology manufacturers, shipping companies and firms from the insurance/reinsurance space – has shown significant support for a more proactive private sector role in both the design and administration of "trusted trader" initiatives. Some USG efforts now underway, such as implementation of the *National Strategy for Global Supply Chain Security*, could offer a testing ground for more modern mechanisms.

There is urgent need for a "new normal" in public-private relationships. This report aims to facilitate the critical dialogue on these issues.

Global commerce is stretching traditional tools of governance to their limits – and beyond. In the security sphere, illicit trafficking threats are evolving alongside a global diffusion of technological capacities that are themselves rooted in, and facilitated by, a growing network of private sector actors. While the "means of production" for weapons of mass destruction (WMD) and other dangerous technologies was once the exclusive purview of governments, privatization and reduced trade barriers have blurred the lines between WMD proliferation and a wider array of cross-border trafficking threats.

These facts may lead security analysts to despair. Viewed more objectively and expansively, though, they open new opportunities to modernize approaches to counter-trafficking and nonproliferation. Recognizing the potential for nonregulatory, market-driven tools to support the public interest while yielding benefits to legitimate industry must be a central part of those efforts.

OBJECTIVE

Most counter-trafficking strategies are rooted in government-defined threats and focused on government-driven solutions. In contrast, this report seeks to open a new dialogue with industry on the convergence of transnational security challenges and the potential for sustainable, mutually beneficial ways of engaging with government to tackle those challenges. In so doing, the project team hopes to fill gaps in the current narrative on "public-private partnerships."

The presumption here is not that industry has a monopoly on wisdom, or that it deserves a platform to advocate for its priorities without critical evaluation. Rather, the aim of the project has been to engage industry with "eyes wide open" and shed greater light on the many variables that shape business priorities, so that ultimately, there emerge new areas where public and private incentives align.

The project's dialogue with industry has been built around these key questions:

What are the specific proliferation or trafficking challenges that thrive on legitimate trade for each given industry sector?
Before any reasonable effort can be made to address the threat of transnational criminal trafficking of any sort, a comprehensive catalogue must be developed outlining the US government's understanding of the threat and specific concerns with the industry. What do existing violations reveal about criminal interest in exploiting private industry? What do trends signal about the evolution of these threats? What are the future threats that will come to define illicit trafficking patterns that industry should be aware of?

What is industry's understanding of the global trafficking challenge?
Government regulations are defined by national security objectives. As tactical implementers, the private sector has a unique perspective on the threat posed and methods used by illicit procurement networks and other transnational criminal agents. How does industry's understanding of proliferation or trafficking threats differ from the strategic perspective of government? How can these often diverging threat perceptions be better aligned to the benefit of US national security?

What are the principal issues of concern for industry with existing regulatory regimes?
Companies and trade associations have long rallied against what they argue to be unfair or unreasonable regulations, whether related to export and transshipment controls, market approvals or other government policies. How do US laws and enforcement practices impede global competitiveness in each of the industry spaces? What are the true direct and indirect costs of compliance?

What efforts has industry initiated already to mitigate illicit trafficking?
Companies with significant "brand equity," along with those that have been targets of legal sanction in the past, often institute sophisticated mechanisms of self-regulation. What are the best practices that might guide future industry action?

What more could each industry sector do to prevent illicit trafficking?
Instinctively, all companies and business associations push back against the need for enhanced regulation. Yet virtually all companies also recognize that there are additional measures that could be put in place to enhance national security. Those measures need not entail additional regulation in all cases.

What incentives that would bring industry to the table and, in turn, inspire reciprocal efforts from government?
In the face of the global economic slowdown, and an unevenly regulated global marketplace, companies cannot afford to engage in non-mandated practices that threaten their bottom lines. Governments, likewise, cannot afford unending subsidies to industry. Examining the broader economic and regulatory environment is necessary to uncover how incentives can be realigned, or market forces otherwise harnessed, for mutual benefit.

GLOBAL COMMERCE AND EVOLVING THREATS

Several decades of cascading liberalization in trade and capital markets has greatly expanded the availability of sophisticated materials, technologies and expertise. It has meant greater prosperity for billions of people and enabled development of a global physical and informational infrastructure that has further reinforced economic integration. But it also has empowered criminals and terrorists on an entirely different scale.

The private sector has been the main driver for greater global access to goods and technologies. Industry today is the dual-use technology innovator, the weapons manufacturer, the air or seaborne carrier, the financial investor or the insurance underwriter. As such, an array of companies – technology innovators and manufacturers, private investors, financial and insurance firms, and a rapidly expanding supply chain industry – has also contributed, knowingly or unknowingly, to the illicit trade in dangerous products, materials and technologies, including dual-use WMD items.

Figure 1 shows states whose territories have been used or whose firms have been complicit in trafficking incidents documented by the International Atomic Energy Agency (IAEA), along with other connections to the A.Q. Khan black market. The information reflected in the figure suggests that a committed proliferator can evade even the most rigorous regulation. Almost always, these incidents have involved an array of unwitting private sector entities whose motivations are legitimate growth and profit.

One need not look beyond the 2005 discovery of an American-made computer circuit in an unexploded roadside bomb in Iraq to realize the perils of technology diffusion.

FIGURE 1
The Modern Proliferation Supply Chain

Regardless of intent or foreknowledge, countries in red have been implicated in the A.Q. Khan Affair and/or listed in the IAEA Illicit Trafficking Database.[1]

In this case, radio frequency modules produced by a Minnesota company were sold to middlemen in Singapore, forwarded to Iran by air freight through a third country, then smuggled across the border into Iraq. The consequences of similar transactions in support of a WMD program, as with the A.Q. Khan Affair, are quite sobering.

The case of European multinational manufacturing firm Oerlikon Leybold (now known as the Oerlikon Group) also reflects the evolving challenge. In 1991, while searching a remote outpost in the Iraqi desert, UN weapons inspectors stumbled upon a small number of vacuum pumps supplied by Oerlikon Leybold Vacuum. At the time, none of the items discovered was listed in any national or multilateral export control regime. But upon closer study, the inspectors realized that the vacuum pump was attached to a cyclotron, which can be used to enrich uranium through electromagnetic isotope separation.

Oerlikon and its competitors had unwittingly advanced the Iraqi government's nuclear weapons program. As news of this spread, the damage to the Oerlikon brand prompted the company to re-think its fulfillment of a growing number of suspicious requests for technology. The incident also highlighted the ease with which proliferators can exploit legitimate companies to obtain weapons technologies, the inability of existing measures to constantly contain this growing threat, and the serious consequences that illicit networks may have on both legitimate business operations and global security.[2] Soon thereafter, an internal "Leybold Charter" was adopted that called for stringent, voluntary self-restraint in export matters and that explicitly expressed support for nonproliferation goals.

Regrettably, the Oerlikon incident was not an aberration. In August 2013, for instance, the US Department of State assessed a civil penalty of $25 million against Meggitt-USA for hundreds of International Traffic in Arms Regulations (ITAR) violations that stretched back into the mid-1990s. Voluntarily disclosed by the company following an internal, post-acquisition review, these violations mainly involved unauthorized export of defense articles, including technical data and the provision of defense services.[3]

Governments around the world, led most often by the United States – one of the most rigorously regulated and enforced marketplaces on the planet – constantly struggle to keep up with rapidly changing technology by developing new restrictions and regulations, backed by an array of export controls and the threat of fines and prosecution. Nonetheless, we continue to see incidents of illicit or otherwise undesirable technology diffusion, including from the United States.[4] This underscores the need for more innovative tools and approaches, not least in government-industry relationships.

THE NEED FOR A "NEW NORMAL" IN PUBLIC-PRIVATE RELATIONSHIPS

The fragmentary state of public-private cooperation on national security issues is a strategic weakness for the United States. The threat environment continues to evolve at great speed. Equally important – but less appreciated by many in the national security community – is that globalization of trade and commerce is changing the nature of *governance* itself. These two trends are related, and formal government institutions will need to confront the latter if they are to have any hope of adapting successfully to the former.

What the policy community often reduces to the term "global supply chain" is actually a complex, multi-layered system of assets owned primarily by private sector entities. Industry and government alike leverage these assets in the air, sea, land, space and cyber domains, which collectively can be thought of as a commons or public good that is shared across national borders. The attendant challenge in preventing transnational crime – whether upstream with the suppliers of raw materials and the technology innovators, downstream with end users or at the many intervening points – is twofold:

Jurisdiction.
In the main, the authorities of national governments are limited to national borders. Bilateral, multilateral and international initiatives go some way toward filling the vacuum beyond, but they employ the same types of mechanisms seen at the state level – often, less effectively.

Complexity and speed of change.
The efficiencies of global commerce and the ever-expanding horizons of new technologies demonstrate how outmoded many traditional legal, regulatory and bureaucratic concepts have become.

These dual asymmetries open new pathways and new incentive structures for trafficking in dual-use materials and technologies that could support a chemical, biological, radiological or nuclear (CBRN) capability. By exploiting legitimate traders and service providers, these illicit procurement networks often hide in plain sight. The same insidious infiltration of legitimate trade has been seen with other forms of transnational crime, including trafficking in counterfeit goods, narcotics and humans. The relationship among these different illicit activities bears directly on the nonproliferation research agenda, meriting further comment below. Whatever the extent of that relationship, the toll of illicit trafficking on public and private interests alike is significant.

To be clear, traditional law and regulation are, and will remain, the central organizing principles for maintaining order and, more to the point, for proliferation prevention. But it would be far more preferable to leverage the market itself to reinforce sound regulations and more systemically discourage or impede

these illicit activities much earlier. Put differently, if the market presented superior options to the various actors throughout global economic networks who, knowingly or otherwise, facilitate illicit trade, it would benefit both the public security interest and legitimate commerce.

Calls for improved public-private cooperation on these issues have grown louder in recent years. Unfortunately, most ensuing efforts – with some notable exceptions referenced below – have unfolded within the traditional and rigid conceptual framework of how government and industry should relate to one another. Thus, familiar bureaucratic obstacles have prevented or rolled back progress time and again.

A truly modernized strategy for proliferation prevention requires two major changes to the narrative on public-private mechanisms:

- **Engaging a broader set of industry stakeholders** for a more informed view of how security imperatives interact with market dynamics, both across and within sectors
- **Exploring more aggressively the potential of market-based incentives** to change industry behavior meaningfully and sustainably in the service of government's security objectives

These changes will not necessarily be easy. And there certainly is no silver bullet that will immediately degrade illicit networks or thwart all proliferation efforts. But prospects under the status quo look much worse.

