STIMSON

MARCH 2016

ADDING MARKET VALUE TO THE NONPROLIFERATION AGENDA

Nate Olson

CONTENTS

EXECUTIVE SUMMARY

Economic globalization has spawned new forms of illicit trafficking threats. The scale and technological sophistication of global value chains, along with their reach across multiple legal jurisdictions, often enable illicit activity to hide in plain sight. In short, decentralized criminal and terrorist networks are moving at the speed of 21st-century commerce.

In the coming years, as investors and export-minded players in industry and governments ramp up overtures to the next wave of emerging markets, these challenges will multiply – and traditional countermeasures will only be further outpaced. It will be crucial to strengthen cross-border governance mechanisms and find more effective ways to harness the private sector's expertise, resources, and reach. The main imperative in that process will be serving the public interest without undermining economic competitiveness.

This report highlights near-term opportunities to advance a shared public-private agenda by leveraging trade network transparency in both the domestic and international contexts. Trade network transparency entails two dimensions of global commerce: business relationships and chain of custody. Historically, most security programs have focused on ensuring a proper chain of custody – that is, the physical protection and integrity of a good at various stages of its life cycle, such as during transport on a container vessel.

In many areas of global trade and investment activity, however, regulators, experts, and advocates are also focusing on business relationships – and the diligence that companies perform to support those relationships. Increasingly, firms are being encouraged – or forced – to assume some measure of accountability for the actions of their business partners. This trend is evident in a number of initiatives that cover the full regulatory spectrum, from "soft law" to traditional, formal legal instruments. In this regard, the international security agenda and efforts to promote various social, political, and environmental goals are increasingly aligned.

The key to unlocking the multifaceted benefits of trade network transparency on both these fronts is "risk segmentation," a concept that is equally simple and underexploited. By distinguishing transactions that involve high-performing business entities from the rest of the pack, governments and public interest advocates can better target oversight and enforcement. By the same token, companies can actually enhance competitiveness.

For government, the ideas elaborated here represent a natural starting point in building a broader portfolio of tools for managing contemporary proliferation challenges. It is vital that industry remain engaged to ensure that the actual implementation of more innovative governance tools remains consistent with profitability in global business operations. That, in turn, will help make implementation – and the nonproliferation dividend – sustainable.

THE NEED TO MODERNIZE THE NONPROLIFERATION TOOLKIT

How the Rise of Global Value Chains Has Reshaped the Threat Environment

Economic globalization has spawned new forms of illicit trafficking threats. The scale and technological sophistication of global value chains, along with their reach across multiple legal jurisdictions, often enable illicit activity to hide in plain sight. At any given time, the illicit aim could be to move drugs or other contraband, counterfeit products, or, most sobering, technologies and equipment intended to support a nuclear weapons capability. Decentralized criminal and terrorist networks are moving at the speed of 21st-century commerce and are able to exploit its vulnerabilities.

Traditional law and regulation will remain the pillars of public security, to be sure. But for cross-border challenges generally and proliferation threats in particular, limitations on governments' jurisdiction and resources are untenable gaps. Enlisting private sector support is an urgent strategic priority. The central challenge for these efforts is finding ways to leverage the private sector's capabilities and expertise to serve the public interest *without* undermining economic competitiveness. Mutual benefit is the key to sustainability.

In some cases, governments continue attempts to bring cross-border trade more within their reach through the usual countermeasures of customs enforcement, intelligence gathering, and industry mandates. Yet even with a laudable policy objective, use of the traditional tools alone typically does not suffice.

ENLISTING PRIVATE SECTOR SUPPORT IS AN URGENT STRATEGIC PRIORITY.

For example, an increasingly global technology marketplace has prompted many countries to make exports a more prominent focus of their nonproliferation strategies. Supported by the wider nonproliferation community, they have sought to sharpen their export-control regimes in recent years. But such steps are seeing diminishing returns for the same reason: an ever-widening access to proliferation-sensitive technologies. A Department of Justice compilation of select export violations highlights many examples, which often entail false declarations of end-users and other commodity or shipping manifest data.[1] Such violations are particularly disconcerting as a number of countries continue to enhance their nuclear weapons capabilities.

All this underscores the need for complementary efforts by a wider set of nonproliferation partners – including those for whom nonproliferation is not a primary concern.