ECONOMIC CONVERGENCE BEGETS THREAT CONVERGENCE

Greater complexity in the global economic environment has spawned greater complexity in the threat environment. Many contemporary security challenges do not respect national borders or policy stovepipes. Nor do they lend themselves to precise measurement. As experts in both academia and government have argued recently, statistics on illicit trafficking often rest on dubious foundations.[5] On the whole, however, prevailing indicators suggest that these problems, commonly subsumed under the rather abstract heading of "transnational threats," are eluding the determined efforts of traditional players in law enforcement and intelligence. For example:

One quarter of the annual $4 billion small arms trade is unauthorized or illicit.
Every day around the world, 1,000 people die because of guns.[6] And on average, 300,000 intentional firearm deaths occur each year as a direct result of armed conflict.[7]

According to the US government, approximately 800,000 incidents of international human trafficking occur every year.
This figure does not include millions of other incidents involving people trafficked within their own countries. The International Labor Organization estimates 20.9 million individuals worldwide are in forced labor, bonded labor, forced child labor or sexual servitude. Other estimates range up to 27 million people.[8]

The IAEA's Illicit Trafficking Database records 419 incidents involving unauthorized possession of nuclear or radiological materials between January 1993 and December 2012.
Sixteen involved highly enriched uranium (HEU) or plutonium.[9] A fission-based nuclear weapon requires only 7 to 8 kilograms of plutonium, or 25 kilograms of HEU. The balance of the IAEA-reported incidents could contribute to a "dirty bomb" whose second-order economic and political consequences would be severely disruptive.[10]

The spread of counterfeit goods has become a global phenomenon in recent years, and the range of goods suffering infringement has increased significantly.
According to a study by the Counterfeiting Intelligence Bureau of the International Chamber of Commerce, counterfeit goods make up 5 percent to 7 percent of world trade. The US Federal Bureau of Investigation believes that the first bombing of New York's World Trade Center was financed by the sale of fake Nike and Olympic t-shirts by followers of Sheikh Omar Abdul Rahman.[11]

As the international financial industry ballooned through the 1990s, money laundering grew commensurately.
By 1998, the International Monetary Fund estimated the global flow of dirty money to be 2 percent to 5 percent of the global economy. More recent estimates place the flow of laundered money at upwards of 10 percent of global gross domestic product (GDP).[12]

According to the UN Office on Drugs and Crime, the global drug trade is worth an estimated $322 billion annually with 52,356 metric tons of opium, cannabis, cocaine and amphetamine-type stimulant (ATS) produced each year.[13]
The economic costs alone of drug abuse in the United States have been estimated at $193 billion per year.[14] And 26 million people worldwide are considered "problem drug users."[15]

The aggregate consequences of these crimes reach much further. Criminal networks invade weak and failing states, capturing key government agencies, undermining and ultimately controlling many of the critical functions of government – customs and border controls, the judicial system, police and banks. Moreover, the convergence of these networks appears to be strengthening, with criminal groups profiting not just from one but various trafficking and smuggling activities.[16] One of the most daunting perils in this regard is that these networks could facilitate trafficking in WMD materials and other dangerous weapons and technologies that threaten global security.[17]

For instance, according to the US Drug Enforcement Agency, terrorist "enablers" in the Tri-Border Area of South America funnel the profits of their drug enterprises through money laundering operations to Islamic Jihad and Hezbollah.[18] And the black market nuclear network of A.Q. Khan, preying in part upon legitimate technology manufacturers and shipping companies in a dozen countries around the world, helped facilitate the nuclear programs of North Korea, Iran and Libya, and may have even had interactions with Al Qaeda.[19]

These cases again show that the complexities of today's transnational trafficking threats are interconnected, and cannot be solved within the traditional policy stovepipes and state-centric thinking that have dominated policymaking in the past. While illicit flows of narcotics, counterfeit goods and money often circumvent the formal economy – on the backs of mules across the Afghan border, or aboard pleasure craft from the Caribbean into US territory – a large share intersects at some point with the legitimate supply chain. And even though the "end users" in a proliferation supply chain (say, the government of Iran) may differ from those in other contraband product lines, the intervening points on the supply chain that coordinate, ship, insure and otherwise underwrite the movement of WMD items often facilitate these other forms of illicit trafficking. Governments have worked hard to educate, regulate and enforce standards of good behavior across these "middleman" industries. Regrettably, in most instances, these efforts simply have reshaped, not mitigated, the threat.

Meanwhile, globalization has yielded a competitive landscape wherein the most vigilant private firms face economic disincentives to combat illicit activity proactively. In the eyes of many private actors, particularly in the dual-use technology and shipping sectors, government regulation has often been haphazard and inimical to fair competition. As a result, relations between government and industry have eroded appreciably over the past two decades, as has much of the rationale for industry to exceed legal obligations in the prevention of illicit activity that does not directly affect its own business operations.[20]

With a growing consumer base outside the United States, and with uneven regulation across virtually all nations' legal and regulatory systems, companies and business associations consistently call for a level playing field in order to ensure fair competition – or, at a minimum, countervailing incentives to accept uneven regulatory standards.[21] Even companies prepared to act above the letter of the law can find their efforts undercut by those eager to seize on legal loopholes and weak links in the supply chain for their own gain.

In short, disparities in regulation further undermine the ability of governments to confront trafficking challenges.[22] As such, there is growing recognition that success in counter-trafficking requires a layered defense involving efforts to inculcate more rigorous industry participation. A growing litany of government, business and academic reports has concluded that if government fails to engage industry more effectively in the detection and disruption of illicit networks, it is less likely to find durable solutions.[23]

FOUR INDUSTRY SPACES OF SPECIAL INTEREST

Unlike previous efforts to educate or to help enforce regulatory standards that are largely antithetical to business interests, Stimson has worked with industry to develop ideas for positive inducements for heightened diligence and more effective information sharing. These measures will not be a panacea to transnational criminal activity. Instead, they promote a layered, cost-neutral and sustainable approach to prevent trafficking and proliferation.

The project focused on four industry spaces: **dual-use technology manufacturers, the radiopharmaceutical sector, shipping/transport firms and the insurance industry.**

These four spaces, of course, do not capture all global economic activity. They can, however, help build a template for a more comprehensive approach to industry that government and industry, working together, can adapt to relevant market and security variables. A description of the project rationale for selecting each of these industries, along with a brief overview of top-line findings, is below.

Dual-Use Technology Manufacturers: Notable Observations from Industry*

- Belief by some in USG that government can act as its own industrial and technological systems integrator – in fact, that role requires deep systems engineering expertise
- Need "trusted trader" regimes on export side
- Insufficient USG guidance on anticipated program/tech requirements
- Limited pool of highly skilled labor – need education/immigration changes
- "Information sharing" with USG largely a one-way relationship

** Derived from interviews with industry*

DUAL-USE TECHNOLOGY INNOVATORS AND MANUFACTURERS

The project team chose to engage the dual-use technology space in light of the sector's long history of regulation. This sector, and particularly the part that relates to the proliferation of nuclear weapons, has been the focus of US government regulators since the dawn of the nuclear age.

Furthermore, these dual-use technology innovators and manufacturers told a Stimson project team member that on several occasions US regulators have asked industry to sacrifice potentially legitimate sales in the interest of national security.[24] In some cases, those requests carried a thinly veiled threat of fines and prosecution. Yet despite these tactics and myriad regulations, incidents of technology diffusion continue, even from the United States.[25]

Incidents such as that described above involving Oerlikon Leybold surface with increasing frequency and suggest a growing challenge to the existing regimes, as well as the decreasing wherewithal of governments alone to implement effective solutions.[26] Unfortunately, to date, the nonproliferation community has not focused sufficient attention on quantifying the scope of the challenge and identifying industry's potential role in developing workable solutions that go beyond more intrusive state enforcement. According to some of the Stimson Center's industry participants, and to Oerlikon itself, the troubled state of government-industry relations in the United States has set back progress in establishing effective public-private partnerships even further than the lag seen in Europe.

SHIPPING INDUSTRY

If there is a sector that touches upon virtually every flow of contraband, be it WMD proliferation, narcotics, counterfeit intellectual property or small arms and light weapons, it is the legitimate shipping industry. Innovative transportation technologies have accelerated the transshipment of goods around the globe.

Shipping/Transportation Firms: Notable Observations from Industry*

- USG-designed incentives (as in C-TPAT) often are not meaningful or do not materialize as promised
- "Information sharing" with USG largely a one-way relationship
- Insufficient understanding by USG of many different business models across supply chain and transport space

** Derived from interviews with industry*

Containerization, larger and more efficient ships, roll-on/roll-off cargo container vessels, new loading and unloading tools, more efficient port management, improved logistics and satellite navigation and tracking all have become part of a critical system within which globalization itself has been able to flourish.

By 2007, the volume of international seaborne trade reached an unprecedented 8 billion tons. Even in the midst of a global economic slowdown, at any given moment, there are some 20 million intermodal freight transport containers moving around the globe. More than 4,600 ships carry many of those containers on over 200 million trips per year.[27]

However, as the global flow of legitimate goods has grown, so has the transshipment of illicit items, including small arms, drugs, counterfeit products and, perhaps most worrying, weapons-useable materials and technologies. In response, governments have introduced an array of rigorous security measures to help weed out contraband from the legitimate supply chain: the Customs-Trade Partnership Against Terrorism (C-TPAT), the Container Security Initiative, new air cargo security rules, the Trade Act of 2002 (including the 24-hour rule), the World Customs Organization Framework, the SAFE Ports Act and the Authorized Economic Operators (AEO) guidelines are just a few.

As with the dual-use technology sector, these additional regulations layered in the wake of the 9/11 terrorist attack have created similar push-back and criticisms from industry, rather than meaningful partnerships with mutual benefit. For instance, four years after 9/11, Customs and Border Protection (CBP) inspected less than 3 percent of the 20 million annual inbound shipments to the United States.

Unable to police the supply chain effectively, CBP introduced C-TPAT, which mandates that US companies

help shoulder the burden of cargo screening. While a reasonable premise, companies canvassed for this study routinely complained that participation in C-TPAT – today a near necessity for all major companies in the sector – offers few meaningful incentives. Further investigation reveals that those incentives were defined not by industry, but by government regulators and, as such, have in many cases failed to meet the minimal standards to provide meaningful benefit to industry.[28]

Providing proper incentives to the shipping industry, in addition to sound regulation, would better enlist the long-term support of legitimate supply chain companies and help counter the illicit flow of items around the globe. Identifying ways to transform the industry from a conveyor belt into a "choke point" for these illicit items without hampering the competitiveness of legitimate companies will be critical to prevent proliferation and other illicit trafficking.

RADIOPHARMACEUTICAL MANUFACTURERS

At present, more than 10,000 hospitals worldwide actively use radioisotopes to detect and treat diseases. Radiopharmaceutical research involves radioisotopes attached to drugs administered to patients for more than 50 different types of diagnostic tests.

Radiopharmaceutical Manufacturers: Notable Observations from Industry*

- Uneven regulatory treatment of certain imaging technologies
- Insufficient desire within USG for nuclear-science technology transfer to industry, even though it would be "win-win"

** Derived from interviews with industry*

And in the US alone, there are some 18 million nuclear medicine procedures per year among 305 million people.[29]

The bulk of radioisotopes used, like technetium-99, are derived from HEU, and the nonproliferation community has rightly raised concerns about the lack of regulation at both ends – from the major producers of medical isotopes to the sites that secure the material.[30] As new technologies are introduced, regulators are now starting to consider another critical component in the radiological supply chain: the actors between the industry and end-users, the diagnostic machine fabricators who represent the critical hub in the research, development and manufacturing sector.

Some in the nonproliferation community have advocated for the conversion of these facilities from HEU to low-enriched uranium (LEU) production.[31] Elected officials and non-governmental organizations also have pointed to the ease with which highly dispersible material, such as Cesium 137, could be removed from inadequately secured sites and the possibility of non-state actor use of a radiological dispersion device. Most point to hospitals and other treatment centers, but radiological sources are used also in the construction, petroleum and airline industries. In response, the US Department of Energy's Global Threat Reduction Initiative launched a voluntary program to secure this material.

INSURANCE PROVIDERS

The insurance industry is an essential partner to each of the above sectors. As such, its influence over the proliferation and counter-trafficking space, while indirect, is substantial. Insurance delivers essential services to the market that simultaneously could be leveraged and expanded to address global security challenges: risk sharing, price discovery and, in the interest of national security, the identification of risk mitigation measures. While risk sharing and

price discovery are attributes of every functioning insurance marketplace, industry – both insurers and insured – can help identify measures that would mitigate risks, reduce insurance costs and extend coverage. The market itself can be leveraged to develop new standards and to incentivize positive adherence to existing or new standards of self-regulation, as defined by these discrete industry sectors.

For industry, compliance with best-practice standards is voluntary but could be incentivized through multiple factors – including through insurance, thereby building a business case for heightened self-regulation. With standards, the insurance industry will benefit from better risk information, and potential claims will fall as compliance with standards increases. In addition, new types of coverage could be encouraged, including perhaps government-based incentives for offering nonproliferation or counter-trafficking mitigation in those policies. In that regard, several insurance industry representatives told the project team that the addition of coverage for chemical, biological, radiological and nuclear (CBRN) incidents under the Terrorism Risk Insurance Program was conceivable.

Insurance Providers: Notable Observations from Industry*

- State-based regulatory regime means industry does not share in many benefits that adjacent industries enjoy
- USG does not understand how insurance markets work, or how products could advance USG goals in some circumstances

** Derived from interviews with industry*

The Key Functions of Insurance: A Primer

Risk-sharing

Risk premiums from many different insured entities are pooled to cover potential losses. As a direct benefit of insurance, those at risk who comply with certain standards could pay a smaller premium to the insurer or have lower deductibles. When the insurer later uses accumulated funds to reimburse those parties suffering actual losses, both the insured and society benefit. While risk-sharing in itself may not directly reduce the likelihood or losses from a WMD terror event, most economic activities, from redevelopment of the World Trade Center site in New York to the reconstruction of the Mumbai hotels destroyed in the 2008 terrorist strikes there, could not happen without it. Insurers have guaranteed that private development can continue in the face of a rising WMD threat.

Price discovery

Price discovery involves assessments of the probability of an insured incident and its anticipated consequences. Insurers rely largely on computer models to help estimate these factors and insurers' potential payouts. While predicting the likelihood of catastrophic events is challenging, for illicit activities such as theft or diversion, the actuarial science perfected by the insurance industry, combined with computer-based simulations and modeling techniques, offer a major benefit to insured clients and perhaps even to governments seeking to prevent a range of illicit activities that can be modeled. However, given the limited loss history in terrorism- and WMD-related events, insurance pricing is difficult, and typically has relied on federal backstopping when it has been available.

Mitigation
By establishing insurance pricing and cover, the insurance industry mitigates undesirable behavior. This is the process by which insured parties take actions to reduce their expected losses in order to obtain lower premiums and lower deductibles, or to qualify for additional coverage. For example, one incentive to mitigate is created by risk-based premiums, whereby each insured party pays a premium commensurate with individual risk.

ASSUMPTIONS AND SCOPE

Two major assumptions have framed the project team's work with industry on identifying nonregulatory tools to prevent proliferation and related transnational crimes:

1. Governments' primary concern in the proliferation context is the prevention of a wider diffusion of materials, technologies and know-how to would-be proliferators at the state or sub-state levels. Conversely, private companies, rightly concerned with trafficking challenges, must also act on the basis of their core obligations to investors or shareholders. Yet despite these differing motivations, private industry can be brought more meaningfully into nonproliferation and counter-trafficking compliance beyond facile appeals to corporate social responsibility.

2. Legal regulation is and will remain a fundamental necessity. Moreover, for some mission areas, and for some functions, private sector cooperation is either more difficult to establish or altogether inappropriate. For instance, sharing certain intelligence with industry interlocutors, or engaging specific companies to the exclusion of others, is often illegal. Ensuring the appropriate balance between punitive regulation and positive incentives is more the focus of this report.

APPROACH

As noted above, economic globalization implies the need for a "threat-convergence" approach to counter-trafficking at the strategic level. Put differently, it requires a broader view of how illicit trafficking activities are situated within the complex, interdependent networks that drive the global economy.

According to multiple US intelligence sources interviewed by the authors, Western intelligence agencies have devoted much attention since 2001 to identifying connections between the trafficking in WMD items and materials, and the trafficking in other (unrelated) forms of contraband.

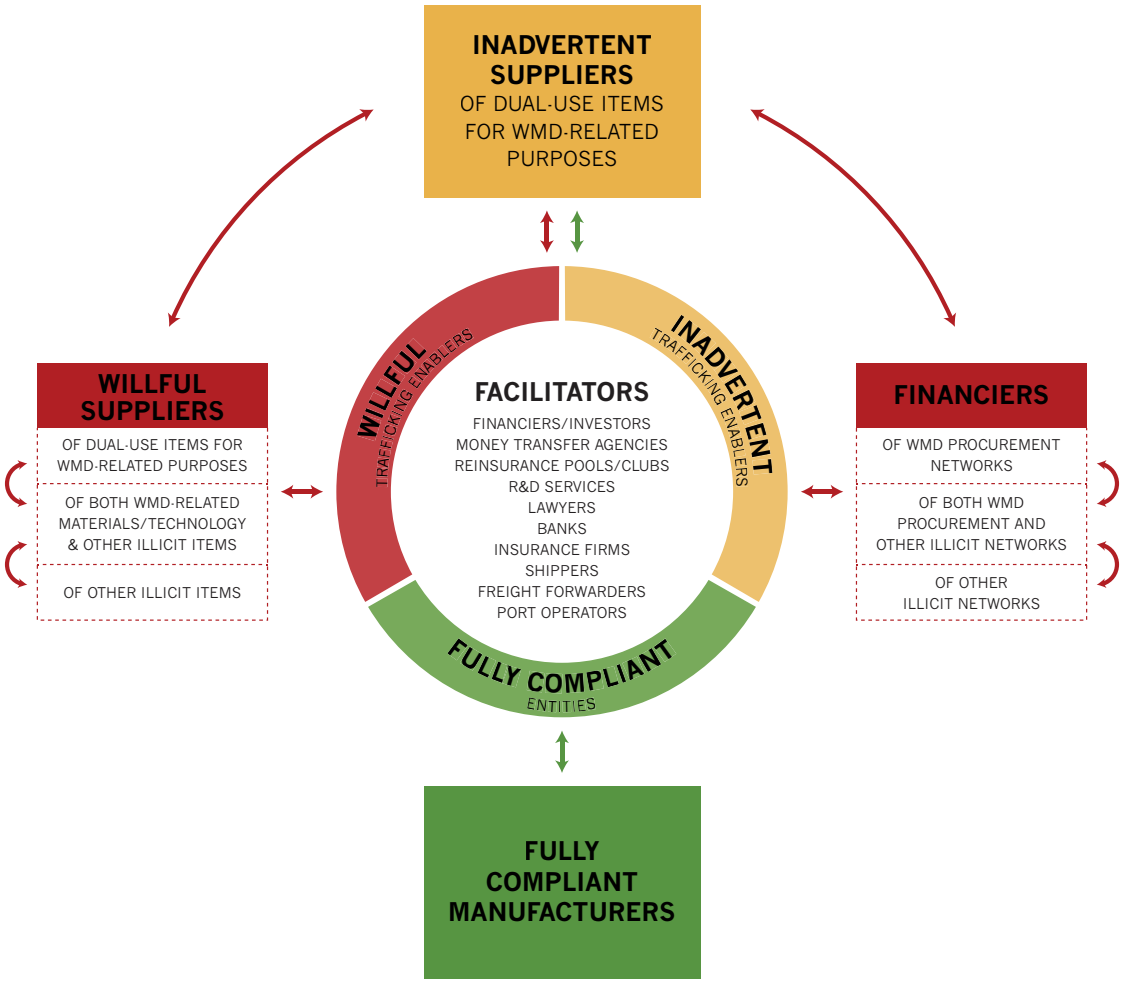
When proceeding with the strict parameters of producer and ultimate customer, evidence for these connections is limited. Yet recent incidents of proliferation also indicate that many of the "facilitator" industries – from shipping to insurance to banking – are common to multiple trafficking portfolios.

A WMD-crime-terrorism nexus is coming into view for many officials and experts.[32]

In short, the same ship carrying a dual-use nuclear item is equally capable of unwittingly conveying narcotics, counterfeit pharmaceuticals or even human slaves. As such, considered more expansively, various forms of illicit trafficking are likely to share some common attributes, *whether or not those commonalities are known at any point by any of the individuals or organizations involved*. Informed by this approach, the project team has explored how better to align industry incentives and different modalities for government-industry cooperation, without regard to a particular brand of proliferant activity.

Figure 2 is a stylized representation of the exchange in goods, services and information that ultimately might support global proliferation networks. It sets the parameters of the challenge beyond the producers of raw materials, technology innovators and manufacturers, and includes the spectrum of facilitator industries that are critical to supporting the proliferation of CBRN weapons, materials and components, as well as the global movement of licit and illicit goods more generally.

FIGURE 2
Links Between WMD Procurement and Other Illicit Networks: The "Facilitators" of Terrorism and Transnational Crime



The yellow circles mark the key points of interest. They capture network links – that is, the "commonalities" discussed above – between licit and illicit trade. In this case, legitimate firms, as well as deliberate traffickers of both WMD materials and other illicit goods, interact with some of the same actors from the "facilitators" space. Note that Figure 2 does not make any spatial representations, so the network linkage does not imply a synchronous or asynchronous overlap in physical location.

A particular virtue of the threat-convergence perspective is that it can lead stovepiped institutions to build capacity for sharing and adapting information and lessons learned. Security bodies at the national and international levels increasingly are drawing on this approach. Consider the views of this senior practitioner, recorded in a June 2010 study:

"The IAEA has amassed over fifty years of experience implementing … what was referred to by one senior IAEA official … as a 'vertical approach' to nuclear security aimed at securing radiological and nuclear materials – and blocking their illicit transfer – up and down domestic supply lines and decision-making chains within participating states. When the IAEA's vertical approach is linked to a horizontal approach embracing the programs of other anti-trafficking organizations, nuclear safety and security would be… advanced still further."[33]

But what would enhance this IAEA official's concept – what would position these newly linked anti-trafficking organizations to unlock the other critical set of tools in the threat-convergence toolkit – is an explicit strategy to leverage private sector resources and expertise. Formulating that strategy first requires an understanding of the challenges that must be navigated.

The simple desire to improve mission performance by enhancing public-private coordination is but one small step on the road to success. The project team reviewed a wide body of writing on this topic and incorporated relevant feedback from its own discussions with industry and government representatives. In trying to distill the most common and the most problematic challenges to coordination, three basic themes emerged: government-industry gaps in knowledge, in communication and in structural variables. It is important to emphasize that these themes are highly interrelated, with fluid boundaries separating them. The project team still found it helpful to conceptualize them independently, both for general understanding and for evaluating potential solutions.

KNOWLEDGE GAPS

ESTABLISHING A "CONOPS"

Even when they work in related fields or on shared problems, government and industry frequently remain ignorant of what the other party wants, needs or is empowered to do. Many times, this missing information takes the form of straightforward facts. Even though such a simple knowledge gap could quickly be remedied, it occasionally persists due to related communication problems, such as unease about sharing certain kinds of information. Whatever the cause, if these gaps are not recognized early in the process, they can lead to incorrect assumptions or unexplored opportunities.

SUBJECT MATTER EXPERTISE

In other cases, the knowledge gap centers more on technical information or subject matter expertise. On the whole, industry's profit motive drives innovation so rapidly that government – particularly in an open, capitalist system like the US – has great difficulty keeping pace "at scale." In other words, government is often unable to hire and retain a sufficient number of subject matter experts (SMEs) for tracking industrial and technological trends, and for supporting associated private sector outreach.

There is a similar problem in areas where government chooses to execute research and development (R&D) directly in support of mission requirements. In a time of intense budgetary pressures, these problems are certain to become more severe – though they might also prompt more innovative mechanisms. The CBRN context is perhaps one of the leading examples in this regard. A September 2012 report by a National Research Council panel recommended that the Department of Defense (DoD) consider shifting some of its CBRN technical research to the private sector, as the number of potential threat vectors continues to climb. Of particular interest, though, the report also encouraged a "tech watch" capability that would give relevant DoD offices "mechanisms for searching and identifying relevant breakthroughs in the literature and private sector."[34]

Stimson's industry and government interlocutors noted several specific knowledge gaps with greater frequency.