Industry-led approaches may be most advantageous for managing access to items that are sensitive but whose underlying technologies are nonetheless widely available. For example, the Traceability Committee overseen by SEMI, a trade association of electronics companies, establishes standards for the traceability of semiconductor manufacturing equipment. Among other things, the committee has a set of common definitions for manufacturing items and for encoding and decoding semiconductor manufacturing materials and resources.[2] These standards are intended to protect against the potential for counterfeiting or the possible diversion of technical equipment during shipment.

Key Industry Comparative Advantages

Identifying industry's comparative advantages vis-à-vis government is fundamental to understanding its potential roles in a multilayered security architecture. Here we note two illustrative areas that are crucial: resourcing and information-sharing capabilities.

Resourcing

Like much of the public agenda, nonproliferation is at serious risk because of greater constraints on public budgets in the modern era. But resourcing challenges are particularly acute with respect to trade-based risks, since multiple agencies and jurisdictions are usually involved. In other words, siloed agency portfolios and limited cooperation among jurisdictions often underdeliver the public services needed to support cross-border trade.

One development spurred by these resourcing gaps is the recent rise of reimbursable service agreements. These are a type of funding vehicle now used in the United States to support enhanced trade facilitation services at domestic ports of entry. Private sector entities (which can include municipal corporations like entire cities) provide funding in exchange for specific identified benefits, such as additional officers from US Customs and Border Protection (CBP) and infrastructure upgrades.

A 2013 law authorized CBP to enter into five such agreements with state, local, and/or private parties. Each partnership could last for up to five years, and the respective public or private sector organizations were to reimburse CBP for any new or expanded services.[3] In December 2013, CBP finalized agreements for partnerships with five entities intended to cover air, land, and sea operations (the Dallas/Fort Worth International Airport; the City of El Paso, Texas; the South Texas Assets Consortium; the City of Houston Airport System; and Miami-Dade County).[4] CBP has noted that these partnerships make up part of a larger long-term funding strategy to support additional requirements for security and efficiency, and continued growth in expected trade and travel volumes.[5]

While these agreements have enabled additional funding streams, they may prove difficult to adapt for other scenarios. As noted, CBP had to receive legislative approval before finalizing these agreements, and the procedural hurdles may deter other government agencies from committing to similar endeavors. In the private sector, there is also concern that these vehicles could set a bad precedent. Companies and trade associations fear that they could contribute to a trend of unfunded mandates whose costs ultimately must be borne by industry.

SILOED AGENCY PORTFOLIOS AND LIMITED COOPERATION AMONG JURISDICTIONS OFTEN UNDERDELIVER THE PUBLIC SERVICES NEEDED TO SUPPORT CROSS-BORDER TRADE

Information Sharing

Logistics providers hold a clear comparative advantage over government counterparts in collecting, disseminating, and interpreting the data at their disposal. Innovations in "track and trace" technologies, such as radio-frequency identification tags and next-generation GPS systems, are allowing much greater visibility into

how goods and information move through supply chains. Enhanced tools for analytics and risk management also show promise. Even for operations that are strictly in the open-source domain, these capabilities can make further inroads against illicit trafficking in the coming years. Logistics service providers, in particular, could see even greater returns as they identify new opportunities to dovetail data with adjacent industry spaces like port and warehouse operations, analytics and ratings services, and even insurance.

Public-Private Initiatives to Date

Government recognizes the benefit of engagement with industry, but has not taken full advantage of this opportunity. The US government has pursued broad engagement with the private sector, but has only made strides in certain areas of national security.[6] Thus, despite the potential for the private sector to fill gaps left by traditional trade controls, public-private initiatives have exhibited several limitations to date. Shortfalls in past public-private partnerships can be seen in stakeholder-engagement efforts, information-sharing initiatives, and the use of incentives.

Stakeholder Engagement

Stakeholder engagement often suffers from inhibited communication and cooperation. Even in fields of heightened engagement, such as disaster response and critical infrastructure, government efforts have fallen short. For instance, critical infrastructure outreach has taken place primarily through larger Fortune 500 companies and major trade associations. As a result, potential information from smaller companies and distributors, who constitute a greater proportion of economic activity, is not accounted for. Furthermore, stakeholder engagement has not yet moved beyond the 16 critical infrastructure sectors, once again excluding small businesses as well as third-party logistics providers.[7]

The national planning frameworks represent a stakeholder-engagement initiative that is narrow in scope. The planning frameworks specify a variety of ways in which industry can play a role in strengthening national security, in terms of preparedness, response, prevention, and mitigation.[8] These recommendations, however, do not address wider national security concerns and do not provide guidance for prioritizing these responsibilities.[9] This shortcoming may be traced to the Department of Homeland Security's Strategic National Risk Assessment (the foundation for the frameworks), as it prioritizes high-risk events and explicitly ignores continuous threats.[10]