Of these, the project team found two to be most pertinent to future public-private coordination on trafficking issues:

1. **Within industry, companies in many sectors – not least in the shipping and transport space – need to develop greater sensitivity as to how illicit trafficking networks operate.** A basic example is the need to better track "red flag" information (e.g., various control lists published by government agencies, such as the Commerce Control List [CCL], specifying restricted dual-use items). The export control reform effort is likely to increase some of these problems in the short term. Many manufacturers of products currently listed on the US Munitions List will soon face a completely different set of compliance requirements, as some of these products are being migrated to the CCL. Small- and medium-sized businesses, in particular, are likely to need assistance in understanding the rule changes and developing compliant processes.

2. **Within government, the lack of knowledge of the insurance/reinsurance space is especially acute.** Stimson heard this concern from sources in government, industry and other think tanks and academic institutions. In some cases, even those government offices working frequently with the financial services and insurance industries had deficiencies in this regard. The project team was told of at least one instance in which the problem affected mission performance modestly but directly.

THE INTRA-INDUSTRY LANDSCAPE

A longer-term but equally important goal for government is to understand the intra-industry breakdown – the economic and political landscape determining what actors hold what influence. For instance, if a sector has multiple trade associations with at least some overlap, as often happens, which one has the most mindshare? Which standard-setting organizations (whether of a technical, managerial or other emphasis) seem to shape a particular sector's behavior the most? Occasionally, all of the institutional focal points for such matters can be found within the US. More often, though, these high-level questions of economic and political influence also have an international dimension. The answers do not necessarily turn exclusively on market share and revenue streams.[35] Moreover, these questions might prove sensitive in some contexts – particularly when a government official makes the inquiry – but Stimson found individual companies and trade associations to be open with their evaluations. The input from multiple sources revealed only occasional discrepancies that were rooted more in perspective and opinion than in fact or bad faith.

COMMUNICATION GAPS

VOCABULARIES AND CONCEPTUAL FRAMEWORKS RELATED TO RISK

Highly specialized communities of interest (COIs) often develop their own terminologies out of necessity, given the technical nature of their work. That issue falls more in the realm of knowledge gaps, discussed above. There is a separate language-related challenge that is subtler but, once identified, somewhat more tractable: differences

in how certain terms and concepts are used, adapted and interpreted. This challenge is rooted less in subject matter expertise than in organizational culture, priorities and associated processes. And once again, the key issues to consider are not only the government-industry differences, but also the intra-industry and intra-USG differences.

The language and concepts employed to describe *risk, risk management,* and *resilience* deserve special attention. Government and industry use these terms regularly when discussing topics like proliferation, supply chains and international trade. There are many fault lines along which such discussions can be diverted into other issues or break down into miscommunication and confusion. As a result, several recent and continuing efforts aim to promote shared conceptual frameworks.

For instance, the International Organization for Standardization (ISO) released its ISO 31000 series of standards for risk management processes in 2009, alongside a risk management vocabulary reference.[36] The Department of Homeland Security (DHS) issued its own risk management "doctrine" in April 2011.[37] The World Economic Forum's Risk Response Network has ongoing activities to develop what it calls "a blueprint for resilient supply chains." Its model deconstructs resilience into four variables: partnerships, policy, strategy and technology/IT.[38]

In June 2011, the European Commission launched a three-year project called CASSANDRA (Common Assessment and Analysis of Risk in Global Supply Chains), which is promoting use of the so-called Risk Based Audit (RBA) approach among European government agencies. Many government entities base their customs processes and other risk evaluations exclusively on the transaction-level data supplied by the importer/exporter for a particular shipment. In contrast, RBA seeks to incorporate information on underlying process management issues, including a company's internal security policies and standards.[39] Similar principles inform the "account management" concept that DHS's Customs and Border Protection (CBP) has sought to advance; we will briefly consider it in the next section.

Finally, there is much relevant work underway pursuant to the *National Strategy for Global Supply Chain Security,* released by the White House in January 2012. One of the implementation tasks, coordinated by DHS's Domestic Nuclear Detection Office and completed in late 2012, was a Radiological/Nuclear Global Supply Chain Risk Assessment. More to the point of harmonizing risk-related concepts, a January 2013 *National Strategy for Global Supply Chain Security Implementation Update* designated the following task as a "priority implementation activity" for 2013: "Develop and institutionalize a process to characterize and assess system-wide risk in coordination with industry and foreign government stakeholders globally."[40]

MISTRUST

Several types of trust-related issues can impede public-private engagements. An underlying issue, of course, is frequently the absence of any extensive relationships or shared cultural norms. For instance, government has an understandable desire to protect sources and methods on intelligence issues, and an understandable need to know what risk a private sector party's international economic activities might pose. Overcoming that type of trust deficit inevitably takes time, but the parties involved can shore up early progress by addressing some of the challenges above – not least, establishing a common operating picture and making explicit how key concepts are to be understood and operationalized. That preliminary work helps ensure that initial expectations and problem definitions are in sync. Otherwise, the parties have a greater tendency to operate at arm's length, forgoing any opportunities to venture outside whatever language might have been agreed upon to guide the relationship (if they were able to reach such an agreement, that is).[41]

Several industry interviewees cited a similar underlying dynamic: Some government security officials have a strong predilection to resort to familiar, traditional tools that "check a box" – that is, that endow these officials with a

sense of special insight into, and control over, industry behavior. One such tool, of course, is the license required for export of munitions or dual-use items (i.e., items on the US Munitions List or Commerce Control List, respectively). The Center's industry interlocutors cautioned that officials sometimes become too wedded to particular processes, and are unable or unwilling to consider other ways that security objectives could be achieved – especially if those other ways mean "letting go" of particular oversight mechanisms in some respect.

A more concrete, and critically important, trust-related challenge can be unwillingness or unease to share sensitive information, *apart* from any legal prohibitions related to classification or similar issues. For both government and industry, there is often fear that information disclosures will have unintended consequences if and when security measures lapse, whether due to human error or deliberate exploitation. Government's concerns on this front relate principally to national security and national economic competitiveness. Private sector concerns tend to focus on brand/reputational risks; liability risks related to, for instance, shareholder claims that a company's participation violates its fiduciary responsibilities; and firm-level or industry-level economic competitiveness. More specifically, the risk to intellectual property can be a stumbling block, particularly when cooperation entails electronic exchange of proprietary information.

Taking a step back, however, one actually sees potential for intellectual property rights (IPR) to be an area of common ground for government and industry in many contexts. As an Office of the National Counterintelligence Executive report to Congress in October 2011 stated:

> *"The migration of most business and technology development activities to cyberspace is making it easier for actors without the resources of a nation-state or a large corporation to become players in economic espionage. Such new actors may act as surrogates or contractors for intelligence services or major companies, or they could conduct espionage against sensitive US economic information and technology in pursuit of their own objectives."*[42]

Again, protecting against such exploitation benefits potential US corporate targets, as well as our broader national economic competitiveness. It also is a significant national security issue, as the recent scrutiny of counterfeit electronics in DoD supply chains has shown.[43] This issue, in its own right, could be a point of departure for many innovative public-private efforts at the nexus of IPR and information security. A number of Stimson's industry contacts emphasized some variation on this theme. Recent high-level policy statements suggest that senior USG officials also are willing to engage with industry in a proactive manner.[44]

Finally, trust can erode when past experience gives one party cause to doubt the other's credibility. Some of CBP's outreach efforts and "trusted trader" initiatives are instructive in this regard. CBP has adopted industry-friendly language and themes in programs intended to improve supply chain security. It now explicitly counts "economic competitiveness" among its mission objectives.[45] This might be what industry wants to hear, and it might indeed be the normative public policy outcome, but it is a major departure for an agency that has two centuries of experience with, and cultural orientation toward, functioning as an enforcer and revenue collector. Problems in making the transition have sometimes been interpreted by industry as an unwillingness to make the transition altogether.

For instance, under C-TPAT, US importers technically are entitled to certain trade facilitation benefits once certified for compliance with specified security standards. CBP claims these benefits include lower probability of border inspections and expedited processing procedures. Stimson's interviews indicate that, for many C-TPAT participants across a variety of sectors, rhetoric and reality have diverged significantly.

Another CBP effort that some industry observers feel has "overpromised and under-delivered" is the "account management" initiative, begun in 1997.[46] Account management refers to evaluating companies on the basis of historical, company-wide performance on security and compliance issues, rather than on a transactional basis, in which customs officials do not consider

factors beyond a given shipment's import/export documentation. In the latter case, companies essentially must start from scratch with every shipment, proving themselves time and again, with a highly compliant company being treated the same as a highly suspect company. When executed correctly, therefore, account management improves security through more sophisticated risk management (risk segmentation) and by providing an incentive for companies whose security practices are substandard to make improvements. It also promotes economic competitiveness by facilitating trade.

For most of its history, though, the account management initiative has been short-staffed and otherwise poorly resourced. As of May 2010, CBP estimated that it employed 50 full-time national account managers and about 400 part-time port account managers.[47] These personnel serve as primary points of contact for participating companies. The May 2010 figures show a significantly under-resourced effort.

This track record has cost CBP significant credibility with much of industry. But after urging further action to make good on the promise of C-TPAT and account management, several of Stimson's industry interlocutors added an important qualifier: "Action" need not mean "perfection." A good-faith effort to improve identified program deficiencies and to feed industry perspectives into the design of future efforts would be sufficient to maintain industry buy-in for now.[48]

And indeed, more recently, there have been some positive developments in account-based management by CBP, including its "co-creation" efforts and establishment of the Centers for Excellence and Expertise (CEEs).

A major test of CBP's ability to build on this progress and advance both economic and security goals is now at hand, as it begins implementation of a more formal "Trusted Trader Program." As one of the priority actions pursuant to the *National Strategy for Global Supply Chain Security*, the program ultimately is intended to be a government-wide framework that streamlines both requirements and benefits for disparate USG trade compliance initiatives. The initial phase of the program will be focused on imports, providing a limited number of companies with a consolidated process for participation in both C-TPAT and the Importer Self-Assessment (ISA) Program. Serving as lead agency for the new program will require substantial effort on CBP's part to collaborate with interagency and industry partners.

A separate example of counterproductive actions can be seen in several of the US Department of Commerce's (DOC) past efforts to modify regulations so as to address some of industry's most consistent objections. The October 2008 proposal to create a license exception for intra-company transfers (ICT) was a particularly disappointing experience for some of Stimson's industry interviewees.[49] To simplify, an ICT takes place when one part of a company provides a controlled item or sensitive information to another part of the same company – including, for example, an overseas affiliate – for internal company use. The definition also encompasses providing sensitive information to a foreign national working in the US (a "deemed export"). Under the DOC's Export Administration Regulations, every ICT requires a license.

For many companies, compliance with this mandate is quite time-consuming. Moreover, the firms most affected tend to have the most stringent supply chain security processes and the most frequently recurring transactions, so repeat licenses are arguably superfluous. Instead of providing these companies with a better alternative that also would enable DOC licensing officers to focus more time on higher-risk transactions, the 2008 proposal contained a byzantine compliance process of its own. Industry's cost-benefit assessment was that it made more sense to continue the status quo, seeking individual licenses for each transaction.

More recently, the strong and consistent outreach on export control reform (ECR) by Commerce and other departments has impressed many private sector stakeholders. In public and behind closed doors, several industry figures have said that, for the companies affected, the public-private dynamic is at one of its strongest points in recent memory. Much work remains for the larger ECR effort, but on that front and others, there seems to be a strong foundation for further progress.

The fact that CBP and Commerce both have made inroads in areas where they stumbled not long ago is testament to the importance of patience and persistence on the part of all involved in public-private initiatives. Yet in a competitive, profit-driven climate, industry is not usually best suited to patience. Thus the earlier struggles at CBP and Commerce also are an argument for government and industry to risk-manage their own process, as it were. Put differently, spending some additional time on the front end to identify more than one shared objective in the relevant problem space keeps some doors open even when another closes. In like manner, exploring more than one modality – for example, one highly formal mechanism with multiple parties, and one informal mechanism involving only a few parties – can allow for a pivot to firmer ground when one mechanism is not generating much traction.[50] This, of course, presumes that those involved know the options available to them, and the relative strengths and weaknesses of each.