Information Sharing

Information sharing is often advocated as a key tool in strengthening public-private partnerships. Government directives on information sharing include the National Strategy on Information Sharing and Safeguarding, establishment of the Program Manager for the Information Sharing Environment, and the Suspicious Activity Reporting Initiative.[11]

Other agency-specific programs consist of the CBP Private Sector Intelligence Liaison Office, the Office of the Director of National Intelligence's Trade Association Partners Group, the FBI's InfraGard, and the FBI Domestic Security Alliance Council. However, information-sharing programs are often constrained by coordination barriers, which complicate the benefits and implementation of the partnership. For instance, industry often perceives a unidirectional flow of information in that current information-sharing schemes require industry to provide information quickly to government agencies, without receiving the same actionable intelligence.[12]

Information-sharing partnerships have also been hindered by institutional barriers. With numerous agencies involved in data-sharing programs, coordination between the public and private sector becomes more time-consuming. Up to 48 agencies require similar data to be submitted by importers or exporters, creating duplicative requirements and conflicting agency records, and hampering international cooperation as well.[13]

This byzantine arrangement has prompted industry concern regarding the burden of data requirements.[14] The government's desire to collect a large amount of data has led the private sector to call for more targeted data collection, as well as greater specificity as to what data is sought. Government efforts to facilitate data-sharing when importing or exporting goods have remained largely ineffective. Following the 1993 Customs Modernization Act, CBP hoped the Automated Commercial Environment (ACE) would increase automation when reporting to the government. However, the ACE remains incomplete.[15]

Competitive dynamics are sometimes another limitation on information-sharing partnerships between the public and private sectors. Industry is often hesitant to share sensitive information for fear of eventual disclosure, whether unintended or malicious.[16] Such disclosures can bring substantial risk that industry competitors will acquire intellectual property or proprietary technology. This concern can run together with an unclear understanding of the processes and technical tools used by government when handling sensitive material – as well as fears that sharing such information could prompt regulators to single out cooperators for greater scrutiny.[17]

There are few (if any) genuinely anonymous means to share information with government. Government has begun to address this worry by explaining how it uses data in the "protected critical infrastructure information" model, but this has not been expanded into other programs.[18] A Transportation Board Research assessment noted several approaches to overcome the competition barriers to information sharing.[19] For instance, nondisclosure agreements, compensation for data-sharing projects, and restrictions on data use are tools to motivate industry participation in information-sharing partnerships.[20]

The Use of Incentives

Another shortcoming in recent public-private partnerships has been a lack of sufficient incentives for the sustained participation of industry. Although government often trumpets the advantages of participation in its initiatives, the private sector often contends that the promised benefits have not materialized. Industry's low return on investment in such cases can also undermine prospects of future public-private efforts.[21]

This dynamic is frequently discussed in the context of CBP's Customs-Trade Partnership Against Terrorism (C-TPAT). The C-TPAT was designed to deliver certain trade benefits, such as fewer cargo inspections, for US importers that volunteered to meet specific security standards across the supply chain.[22] Despite CBP's repeated emphasis on the program's trade facilitation benefits, some industry segments claim to have seen a modest or negligible impact. In addition, while C-TPAT membership now exceeds 10,000 firms, not all relevant industry actors are eligible.[23]

Proliferation risks increase when governments fail to effectively target incentives for more rigorous due diligence. Policymakers and enforcement bodies cannot take advantage of opportunities to streamline and strengthen measures aimed at prevention. Companies likewise are not able to realize improved visibility into cargo movements. More generally, the credibility of such programs suffers, which can undermine the success of future initiatives even if they are better designed.

A major reason why governments are often unable to marshal sufficient benefits for programs like C-TPAT is that the relevant decision-makers are spread across many disparate agencies. As an example, the table below highlights a number of US government agencies with export-related authorities. These are only the seven most prominent and high-level agencies; many other relevant authorities are located among other, more obscure agencies.

Oversight of US Exports: Relevant Agencies and Regulations

	AGENCY	REGULATION	PURPOSE
	Department of State: Directorate of Defense Trade Controls	International Traffic in Arms Regulations (ITAR) 22 CFR Parts 120-130	Regulates the export of defense articles, services, and technical data controlled under the United States Munitions List
	Department of Commerce: Bureau for Industry and Security	Export Administration Regulations 15 CFR Parts 700-799	Regulates the export of sensitive goods and technologies – including but not limited to so-called "dual use" items – controlled under the Commerce Control List
	Department of Energy: National Nuclear Security Administration	10 CFR Part 810	Regulates activities of US people engaged directly or indirectly in the production of special nuclear material outside the United States.
	Nuclear Regulatory Commission	10 CFR Part 110	Regulates the import and export of nuclear material in and out of the United States
	Department of the Treasury: Office of Foreign Assets Control	Foreign Assets Control Regulations 31 CFR 500-599	Defines foreign and economic embargoes and sanctions that reflect United States foreign policy and national security interests
	Department of Commerce: Census Bureau	Foreign Trade Regulations 15 CFR Part 30	Requires exporters to accurately file transaction and shipment information through the Automated Export System
	Department of Homeland Security: Customs and Border Protection	Customs Regulations 19 CFR Parts 1-199	Defines the authorities and the regulations related to the transit of goods into and out of the United States

HOW TRADE NETWORK TRANSPARENCY CAN SUPPORT NONPROLIFERATION

Risk Segmentation: A Simple But Underexploited Principle

"Risk segmentation" is the key that can unlock the value of trade network transparency for nonproliferation. The concept is straightforward: By distinguishing transactions that involve high-performing exporters and relatively reliable end-users from the rest of the pack, governments can better target oversight and enforcement. With sufficient benefits for participation, companies will voluntarily opt to seek whatever validation is required. The benefits also promote a virtuous cycle of sorts, incentivizing firms whose internal due diligence processes are not adequate to enhance their compliance efforts.

Calls to leverage a risk-segmentation approach for the benefit of both security and private industry go back decades. The US Department of Commerce, for instance, proposed a "gold card" for high-performing exporters in 1986.[24] Nevertheless, while governmental officials increasingly speak the language of risk management, risk segmentation in particular remains an underexploited method.

A Two-Sided Coin: Business Relationships and Chain of Custody

Broadly speaking, trade network transparency entails two dimensions of global commerce: business relationships and chain of custody. Historically, most security programs have focused on ensuring the proper chain of custody – the physical protection and integrity of a good at various stages of its life cycle, such as during transport on a container vessel.

In many areas of global trade and investment activity, regulators, experts, and advocates are also focusing on business relationships – and the diligence companies perform to support those relationships. Increasingly, companies are being encouraged – or forced – to assume accountability for the actions of their business partners. This trend is evident in a number of initiatives that cover the full legal spectrum, from "soft law" to traditional, formal legal instruments.

More formal approaches sometimes serve as reminders of just how formidable the challenges of global trade are for traditional, state-based tools. One example of the latter is disclosure requirements, recently introduced by the Securities and Exchange Commission, for companies whose products incorporate minerals from conflict-affected areas. Some observers argue that the requirements impose unrealistic diligence standards on firms far downstream in supply chains for electronics. Rather than risk legal entanglements, some of those firms might choose to sever trade relationships with all suppliers in the affected regions. The fallout hopefully would see a reduction in illicit commodity flows, but it certainly would threaten the competitiveness of even those suppliers who are strictly in compliance with the regulations. This is a perverse effect of a phenomenon sometimes referred to as "derisking."

Another example – arguably more successful, though on a more limited scale – is the validated end-user regime used by the Department of Commerce. Established by the department's Bureau of Industry and Security in 2007, Authorization Validated End-User (VEU) seeks to minimize the burden placed on industry in applying for export licenses while upholding the priority on end-user evaluation. Through the VEU program, exporters may ship certain designated items to authorized entities in eligible destinations. Currently, China and India are the only countries with eligible destinations for the export, re-export, or transfer of items to validated end-users.

LEVERAGE POINTS IN THE DOMESTIC ENVIRONMENT

International trade, of course, always involves two or more countries. More streamlined systems and more robust industry-government cooperation at the national level are crucial to enable similar advances at the global level.

Initiatives of Key Government-Sponsored Industry Advisory Committees

Government-sponsored industry advisory committees represent an opportunity for the private sector to maximize national security within the supply chain.[25] The departments of Homeland Security, Commerce, State, and Treasury are just some of those that regularly solicit industry input in this manner. Among other topics, industry advisory committees offer views on critical infrastructure security, customs facilitation, supply chain competitiveness, and export controls.