STRUCTURAL GAPS

INSUFFICIENT EFFORTS TO SHARE LESSONS LEARNED

In both government and industry, Stimson found that new initiatives to facilitate public-private coordination often failed to build on previous efforts. Cross-functional initiatives, in which more than one professional/subject-matter community of interest (COI) was represented, were particularly susceptible in this regard. To an extent, this makes sense, as a single COI by definition has a shared history and shared conceptual approach that allows it to identify problems and next steps more easily. But it also is sobering, because many of the security challenges that will compel public-private approaches in the years ahead will require disparate COIs to pool capabilities and expertise.

In public remarks at a June 2012 panel discussion, Angela McKay of Microsoft's global security strategy and diplomacy team described four "phases of maturity" that she saw unfold first-hand in public-private collaborations:

1. ***Recognizing the need for a joint effort,*** with at least one government and one industry entity working on a common problem set.
2. ***Defining roles and responsibilities*** for a cooperative effort through basic mutual education, as well as exercises/simulations and similar steps.
3. ***Re-scoping the effort*** to a more focused, discrete space once it is clear how the effort is oriented to related initiatives.
4. ***Scaling the effort*** so that the solutions developed have greater reach but the associated processes do not become overly rigid and thereby stifle progress.

The problem, McKay added, was that many efforts over the years essentially had to reconstruct this road map from scratch, with participants proceeding in fits and starts. If they had known how their cooperation and scope of effort were likely to evolve, she said, it would have made a meaningful difference.[51]

Another important point embedded in McKay's model – essentially a corollary of her description of phase four – is the need for what might be called a preliminary "operational planning" phase. In other words, before embarking on any cooperative effort, it would be useful for all parties to gain a better understanding of the different modalities that could shape their interactions – from informal to highly formal – along with their relative advantages and disadvantages. In addition, this preliminary phase would provide situational awareness of any

related initiatives already underway, along with ideas for how a new effort might complement or otherwise connect to those related initiatives.

Developing an "operational plan" in this manner responds to the strategic imperative discussed above – the need for public-private relationships themselves to be "risk-managed" by identifying multiple potential objectives and the associated paths forward.

STOVEPIPING IN BOTH GOVERNMENT AND INDUSTRY

The need for greater interagency cooperation is clear in many contexts. What is somewhat rare amidst all the admonitions is quantified evidence of how poor coordination endangers security and economic competitiveness. A March 2013 article on the new Export Enforcement Coordination Center (E2C2), established as part of the administration's export control reform effort, provided such evidence.

The article documented several cases in which multiple agencies independently had been investigating trade violations or security threats, until the E2C2 flagged the potential for self-inflicted setbacks and established better situational awareness for all involved. By integrating case files from multiple agencies and cross-referencing target names with other data stores, such as phone numbers, the E2C2 found that about 60 percent of USG targets were being pursued by multiple agencies.[52] In the large majority of cases, the agencies had no knowledge of this wasteful and potentially counterproductive duplication.[53] One would hope such revelations encourage more unity of effort at higher levels of the departments and agencies shown to be complicit in such poor coordination.

With regard to the day-to-day operational needs of industry, a major problem is that 48 agencies have separate filing requirements for US importers and exporters, and some of the electronic interfaces they use are terribly antiquated and are not interoperable. (To be clear: The number of agencies with which any single company must file depends on the number and kind of products being imported/exported, as well as the location and identity of its trading partners.) Some agencies in the maritime space still require thick stacks of paper for each individual shipment.

Congress mandated streamlining of these processes in the 1993 Customs Modernization Act (part of PL 103-182), and implementation of that mandate took shape under the umbrella of the Automated Commercial Environment (ACE). Two decades later, ACE is incomplete. Only recently did work begin on incorporating data from beyond CBP into the most important component of Automated Commercial Environment: the International Trade Data System (ITDS). ITDS is to serve as industry's "single window," which is to say the vehicle to consolidate filing requirements from the 48 agencies noted above. The plodding pace in making ITDS fully operational has meant that true "account management" – in which the USG, working on a whole-of-government basis, can assess and incentivize a company as a whole enterprise – has not yet had even a fighting chance. In the words of the American Association of Exporters and Importers (AAEI): "[T]he single most significant stumbling block to progress is the current state of the ACE."[54]

All of this amounts to a major drag on economic competitiveness. It also represents a critical missed opportunity for the USG, acting within appropriate boundaries, to leverage an integrated set of historical and near-real-time trade data for missions related to national security and trade violations, such as IPR infringements. While the Trade Act of 2002 created a "firewall" between commercial and security-related trade data, leading industry figures have expressed support for the addition of "commercial targeting" to the permitted uses of security data.[55] Any initiatives to that end, of course, would require that government provide sufficient assurances to industry and the broader public regarding the potential for abuses.

Even the USG's more affirmative steps to work with industry are hampered

by stovepipes. One need only look at the sheer number of USG advisory committees, working groups and other bodies aiming to facilitate industry outreach. Recalling the four phases of maturity for public-private engagements articulated by McKay, one can see legitimate value in creating separate mechanisms to focus on discrete problem spaces. But as McKay emphasizes in her third phase, these multiple mechanisms deliver greater value only when they are coordinated – or at least have a basic awareness of one another. The project team found that this coordination typically is weak.

Many departments and agencies have earnestly sought to streamline and strengthen their industry engagement through higher-level reviews. A 2012 Defense Business Board (DBB) report marks a notable effort for DoD.[56] As in the DBB report, the scope for most of these assessments does not extend above the department level. But the USG organizational chart, to put it mildly, does not correspond neatly with private sector networks in general or transnational commercial networks specifically. It remains possible that the USG could derive additional value from these department-level studies through a comparative analysis to identify both gaps and redundant efforts.

Stimson found that industry suffered from stovepipes of its own. A fairly common problem was that communication across functions, or across communities of interest, was either infrequent or significantly inhibited by different cultures and objectives. The project team saw this across firms and, quite often, even within firms. Indeed, in the area of trade controls, it is almost a truism that a company's chief compliance officer operates in a different environment and pursues different goals than the same company's chief sales officer. Upon completion of a rigorous "process mapping" exercise to better understand the chain of transactions for a typical US export, a group of industry experts came to a more sweeping conclusion: "The limited horizontal integration of [the licensing, import, export, and logistics] competencies is the source of many misunderstandings. These misunderstandings typically result in shipment delays, increased risk, and unnecessary exposure for a company."[57]

Considering the government-industry challenges discussed above, the cross-boundary communication problem within industry is not altogether unexpected. But it does have an important implication for government-industry cooperation: Government is likely missing many opportunities for additional private sector support of its security objectives by engaging only limited constituencies among a larger pool of potential private sector interlocutors. "Industry" is far from monolithic.

One specific manifestation of cross-functional separation within industry merits special attention. Within companies – and essentially at any level of analysis one wishes to consider – we found a significant disjuncture between information risk/security officers on the one hand, and most other functional units and COIs on the other. To the particular question at hand, we saw limited evidence within industry that information security specialists had anything approaching a "common language" with subject matter experts in the CBRN domain.

Casual observers might not think this kind of disjuncture would have tangible or direct consequences. But with the growing centrality of the cyber domain in global economic and security dynamics, this is an area where improvement should be an urgent strategic priority within companies, within industries and in government-industry engagements. Here again, the nexus of IPR and information security might be common cause for all concerned.

SET THE RIGHT TONE IN INDUSTRY ENGAGEMENTS WITH THESE THREE MESSAGES

Let there be no confusion: For industry, tangible outcomes are paramount. That of course is why the issue of incentives is so important. But in listening to the project's private sector participants, it became clear that narrative and tone do matter for public-private engagements. In more practical terms, narrative and tone can significantly affect prospects for tangible outcomes. This was especially true in cases where industry felt that previous attempts to work with government had failed to deliver.

We have attempted to capture the high-level themes or "frames" that resonated most with industry, across sectors. They are presented here in three notional messages that should inform how government approaches its industry interlocutor(s), either before or during a public-private initiative.

As these themes started to crystallize for the Stimson project team, they were vetted with select industry figures. On the whole, these individuals expressed strong agreement that the three messages above would go far in establishing a more constructive tone and shaping more mutually beneficial outcomes. What was especially notable, however, was how engaged these individuals were when the Stimson team posed this question to them. Stepping back to think through big-picture issues of tone and process was not a luxury most of them normally had – and perhaps not an exercise that they would have considered useful, before being pressed.

Several even said it would be helpful to undertake a more extensive, more iterative effort to elaborate on such a list, yielding a sort of "framework of principles" for public-private mechanisms. One person suggested that a widely endorsed framework like this could then be adapted at the outset of any new initiative, with more granular statements for the given problem space (e.g., supply chain integrity) nested within the big-picture themes.

These ideas are not to be mistaken as an exercise in branding. Upon conveying such messages to industry, a USG component would have a finite window to translate words into action. Prolonged delay would be tantamount to a lost opportunity. This danger is one reason why we frame the messages with a degree of interaction and shared responsibility built in. The other reason we do so, of course, is that government simply will not be able to achieve by itself the embedded goals of capturing specific business model characteristics, identifying relevant and meaningful industry incentives, and so on – to say nothing of the ultimate national security objectives.

WHAT WOULD INDUSTRY LIKE TO HEAR FROM THE USG?*

1. On incentives that matter. . .

"The USG will consider a more diverse, more industry-relevant, more practically implementable set of incentives for coordinated security efforts – if you help us identify those incentives."

2. On different USG approaches to industry coordination for different business models. . .

"We recognize that 'one size does not fit all.' Help us ensure that we design our joint efforts in a way that reflects the specific business models of participating private sector actors, as well as the specific security goals of government. When we can build on an existing effort to the benefit of all involved, we will."

3. On reinventing "account management". . .

"To the maximum extent possible, the USG will take an 'end-to-end' view of your company's strategic and operational environments, and of all interactions between your company and all USG components. Ultimately, we want you to help us re-invent 'account management,' on a government-wide scale."

** To be clear: What we articulate here are merely stylized, hypothetical statements that a USG representative could deliver in dialogue with industry representatives. These statements capture high-level industry preferences in spirit and in substance.*

ENHANCE UNDERSTANDING OF THE INDUSTRY LANDSCAPE

How might government actually deliver these messages with credibility? And what comes next?

Stimson's private sector participants said on several occasions that one answer to both questions could be found in a more thoroughgoing and consistent effort by government to learn about the industry landscape. There already are several examples in the supply chain security space where the USG is taking on this challenge. For example, the National Customs Brokers and Forwarders Association of America (NCBFAA) recently established a series of education seminars for senior CBP officials. NCBFAA says that the goal is to help CBP better understand "the functions and capabilities of a customs broker so that this expertise can be better leveraged by CBP," even though the customs broker "must direct his primary loyalty" to his client, the US importer.[58]

While brokers (and freight forwarders on the outbound side) might strike some as playing unremarkable "middleman" roles, the NCBFAA initiative matters. Brokers and freight forwarders are increasingly influential in the modern economy, even if their growth prospects are uneven.[59] (In fact, one could argue that difficult economic periods heighten their profile in the security conversation.) They are a window onto many of the other "facilitators" cited earlier as key to understanding both licit and illicit trade. Couple their roles with ongoing changes within the transport/supply chain space, and the implications for law, regulation and security are significant.[60] In the words of NCBFAA President Darrell Sekin, "A customs broker assumes a special, unique place in accomplishing [CBP's] mission."[61]

Whatever the issue and whomever the participants, the structure and setting for less formal initiatives do deserve scrutiny. It might benefit the principal actors on both the government and industry sides for such initiatives to be convened by a third party with sufficient knowledge of, but not a vested interest in, the relevant industry and regulatory variables. A trusted third-party facilitator also can help such dialogues endure beyond a one-off meeting or navigate through especially difficult discussions.