A key government-sponsored industry advisory committee to the Department of Homeland Security is the Critical Infrastructure Partnership Advisory Council (CIPAC), which serves as a forum for discussion between the Department of Homeland Security and critical infrastructure owners across a variety of sectors. These different sectors are represented by the CIPAC's 17 working groups, including the financial, transportation, and manufacturing sectors. The CIPAC more generally supports the National Infrastructure Protection Plan (NIPP) 2013, "Partnering for Critical Infrastructure Security and Resilience." The NIPP provides a framework for collaboration between the private sector and government to manage risk and strengthen critical infrastructure.[26]

The development of the NIPP was a response to Presidential Policy Directive 21 – Critical Infrastructure Security and Resilience, which specifically called for a risk-management framework. Through the numerous working groups and the NIPP, the CIPAC allows for government and industry to collaboratively strengthen critical infrastructure through identifying risks, addressing vulnerabilities within systems, and minimizing damage in the event of an emergency.[27]

The Advisory Committee on Commercial Operations to US Customs and Border Protection (known as COAC) represents another important advisory body to the Department of Homeland Security. The COAC more specifically provides guidance to CBP on a variety of issues including global supply chain security, export enforcement and facilitation, trusted-trader programs, and trade modernization. Most industry members of the COAC come from transport and logistics firms. Professionals in this space are peerless in their understanding of the complexity of the global economic and regulatory environment. Similarly, they are among those best positioned to fast-track a more modern approach to public-private security cooperation that boosts economic competitiveness while advancing the public interest.

Although six distinct subcommittees comprise the COAC, the committee has more broadly called for ongoing efforts by the US Single Windows initiative and the assessment of developing programs, including the Trusted Trader Pilot and the export entity of C-TPAT.[28] Regarding the trusted-trader program, the COAC has stressed that CBP complete its selection process of its trusted-trader program and provide updates on the various participants. In addition, the COAC has recommended that CBP

strengthen the program through trade compliance and enforcement.[29] Regarding the export C-TPAT program, the COAC has recommended that CBP specify program requirements and benefits, and engage with the trade community to receive feedback on the program.[30] By working to strengthen the US Single Window initiative, the trusted-trader program, and C-TPAT, the COAC aims to facilitate trade by improving customs matters.

Another important advisory committee for the Department of Commerce is the Advisory Committee on Supply Chain Competitiveness, which provides recommendations on elements in local, state, and national policies that influence national economic competitiveness.[31] The committee also has evaluated the impact of multilateral policies on supply chain competitiveness. Most recently, it has evaluated the World Trade Organization Trade Facilitation Agreement, the Transatlantic Trade & Investment Partnership, the Trans-Pacific Partnership, and the Trade in Services agreements.[32] The committee supports these initiatives as they continue to simplify and harmonize trade regulations.

The Advisory Committee on Supply Chain Competitiveness has also supported trade transformation programs managed by CBP.[33] The committee has particularly approved of the trusted-trader initiatives for exports, including the nascent C-TPAT for Export initiative. However, the committee has strongly opposed the adoption of the US Census Bureau's Advanced Export Information (AEI) pilot program. This program would eliminate certain companies' eligibility for post-departure shipment filings, or "Option 4." The committee finds that such a step would result in economic costs for exporters, and would undermine account-based initiatives for importers and exporters.[34]

A final important advisory committee serving the Department of Commerce is the President's Export Council Subcommittee on Export Administration (PECSEA). The PECSEA more specifically provides recommendations to the Bureau of Industry to minimize the impact of US export controls.[35] The PECSEA devoted substantial time and attention to the Obama Administration's Export Control Reform initiative, which has harmonized a number of regulations in the International Traffic in Arms Regulations and the Export Administration Regulations.[36] This initiative would simultaneously reduce the impact of export controls and promote compliance.

The PECSEA is also pursuing several priority reform and implementation priorities in collaboration with the Trade Security Steering Group, a group of trade specialists organized by the Stimson Center and the National Association of Manufacturers. One of these priorities is streamlining US regulation of intracompany technology transfers, particularly for "deemed exports" that transfer technology to non-US entities.

US-style deemed export controls are found only in a small handful of national export control systems worldwide. US parties engaged in the research, manufacturing, or export of controlled technologies must obtain an export license before releasing controlled technology to a foreign person in the United States because that release is "deemed" to be an export to that person's country of nationality. The practical effects of this process go much further than incurring administrative costs in obtaining export licenses. In some cases, private sector and academic organizations spend significant time and money to separate controlled information from employees who are not US citizens. In other cases, they elect not to hire exceptionally qualified foreign individuals. And in still other cases, they simply choose to locate various stages of value chain activity abroad.

Previous attempts to reform US-deemed export regulations include a 2008 proposed rule from the US Department of Commerce Bureau of Industry and Security (BIS), which would have created a new license exception to intracompany transfer. Public comments submitted to the BIS included an extensive set of recommended changes to the proposal, which was never finalized. Nevertheless, real opportunity exists for targeted reforms, guided by lessons from these previous efforts and by the determined work of research and practitioner groups such as the Coalition for Excellence in Export Compliance.

The Trade Security Steering Group is exploring the potential for a more streamlined license exception/exemption process – one that better leverages the market imperative for US entities to safeguard their intellectual property from unauthorized parties. US parties that have adopted certain screening and technology control programs would more easily be able to release technology controlled under the Export Administration Regulations to non-US citizens in the United States. This straightforward reform – achievable by the current administration – would serve the interests of regulators, large and small companies, and research institutions and universities.

Several other stakeholder groups, including other advisory committees, are devoting significant attention to deemed export issues. Along with the Trade Security Steering Group, they all have helped regulators identify options for implementation of the proposed exception/exemption that would reinforce other US government moves to streamline the regulation of exports, such as creation of the C-TPAT for Exports program.

In mid-2015, the Trade Security Steering Group conducted a major survey of companies and universities on deemed export issues. The survey results continue to inform the group's engagement with regulators and industry partners alike.

The "Single Window" Initiative and the Border Interagency Executive Council

The varied technology platforms, data requirements, and administrative processes seen across government agency systems have caused major inefficiencies for both government and industry. Some agencies regulating maritime commerce still require thick stacks of paper filings for each individual shipment. The International Trade Data System (ITDS) is a so-called "single window" through which US exporters and importers will be able to submit required documentation to government regulators.

A February 2014 executive order sets a deadline for full ITDS deployment.[37] It also codifies and elevates the role of the Border Interagency Executive Council (BIEC), expanding its purview to include a number of important responsibilities related to both imports and exports.

Beyond these headline provisions, two other aspects of the directive offer major leverage points for trade-security dual benefits. The first is a clearly articulated priority of more efficient and effective enforcement as a key part of – and not an impediment to – streamlined trade facilitation efforts. The second, related to but distinct from the first, is a requirement for the newly codified BIEC to "engage with and consider the advice of industry and other relevant stakeholders regarding opportunities to improve supply chain management processes, with the goal of promoting economic competitiveness through enhanced trade facilitation and enforcement." This broad mandate presents a major opportunity for modernized international trade policies and processes. Among other things, the BIEC could become a vehicle for more integrated, cross-agency trade facilitation regimes.

The nonproliferation benefit from these developments is at least twofold. First, the greater efficiency and uniformity of agency data processing will improve security oversight by surfacing anomalous transactions more quickly. Indeed, the Department of Homeland Security has stated publicly that the ITDS will enhance export enforcement – a claim that senior US government trade enforcement officials have confirmed to the Stimson Center in separate conversations. Second, the BIEC's ability to bring a larger number of relevant government agencies to the table makes it uniquely positioned to consolidate a fuller menu of incentives for industry. It thus may succeed where prior efforts, such as C-TPAT for Exports, have faltered.

LEVERAGE POINTS IN THE INTERNATIONAL ENVIRONMENT

Regulatory Cooperation Efforts

At the bilateral, regional, and global levels, regulatory cooperation measures can offer a natural jumping-off point for stakeholders to create new trade facilitation frameworks or enhance existing ones. Efforts by peer regulatory agencies to learn about their counterparts' regimes – and subsequently, to harmonize their respective regimes – are important force multipliers. In North America, for instance, longstanding US-Canada and US-Mexico bilateral initiatives, as well as a maturing suite of trilateral projects, continue to integrate the continent's economies and harmonize regulatory frameworks. But regulatory cooperation comes in many other forms, too.

Mutual Recognition Arrangements

Mutual Recognition Arrangements (MRAs) are bilateral agreements that harmonize specific trade regulations. Though they can differ substantially in their particulars, MRAs are broadly based on the World Customs Organization's Framework of Standards to Secure and Facilitate Global Trade (the SAFE Framework). The standards set out in the SAFE Framework are intended to prevent international terrorism while facilitating legitimate international trade.[38] The framework has helped customs administrations harmonize the security standards used in national trade facilitation programs – referred to as Authorized Economic Operator (AEO) programs under the SAFE Framework.[39] MRAs are negotiated and signed by customs administrations to spell out these security requirements. MRAs also stipulate the conditions that apply to AEO authorizations and their subsequent benefits, and the ways in which mutual recognition can be sustained.[40]