Two other CBP outreach initiatives hold particular relevance for USG awareness of industry dynamics. One is establishment of the Centers for Excellence and Expertise (CEEs), a new model for oversight of US imports. The CEEs are sector-specific and mostly virtual organizations in which a central office patches in CBP's top industry experts when a relevant import-related issue arises, then broadcasts their assessment to all US ports of entry. In so doing, the CEEs aim to provide participating US importers faster and more consistent CBP decisions on clearing cargo for entry.

It bears mention here that the CEEs are one product of a new, overarching concept for industry engagement that CBP is aggressively publicizing. CBP calls it "co-creation." While there is no precise definition for the term, co-creation is part process and part ethos. It involves working with one or more stakeholder groups to iteratively design, implement and maintain a product or service. The term is borrowed from the management consulting world, which used it first in business-to-consumer and business-to-business (B2B) relationships. Some of the most common B2B applications center on supplier relationships and supply chain management more broadly.[62] While some might deride CBP's use of the term as window-dressing, Stimson's feedback from industry suggests a need to reserve judgment. One interviewee called the CEEs a "ray of hope" amidst an often-frustrating relationship with CBP.

The CEEs also are focal points for CBP to gather what it calls "trade intelligence" – essentially all manner of information that CBP could use for targeting, enforcement or broader situational awareness. Thus far, the trade intelligence function has been deployed at two CEEs: the electronics CEE in Los Angeles and the pharmaceuticals CEE in New York City.[63]

The second CBP outreach effort, also branded as "trade intelligence," is the Private Sector Industry Liaison Office (PSILO). The PSILO identifies suitable industry contacts within the customs compliance, security and supply chain sourcing departments of firms and trade associations. According to CBP, those representatives will then "provide critical insight to CBP on enforcement issues related to developments in the [IPR], anti-dumping and countervailing duty, and trade preference areas, as well as advise CBP on the latest industry-wide changes."[64]

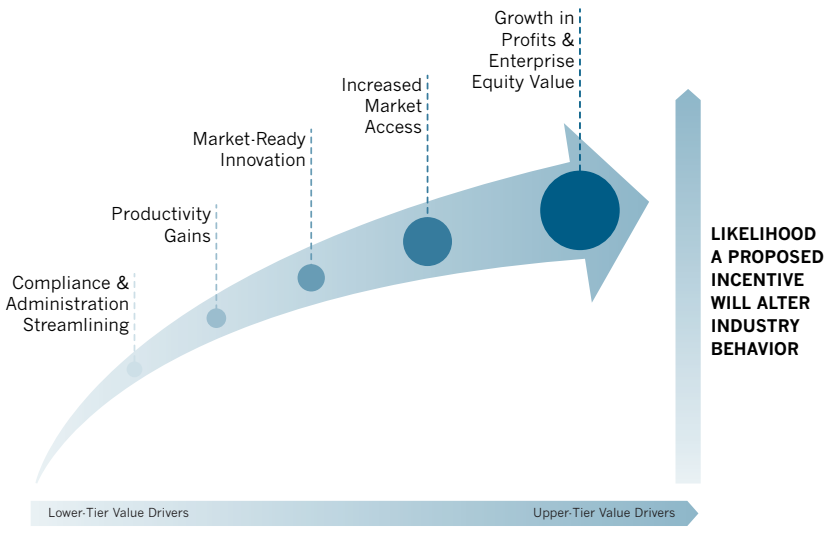
While the industry representatives and CBP officials are not physically co-located, what this initiative is attempting (both in kind and in degree) certainly will test boundaries in several respects. For instance, it will be intriguing to watch for any notable dissension among companies that are taking part in the PSILO concept and those that are not. As to the governance and accountability dimension, it must be noted that CBP is making no secret of this effort – but all the same, now is an appropriate time to raise the role of Congress. USG offices contemplating any sort of unconventional initiative along these lines in their private sector outreach – especially one that will not be in the public eye regularly – would do well to seek congressional input early and often.

LOOK TO THE FULL SPECTRUM OF INDUSTRY'S VALUE DRIVERS

To what end should such outreach mechanisms and other educational efforts be directed? One major need is now clear to the project: Government must significantly enhance its knowledge of the full spectrum of value drivers for its industry interlocutors. This is part and parcel of developing a well-rounded understanding of contemporary global economic networks, as already emphasized. But it also is a fundamental prerequisite to identifying what incentives can elicit meaningful industry engagement in security dialogues.

Figure 3 depicts a simplified view of how industry evaluates any given government-proposed incentive against its full range of value creation opportunities. This depiction is based on input from one of Stimson's industry participants. The simple but striking fact is that most of the public-private narrative on incentives for security coordination is anchored in the lower left portion, the compliance and administration area.

FIGURE 3
A Simplified Industry Perspective: Assessing the True Significance of "Incentives"



WHERE A PROPOSED INCENTIVE FALLS AMONG INDUSTRY VALUE DRIVERS

In large part, this compartmentalized thinking appears to have its roots in the same stovepiping and communication challenges we highlighted above. Most government officials tend to deal with a limited breadth of issues in their work, and their mental models for those issues have a similar scope and orientation. To the extent their work involves communicating across the public-private divide (e.g., on customs matters), the substance of those interactions likewise does not typically depart from a limited range – the transactional, business-as-usual range. These are dangerous tendencies for a government that wants to leverage private sector advantages in a fast-paced market environment. The USG must think more expansively about how it can fashion incentive structures that transcend the transactional level.

To illustrate, focus on just one of the higher-level value drivers in our visual: innovation. Some of Stimson's industry participants voiced dismay that potential commercial applications of USG-funded technologies did not figure more prominently in their conversations with government. Some in government might not see the merit or potential for technology transfers. But it is important to realize how rapidly and effectively industry can extend and rejuvenate the innovation cycle.

One instructive story in this regard is the commercialization of Global Positioning System (GPS) capabilities. The US steadily increased GPS functionality for civilian and commercial use after the end of the Cold War, with a major breakpoint coming in the Clinton administration's March 1996 policy statement.[65] While hopes were high, consider how uncertain the market prospects for GPS were at the time – even to those well acquainted with its underlying technologies and the contemporary business environment:

> *"Like other information-based technologies, the generic applicability of GPS makes it an enabler of productivity improvements through reducing costs, enabling new functions or enhancing revenues. The economic benefits of civil and commercial applications of GPS are thus broader than might be measured by sales of GPS equipment and service-related sales alone. At the same time, projecting future benefits is uncertain at best – it is difficult to predict where GPS-dependent productivity benefits might be found in the economy. Lowering the cost of using GPS is seen by industry as a crucial aspect for the growth of GPS, not only in terms of increasing demand from people who know what they want to use GPS for, but also in terms of encouraging experimentation with GPS by persons who are not sure if it will be useful."*[66]

As the conclusion of this passage notes, technology transfer can enable a virtuous cycle of innovation, even if immediate private sector applications are not apparent. Initial innovations, though modest, can drive costs down to the point that a technology reaches critical mass among interested firms. The broader experimentation makes substantial breakthroughs more likely.

A more comprehensive framing of industry value drivers is also a fitting backdrop against which to reiterate our earlier point about intellectual property and information security. Intellectual property is a tremendous store of value for many US firms – a resource to defend, yes, but also a resource to leverage proactively for new growth. The USG advances both public and private sector interests when it empowers trusted partners in industry to put potentially valuable knowledge or technology to productive ends, and when it helps create secure channels to share information around the world. Indeed, the free flow of information across borders will be increasingly vital.[67] There are several projects and programs across government that provide positive examples in this regard.[68]

DIVERSIFY THE USG "PORTFOLIO" OF OUTREACH TOOLS

As emphasized earlier, it is crucial that government be able to draw on a fuller set of tools in working with industry, underpinned by a better understanding of what has and has not been effective in past efforts. Part of the work here is learning the comparative advantages of different modalities, particularly as they are suited to the relevant mission area.[69]

A more fundamental task is establishing a capability to capture those lessons and put them in a broader framework. Many in senior USG positions recognize this need, as evidenced by an April 2013 "best practices guide" that the National Security Staff developed for use by agencies.[70] But the perspectives of industry figures with substantial experience in public-private efforts are at least as valuable. Further work to collect their views and identify major themes is imperative. Recent USG efforts to update the National Infrastructure Protection Plan (NIPP) and evaluate the Critical Infrastructure Partnership Advisory Council (CIPAC) model serve as reminder how fluid the contemporary security and economic environment is, and how difficult this work can be.[71]

To combine several of the threads woven throughout earlier discussion: Industry figures who have worked in cross-functional settings on a problem involving information risk, or secure information-sharing, deserve particular focus. More generally, any past effort in either government or industry that has succeeded in breaking down stovepipes and spurring cross-functional problem solving should be examined carefully.

The clear limits on governments' reach, and the central role of industry in global commerce and technology transfer, mean the US government must adapt in order to identify and disrupt rapidly evolving illicit trafficking networks. Adaptation in this environment does not only entail employing conventional tools in a different way or at a different pace. It also means adding new tools, reassessing how various stakeholder groups should relate to one another and making sometimes difficult decisions about how to reach that end.

Moving beyond direct government enforcement, and finding complementary models of industry-driven countermeasures, is now essential to prevent proliferation and other forms of illicit trafficking. To be sustainable, those models will need to accommodate the private sector's profit motive. The modern-day Oerlikon, professing a "corporate goal of actively supporting a policy of non-proliferation [that] has priority over commercial interest … [w]ithout prejudice to the legal permissibility of a specific transaction," is the exception that proves the rule.[72]

Accordingly, government will need to help fashion an environment and an incentive structure – all of which can be cost-neutral – that elicit durable industry support for its security objectives. To get there, it must first enhance its knowledge of the industry landscape. A good place to start is the assorted mix of "facilitators" that enable cross-border flows of goods and technologies by underpinning a physical and informational infrastructure for global trade.

To be sure, governments never will be able to innovate – organizationally, statutorily, or otherwise – at the speed of 21st-century commerce. Their efforts to respond more flexibly to market realities are bound to remain imperfect, always demanding reappraisal. But it is equally clear that, even in the short term, meaningful progress is within reach.

ABOUT THE AUTHORS

Nate Olson is research associate for the Managing Across Boundaries Initiative at Stimson. He works with both industry and government to facilitate models of public-private cooperation that better align the market and regulatory environment with US and global security interests. This role continues Olson's long record of research, analysis, and pragmatic stakeholder engagement on these issues. His graduate studies examined the rise of private regulatory systems for transnational supply chains and the interrelationship between public and private forms of governance. He also has extensive experience working with government agencies, civil society groups, and the business community on issues including enterprise risk management, trade facilitation, cybersecurity, and cross-functional teaming. Olson previously served as director of government relations for the Project on National Security Reform.

Brian Finlay is the managing director at Stimson, and also directs the Center's Managing Across Boundaries Initiative. His areas of expertise include nonproliferation, transnational crime, counter-trafficking, supply chain security and private sector engagement. Finlay is also an Adjunct Instructor in the School of International Service at American University in Washington. Prior to joining Stimson, Finlay served four years as executive director of a Washington-based lobbying and media campaign focused on counterterrorism issues, a senior researcher at the Brookings Institution, and a program officer at the Century Foundation. He was a project manager for the Laboratory Center for Disease Control/ Health Canada, and worked with the Department of Foreign Affairs and International Trade. He sits on the advisory board of Trojan Defense, LLC, and is a member of the board of directors of iMMAP, a pioneering organization leading the way forward in the effective use of information management practices in the service of humanitarian relief and development.

ABOUT THE MANAGING ACROSS BOUNDARIES INITIATIVE

The Managing Across Boundaries Initiative works to address an increasing array of transnational challenges – from WMD proliferation and the global drug trade, to contemporary human slavery, small-arms trafficking and counterfeit intellectual property – by looking for innovative government responses at the national, regional and international levels, and for smart public-private partnerships to mitigate these threats. Our experts and researchers work to conceptualize and catalyze whole-of-society solutions to the most pressing transnational challenges of our day.

ABOUT THE STIMSON CENTER

Founded in 1989, the Stimson Center is a nonprofit, nonpartisan institution devoted to enhancing international peace and security through a unique combination of rigorous analysis and outreach.

The center's work is focused on three priorities that are essential to global security:

Strengthening institutions for international peace and security.

Building regional security.

Reducing weapons of mass destruction and transnational threats.

The Stimson Center's approach is pragmatic – geared toward providing policy alternatives, solving problems and overcoming obstacles to a more peaceful and secure world. Through in-depth research and analysis, the Center seeks to understand and illuminate complex issues. By engaging policymakers, policy implementers and nongovernmental institutions as well as other experts, Stimson crafts recommendations that are cross-partisan, actionable and effective. The center is honored to have received the 2013 MacArthur Award for Creative and Effective Institutions.

Online at www.stimson.org.

1. International Atomic Energy Agency, "Illicit Trafficking Database" (now technically the Incident and Trafficking Database), http://www-ns.iaea.org/security/itdb.asp; see also 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 Press, 2007).

2. A non-American company was deliberately selected for this illustration. For good reason, private companies are rarely willing to openly discuss export control violations. Some major US firms, however, have constructively engaged on best practices for preventing illicit diversions of technology. See, e.g., Kevin Cuddy, export controls manager, General Electric, "Compliance with Targeted Sanctions: Watchlist Screening" (Washington: Stimson Center, 2011), http://www.stimson.org/compliance-with-targeted-sanctions-watchlist-screening/.

3. US Department of State, Office of the Spokesperson, "Department of State Concludes Settlement of Export Violations by Meggitt-USA, Inc.," Aug. 23, 2013, http://www.state.gov/r/pa/prs/ps/2013/08/213483.htm.

4. For a more comprehensive inventory of major violations, see the US Department of Justice's running update: "Summary of Major US Export Enforcement, Economic Espionage, Trade Secret and Embargo-Related Criminal Cases" (Washington: US Department of Justice, Feb. 2013), http://www.justice.gov/nsd/docs/export-case-fact-sheet-201302.pdf.

5. See Peter Andreas, "America and Illicit Globalization in the Twenty-First Century," Chap. 16 in *Smuggler Nation: How Illicit Trade Made America* (New York: OUP, 2013). See also: Susan Offutt, chief economist, Government Accountability Office, "Intellectual Property: Insights Gained from Efforts to Quantify the Effects of Counterfeit and Pirated Goods in the US Economy," written testimony submitted to the House Energy and Commerce Committee, Subcommittee on Oversight and Investigations, hearing on "Cyber Espionage and the Theft of US Intellectual Property and Technology," Washington, July 9, 2013 (Washington: Government Accountability Office, 2013), http://www.gao.gov/assets/660/655781.pdf. See also: Office of the Director of National Intelligence, "Transnational Organized Crime (TOC): A Perspective from the Intelligence Community," April 2013. While this last item is interesting in several respects, note that it does not reflect a coordinated position of either the USG or the Intelligence Community.

6. The International Action Network on Small Arms, "Gun Violence: The Global Crisis" (London: International Action Network on Small Arms, 2007), http://www.iansa.org/system/files/GlobalCrisis07.pdf.

7. Kimberly Thachuk, ed., *Transnational Threats: Smuggling and Trafficking in Arms, Drugs, and Human Life* (Westport, Conn.: Praeger Publishers, 2007), 65.

8. US Department of State, *Trafficking in Persons Report* (Washington: US Department of State, June 2012), http://www.state.gov/documents/organization/192587.pdf.

9. International Atomic Energy Agency, "IAEA Incident and Trafficking Database (ITDB): 2013 Fact Sheet" (Vienna: IAEA Office of Nuclear Safety, 2013), http://www-ns.iaea.org/downloads/security/itdb-fact-sheet.pdf.

10. Debra Decker, "Before the First Bomb Goes Off: Developing Nuclear Attribution Standards and Policies," Discussion Paper #2011-03 (Cambridge, Mass.: Belfer Center for Science and International Affairs, 2011), 12, http://belfercenter.ksg.harvard.edu/files/Decker_DP_2011_FINAL.pdf.

11. International Chamber of Commerce, Counterfeiting Intelligence Bureau, *Countering Counterfeiting: A Guide to Protecting and Enforcing Intellectual Property Rights* (Paris: ICC Publishing, 1997); United Kingdom and Organisation for Economic Co-operation and Development, *The Economic Impact of Counterfeiting and Piracy: Executive Summary* (Paris: OECD Publishing, 2007), http://www.oecd.org/dataoecd/13/12/38707619.pdf.

12. Moises Naim, *Illicit: How Smugglers, Traffickers, and Copycats are Hijacking the Global Economy* (New York: Anchor Books, 2006), 16.

13. United Nations Office on Drugs and Crime, 2008 World Drug Report (New York: United Nations Office on Drugs and Crime, 2008), http://www.unodc.org/documents/wdr/WDR_2008/WDR_2008_eng_web.pdf.

14. Sen. Jim Webb, D-Va., prepared statement for the Joint Economic Committee, hearing on "Illegal Drugs: Economic Impact, Societal Costs, Policy Responses," Washington, June 19, 2008 (Washington: US Government Printing Office, 2009), 34-35, http://www.gpo.gov/fdsys/pkg/CHRG-110shrg44772/pdf/CHRG-110shrg44772.pdf.

15. National Drug Intelligence Center, *The Economic Impact of Illicit Drug Use on American Society* (Washington: US Department of Justice, 2011), ix, http://www.justice.gov/archive/ndic/pubs44/44731/44731p.pdf.

16. John Rollins and Liana Sun Wyler, *Terrorism and Transnational Crime: Foreign Policy Issues for Congress* (Washington: Congressional Research Service, 2012), http://www.fas.org/sgp/crs/terror/R41004.pdf.

17. David M. Luna, remarks at the Trans-Atlantic Symposium on Dismantling Transnational Illicit Networks, Session I, Lisbon, Portugal, May 17, 2011, http://www.state.gov/j/inl/rls/rm/164306.htm.

18. Anthony P. Placido, statement before House Committee on Oversight and Government Reform, Subcommittee on National Security and Foreign Affairs, hearing on "Transnational Drug Enterprises (Part II): Threats to Global Stability and US Policy Responses," Washington, March 3, 2010, http://www.justice.gov/dea/pr/speeches-testimony/2012-2009/ct030310.pdf.

19. Brian Michael Jenkins, *Will Terrorists Go Nuclear?* (Amherst, N.Y.: Prometheus Books, 2008).

20. Finlay interviews, 2008-2011.

21. See, e.g., the Customs-Trade Partnership Against Terrorism (C-TPAT), which offers benefits to private sector companies that meet or exceed C-TPAT supply chain security criteria and best practices. See also: Business Roundtable, *Roadmap for Growth* (Washington: Business Roundtable, 2011), http://businessroundtable.org/uploads/studies-reports/downloads/Roadmap_for_Growth_Full_Report_1.pdf; and Center for Global Regulatory

Cooperation, *GRC Report* (Washington: US Chamber of Commerce, 2010), http://www.uschamber.com/sites/default/files/grc/GRC_Inside.pdf.

22. See, e.g., Moises Naím, *Illicit*; David Albright, *Peddling Peril: How the Secret Nuclear Trade Arms America's Enemies* (New York: Free Press, 2010); Michael Kenney, *From Pablo to Osama: Trafficking and Terrorist Networks, Government Bureaucracies, and Competitive Adaptation* (University Park, Pa.: Penn State University Press, 2008); Leslie Holmes, ed., Terrorism, *Organised Crime and Corruption: Networks and Linkages* (Cheltenham, UK: Edward Elgar Publishing Ltd., 2007); Willem van Schendel and Itty Abraham, eds., *Illicit Flows And Criminal Things: States, Borders, And the Other Side of Globalization* (Bloomington, Ind.: Indiana University Press, 2005); Richard Friman and Peter Andreas, eds., *The Illicit Global Economy and State Power* (Lanham, Md.: Rowman & Littlefield Publishers, 1999); Catherine Collins and Douglas Frantz, *Fallout: The True Story of the CIA's Secret War on Nuclear Trafficking* (New York: Free Press, 2011).

23. Gretchen Hund and Amy Seward, "Self-Regulation to Promote Nonproliferation," *Public Interest Report* (Spring 2011), http://www.fas.org/pubs/pir/2011spring/Self-Regulation.pdf; Chemonics International, *USAID Anti-trafficking in Persons Programs in Asia: A Synthesis,* (Washington: Chemonics International, 2009), http://pdf.usaid.gov/pdf_docs/PDACT220.pdf; Ian Stewart, "Antiproliferation: Tackling Proliferation by Engaging the Private Sector" (Cambridge, Mass.: Project on Managing the Atom, Harvard University, October 2012), http://belfercenter.hks.harvard.edu/files/Antiproliferation-Layout-final.pdf; US Chamber of Commerce, "US Chamber Applauds Public-Private Partnership in Defeating Counterfeiting Ring," July 24, 2007, http://www.uschamber.com/press/releases/2007/july/us-chamber-applauds-public-private-partnership-defeating-counterfeiting-rin.

24. Finlay interviews, 2008-2011.

25. A casual survey of the Department of Commerce's annual reports to Congress reveals a steady increase in the number of criminal cases targeting export control violations: 27 in 2001 (23 against corporations), 31 in 2005 (10 against corporations), and 71 in 2010 (41 against corporations). See US Department of Commerce, Bureau of Industry and Security, *Bureau of Industry and Security Annual Report for Fiscal Year 2002* (Washington: US Department of Commerce Bureau of Industry and Security, 2003), 57-62, http://www.hsdl.org/?view&did=3855; US Department of Commerce, Bureau of Industry and Security, *Bureau of Industry and Security Annual Report for Fiscal Year 2005* (Washington: US Department of Commerce, Bureau of Industry and Security, 2006), 37-40; and US Department of Commerce, Bureau of Industry and Security, *Annual Report to the Congress for Fiscal Year 2010* (Washington: US Department of Commerce, Bureau of Industry and Security, 2011), 25-40, http://www.bis.doc.gov/index.php/forms-documents/doc_view/656-bis-annual-report-2010. Also see: US Department of Justice, "Summary of Major US Export Enforcement, Economic Espionage, Trade Secret, and Embargo-Related Criminal Cases" (Washington: US Department of Justice, 2013), http://www.justice.gov/nsd/docs/export-case-fact-sheet.pdf.

26. Eric Lipton, "US Alarmed as Some Exports Veer Off Course," New York Times, April 2, 2008, 1.

27. James S. Cannon, *Container Ports and Air Pollution: An Energy Futures Inc. Study* (Boulder, Colo.: Energy Futures Inc.: 2009), http://www.mvo.nl/Portals/0/duurzaamheid/biobrandstoffen/nieuws/2009/05/2009PortStudy.pdf.