The harmonization of AEO authorizations provides benefits for both customs administrations as well as industry actors.[41] MRAs allow for enhanced compliance with security requirements and greater protection of the global supply chain.[42] At the same time, they enable customs officials to facilitate the movement of goods between vetted companies while focusing scrutiny on higher-risk shipments.[43] MRAs also provide advantages for industry in partnering countries, such as bypassing technical barriers related to regulatory compliance. Absent such streamlining measures, companies often incur considerable costs in complying with a given trading partner's particular regulations and technical parameters.[44] For instance, product testing and certification often must be duplicated for the different customs administrations with oversight of a particular transaction.[45] These costs directly influence trade and investment flows. MRAs address this challenge by providing a level of consistency across customs administrations, including testing and certification measures. Consequently, industry may export goods more efficiently.

In the US context, MRAs represent an agreement between the CBP Office of International Affairs and a foreign customs administration whose trade facilitation program uses security criteria that are compatible with the US Customs-Trade Partnership Against Terrorism (C-TPAT).[46] CBP has thus far signed 10 MRAs.[47] Most recently, CBP has signed a joint work plan with the Dominican Republic, which represents a step toward a formalized MRA. CBP has noted that the joint work plan may at the earliest translate into an MRA by 2016.[48]

Multilateral Export Control Regimes

Expanding trade volumes in recent decades prompted efforts to mitigate a commensurate rise in illicit commerce, particularly in dangerous materials and sophisticated technologies. These efforts are principally embodied in four major multilateral export control regimes. At various times, activities in these institutions have been driven by individual countries, groups of countries, the United Nations, or civil society actors. All four of the regimes are voluntary and subject to national laws and regulations.

	Year Established	Number of Current Members	Items Covered	Notable Non-Member Countries
The Nuclear Suppliers Group	1974	46	Nuclear Weapons	India, Iran, Israel, North Korea, Pakistan, Syria
The Australia Group	1985	42	Biological and Chemical Weapons	China, India, Iran, Israel, North Korea, Pakistan, Russia, Syria, South Africa
Wassenaar Agreement	1995	41	Conventional Arms and Dual-Use Items	China, India, Iran, Israel, North Korea, Pakistan, Syria
Missile Technology Control Regime	1987	34	Missiles	China, India, Iran, Israel, North Korea, Pakistan, Syria

Free Trade Agreements

Historically, free trade agreements have focused overwhelmingly on specifying tariff levels on a long catalogue of esoteric products. After decades of liberalization, however, tariff-related market access issues have begun to recede into the background. Trade agreements today are genuinely multipurpose vehicles. The most notable examples in the contemporary context are the US-EU Transatlantic Trade and Investment Partnership and the Trans-Pacific Partnership, which emerged from negotiations among the US and 11 Asian-Pacific nations. These instruments address a vast range of subjects, many of them quite specialized, and many of them far removed from what traditionally would have been considered trade-related.

Such is the case for security issues. As US Trade Representative Michael Froman has said, "Trade has emerged as one of America's most important foreign policy tools – both for increasing our strength at home and for exercising it abroad… By leading on these issues, the United States can launch a race to the top, rather than be subject to a race to the bottom that we cannot win and should not run."[49]

The WTO Trade Facilitation Agreement

As the connective tissue among disparate legal jurisdictions, business models, and geographic locales, providers of transport and logistics services are vital to modernizing public-private engagements. So too are national customs administrations that oversee export/import operations across all modes of conveyance. It is no surprise therefore that trade-capacity building is an area of increasing interest among practitioners of both economic development and international security.

In the near term, implementation of the World Trade Organization (WTO) Trade Facilitation Agreement presents a substantial opportunity to promote mutual gains in security and development along several tracks. The agreement mandates that countries set up Authorized Economic Operator programs that give concrete benefits to exporters/importers whose internal management processes meet certain criteria. The competitive advantage created for participating firms is multiplied when countries align various aspects of their trade regulations. Other parts of the WTO agreement advance international harmonization of key trade-related policies and programs. For instance, the pact would set a reasonable global baseline for streamlining government-industry and government-government exchanges of trade data, including protections for sensitive information.

The private sector and emerging-market governments, in particular, see great potential in implementing the accord. In December 2015, a group of government and industry bodies announced a Global Alliance for Trade Facilitation. The public-private entity will help secure and deliver various forms of support to WTO member countries that request assistance with implementation.[50,51]

These trade capacity building measures will not only increase economic returns. They also will advance nonproliferation goals. More efficient processes will enhance trade transparency, which in turn will strengthen government responses to a wide range of violations, from diversions of high-tech equipment to intellectual property theft.