28. Industry motivations are often misunderstood by those outside the relevant sectors. For example, US regulatory authorities and academics have long assumed that the growth of piracy off the Horn of Africa has had a significant detrimental effect on global shipping interests. While large shipping firms like Maersk recognize that piracy has raised costs, for most major firms, these costs are viewed as eminently manageable. Industry estimates the "cost" of piracy at $12 billion per year. While this may seem significant, across a $12 trillion dollar industry, piracy is viewed as a modest tax on the global economy. Accordingly, the global shipping industry often is not as concerned about terrorism or piracy as it is about insufficient physical port infrastructures around the world, corruption and ungoverned spaces in foreign countries, or pilferage. Based on interviews by Brian Finlay on Oct. 26, 2011. See also Lara Sowinski, "Are DHS Security Initiatives Living Up To Their Promises?" (World Trade WT100, Jan. 1, 2005) and Barry Brandman, "Security Brief: It May not be Perfect, but C-TPAT's Here to Stay" (DC Velocity, Nov. 2005), 35-38.

29. World Nuclear Association, "Radioisotopes in Medicine" (Oct. 2001), http://www.world-nuclear.org/info/inf55.html.

30. Today, there are five major producers of medical isotopes: MDS Nordion (Canada), TycoHealthcare/Mallinckrodt (The Netherlands), Institut National des Radioéléments (Belgium), NECSA/NTP (South Africa), and Covidien (Ireland). Together, they provide more than 95 percent of global supply.

31. Cristina Hansel, "Nuclear Medicine's Double Hazard: Imperiled Treatment and the Risk of Terrorism," *Nonproliferation Review* vol. 15, no. 2 (July 2008): 185-208.

32. See, e.g., James Clapper, "Worldwide Threat Assessment of the US Intelligence Community," statement to US Senate Select Committee on Intelligence (Washington: March 12, 2013), 5, http://www.hsdl.org/?view&did=733905; see also George Mason University Terrorism, Transnational Crime and Corruption Center, *Criminal Networks, Smuggling, and Weapons of Mass Destruction*, conference report (March 2010), https://www.hsdl.org/?view&did=715924.

33. Geneva Center for Security Policy and Institute for Foreign Policy Analysis, *A Comprehensive Approach to Combating Illicit Trafficking* (Cambridge, Mass.: Institute for Foreign Policy Analysis, 2010), 17-18.

34. Committee on Determining Core Capabilities in Chemical and Biological Defense Research and Investment; Board on Chemical Sciences and Technology; Division on Earth and Life Studies; National Research Council, *Determining Core Capabilities in Chemical and Biological Defense Science and Technology* (Washington: National Academies Press, 2012), 64.

35. See, e.g., Tim Büthe and Walter Mattli, *The New Global Rulers: The Privatization of Regulation in the World Economy* (Princeton, N.J.: Princeton University Press, 2011).

36. See International Organization for Standardization, *ISO 31000:2009 Risk management—Principles and guidelines,* and *ISO Guide 73:2009 Risk management—Vocabulary* (Geneva: International Organization for Standardization, 2009).

37. US Department of Homeland Security, *Risk Management Fundamentals: Homeland Security Risk Management*

Doctrine (Washington: US Department of Homeland Security, 2011), http://www.dhs.gov/xlibrary/assets/rma-risk-management-fundamentals.pdf.

38. See, e.g., World Economic Forum and Accenture, *Building Resilience in Supply Chains* (Cologny, Switzerland: Word Economic Forum, 2013), 21.

39. CASSANDRA Consortium, "Project Organization," http://www.cassandra-project.eu/articles/risk-assessment.html.

40. White House, National Security Staff, *National Strategy for Global Supply Chain Security Implementation Update* (Washington: The White House, 2013), 8-9, http://www.whitehouse.gov/sites/default/files/docs/national_strategy_for_global_supply_chain_security_implementation_update_public_version_final2-26-131.pdf.

41. John Forrer et al., "Public-Private Partnerships and the Public Accountability Question," *Public Administration Review* (May/June 2010): 479-80.

42. Office of the National Counterintelligence Executive, *Foreign Spies Stealing US Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage*, 2009-2011 (Washington: Office of the National Counterintelligence Executive, Oct. 2011), 10.

43. See, e.g., US Senate Armed Services Committee, *Inquiry into Counterfeit Electronic Parts in the Department of Defense Supply Chain*," S. Rpt. 112-167 (Washington: US Government Printing Office, 2012). See also: "Detection and Avoidance of Counterfeit Parts," National Defense Authorization Act for Fiscal Year 2012, Public Law 112-81, Section 818 (Washington: US Government Printing Office, 2011). See also: Catherine Ortiz, "DoD Trusted Foundry Program: Ensuring 'Trust' for National Security & Defense Systems," presentation to National Defense Industrial Association, Systems Engineering Division meeting (June 20, 2012), http://j.mp/Zcunnd.

44. See, e.g., Executive Office of the President, *Administration Strategy on Mitigating the Theft of US Trade Secrets* (Washington: The White House, Feb. 2013), www.whitehouse.gov//sites/default/files/omb/IPEC/admin_strategy_on_mitigating_the_theft_of_u.s._trade_secrets.pdf.

45. See, e.g., US Customs and Border Protection, "CBP Highlights Recent Trade Successes," Feb. 13, 2012, http://www.cbp.gov/xp/cgov/newsroom/news_releases/national/2012_nr/feb_2012/02102012_5.xml.

46. US Department of Homeland Security, Bureau of Customs and Border Protection, Trade section, Account Management page, http://www.cbp.gov/xp/cgov/trade/trade_programs/account_management/.

47. Frank Vargo, vice president of international economic affairs, National Association of Manufacturers, testimony before the House Ways and Means Committee, Subcommittee on Trade, hearing on "Customs Trade Facilitation and Enforcement in a Secure Environment," Washington, May 20, 2010, http://www.nam.org/~/media/9091BD4E1CA64EE28AF17FE9345099A7/NAM_Testimony_WMs_Customs.pdf.

48. Olson/Finlay interviews with shipping and logistics firms, 2012-2013.

49. Department of Commerce, Bureau of Industry and Security, "Export Administration Regulations: Establishment of License Exception Intra-Company Transfer (ICT)," *Federal Register* vol. 73, no. 193 (Oct. 3, 2008), http://www.gpo.gov/fdsys/pkg/FR-2008-10-03/pdf/E8-23506.pdf.

50. The project team thanks an interviewee from the dual-use technology space for this insight.

51. Angela McKay, public remarks, Center for Strategic and International Studies, Washington, June 22, 2012.

52. As this anecdote shows, communications providers are one of the many industry "facilitators" whose activities can help identify dispositive network ties when traditional investigative and analytic methods cannot. However, recent revelations of the US Intelligence Community's data mining programs compel an important cautionary note. Government-driven efforts to identify these network ties must give due regard to concerns related to privacy and economic competitiveness. Losing the trust of valued partners is not easily remedied.

53. John Shiffman, "New Anti-Smuggling Center Uncovers Internal Surprises," Reuters, March 6, 2013, http://www.reuters.com/article/2013/03/06/us-usa-smuggling-idUSBRE9251FV20130306.

54. American Association of Exporters and Importers, comments submitted to House Ways and Means Committee, Subcommittee on Trade, hearing on "Supporting Economic Growth and Job Creation through Customs Trade Modernization, Facilitation, and Enforcement," May 17, 2012, Serial No. 112-TR05 (Washington: US Government Printing Office, 2012), 143, http://www.gpo.gov/fdsys/pkg/CHRG-112hhrg80260/pdf/CHRG-112hhrg80260.pdf.

55. Vargo testimony before the House Ways and Means Committee, May 20, 2010, 8.

56. Defense Business Board, *Public-Private Collaboration in the Department of Defense*, Report FY 12-04, (Washington: Defense Business Board, 2012), http://dbb.defense.gov/pdf/FY12-04publicprivatecollaborationDOD_0984.pdf.

57. Commercial Operations Advisory Committee to US Customs and Border Protection, Export Mapping Work Group, "Area of Opportunity for Licensed Commodities: Narrative" (Aug. 2013), 2, http://www.cbp.gov/linkhandler/cgov/trade/trade_outreach/coac/coac_13_meetings/aug7_meeting_dc/coac_lic_comm.ctt/coac_lic_com.pdf.

58. Darrell Sekin Jr., president, National Custom Brokers and Forwarders Association of America, written testimony submitted to the House Ways and Means Committee, Subcommittee on Trade: Hearing on "Supporting Economic Growth and Job Creation through Customs Trade Modernization, Facilitation, and Enforcement," May 17, 2012, 2-3, http://waysandmeans.house.gov/UploadedFiles/Sekin_Testimony.pdf.

59. See, e.g., Rob Knigge, "Freight forwarding and logistics: What the high performers know," Accenture Outlook (January 2013), http://www.accenture.com/us-en/outlook/Pages/outlook-online-2013-freight-forwarding-and-logistics-what-high-performers-know.aspx.

60. Olson/Finlay interviews, 2012-2013.

61. Sekin testimony, 1.

62. See, e.g., PwC's PRTM Management Consulting and its portrayal and use of the concept at http://www.prtm.com/strategiccategory.aspx?id=4100&langtype=1033.

63. See, e.g., http://www.cbp.gov/linkhandler/cgov/trade/trade_transformation/tt_2012_accomp.ctt/tt_2012_accomp.pdf; http://www.cbp.gov/xp/cgov/trade/trade_transformation/industry_int/; and http://www.cbp.gov/linkhandler/cgov/trade/trade_transformation/external_trade_trans.ctt/external_trade_trans.pdf.

64. CBP, "Fact Sheet: Trade Intelligence," July 2012, http://www.cbp.gov/linkhandler/cgov/newsroom/fact_sheets/trade/ttfs/tradeintelligence.ctt/tradeintelligence.pdf.

65. Executive Office of the President, Office of Science and Technology Policy, *Fact Sheet: US Global Positioning System Policy* (Washington: The White House, March 29, 1996), http://clinton4.nara.gov/textonly/WH/EOP/OSTP/html/gps-factsheet.html.

66. Scott Pace et al., *The Global Positioning System: Assessing National Policies* (Santa Monica, Calif.: RAND, 1995), 103, http://www.rand.org/pubs/monograph_reports/MR614.html.

67. See, e.g., National Foreign Trade Council, *Promoting Cross-Border Data Flows: Priorities for the Business Community* (Washington: National Foreign Trade Council, 2011), http://www.nftc.org/default/Innovation/PromotingCrossBorderDataFlowsNFTC.pdf.

68. See, e.g., the DHS SECURE and FutureTECH programs as discussed in Thomas Cellucci, *Innovative Public-Private Partnerships: Pathway to Effectively Solving Problems* (Washington: US Department of Homeland Security, 2010), http://www.dhs.gov/xlibrary/assets/st_innovative_public_private_partnerships_0710_version_2.pdf. See also the National Digital Engineering and Manufacturing Consortium (NDEMC) at http://ndemc.org.

69. See, e.g., Linton Wells II and Samuel Bendett, "Public-Private Cooperation in the Department of Defense: A Framework for Analysis and Recommendations for Action," *Defense Horizons* no. 74 (National Defense University, October 2012), http://www.ndu.edu/CTNSP/docUploaded/Defense%20Horizons%2074.pdf; see also William Tobey, "Defining and Implementing Best Practices in Nuclear Security," Discussion Paper #2012-13 (Cambridge, Mass.: Belfer Center for Science and International Affairs, December 2012), http://belfercenter.ksg.harvard.edu/files/William_Tobey_Defining%20and%20Implementing.pdf.

70. Executive Office of the President, National Security Staff, Community Partnerships Interagency Policy Committee, "Building Partnerships: A Best Practices Guide" (Washington: The White House, April 2013).

71. The work to revise the NIPP and evaluate the CIPAC model was mandated by Presidential Policy Directive-21.

See Executive Office of the President, *Presidential Policy Directive – Critical Infrastructure Security and Resilience* (Washington: The White House, 2013), http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

72. Oerlikon Leybold Vacuum, "Export Control Directive," Feb. 24, 2009, http://isis-online.org/uploads/conferences/documents/Export_Control_Directive_2009.pdf.