The "Responsible Business Conduct" Agenda

Trade transparency is a widely shared, and highly valued, objective. Global value chains can pose risk-management and compliance challenges even for sophisticated companies operating in the most advanced industrialized states. In the high-tech space, for instance, companies are increasingly plagued by "gray area" transactions that are legal in the strict sense but raise suspicions regarding ultimate end-use. Whether the concern is development of weapons of mass destruction (WMD), extralegal surveillance, human rights abuses, or some other malevolent end enabled by a high-tech product, industry stakeholders are actively seeking to develop suitable internal measures for due diligence and to manage the diverse range of associated risks. Similar difficulties facing smaller manufacturers, particularly those in developing countries, can be especially daunting.

"TRADE HAS EMERGED AS ONE OF AMERICA'S MOST IMPORTANT FOREIGN POLICY TOOLS – BOTH FOR INCREASING OUR STRENGTH AT HOME AND FOR EXERCISING IT ABROAD."

— Ambassador Michael Froman
US Trade Representative
February 2015

At the same time, of course, the global regulatory environment is becoming more complex, not least because of the upward trend in value chain accountability noted earlier. Companies are facing rising expectations to assume responsibilities across their value chains – including for their business relationships, not just their own direct actions.

While they usually are discussed in completely separate fora and without any reference to one another, the international security agenda and efforts to promote various social, political, and environmental goals are becoming increasingly aligned in the push toward trade transparency.

The initiatives in these latter issue areas are often referred to collectively as the "responsible business conduct" agenda, though the term as yet has no formal scope or commonly understood definition. The main driver of sustained and coordinated action in this sphere has been the United Nations (UN) Principles on Business and Human Rights, finalized in 2011 after a six-year process led by Professor John Ruggie. Many countries have since set out to develop national action plans to adapt the UN principles to their respective legal and regulatory systems. A related UN working group led by Professor Ruggie continues to be active in promoting the principles and informing national and international debates on how to operationalize them.

In September 2014, the Obama administration announced that it, too, would develop a national action plan. In addition to incorporating the UN principles, the US is crafting its document so as to align fully with the Organization for Economic Cooperation and Development's (OECD) Guidelines on Multinational Enterprises.[52] The OECD is an increasingly vocal and influential player in framing the responsible business conduct agenda and, through the guidelines, connecting it to the practical realities of modern business processes and risk-management frameworks.

Connecting the Agenda to Business Practice – and Nonproliferation Benefits

The "responsible business conduct" agenda presents stakeholders across diverse domains – including the nonproliferation community – with an important opportunity to leverage their respective efforts. To take just one specific example, an opportunity for mutually advantageous cooperation can be seen in a chemical industry effort: the Responsible Distribution program.

Responsible Distribution was originally designed by the National Association of Chemical Distributors (NACD) in 1991. It requires independent, third-party verification of NACD members' facilities and practices, focused on environmental impact, health, safety, and security. The program is meant to encompass each phase of chemical distribution, including storage, handling, transportation, and disposal.

The NACD edited the product stewardship section of its Responsible Distribution Code of Management Practice to incorporate end-user verification and evaluation in 2002. The NACD requires members to develop customer vetting processes similar to the Drug Enforcement Administration's "Know Your Customer" policy. Members must take reasonable measures to identify customers and establish legitimacy prior to making a sale. The guidelines also call on distributors to learn how to identify anomalous transactions, and to report suspicious activity to the FBI or other law enforcement agency.

The common cause with the nonproliferation agenda here is strong. A customer vetting process modeled on 21st-century best practices is among the most important tools that companies of all sizes and sectors can employ to prevent security violations, such as diversion, in today's complex risk environment. By supporting the abilities of exporters to recognize and avoid suspect transactions, initiatives like Responsible Distribution are the kind of decentralized countermeasure that deserve higher priority among the nonproliferation community.

NEXT STEPS: PRIORITY BEST PRACTICES

The public and private sectors alike recognize the imperative of greater collaboration. The challenge is crossing the threshold where collaboration yields net gains for each constituency. As they seek to move beyond that threshold, three best practices that should guide government and industry are stakeholder engagement, information sharing, and targeted incentives. The table below shows in stylized form the degree of nonproliferation support each best practice stands to offer in several key issue areas.

For government to more effectively identify risks to national security, the institutionalization of appropriate incentives for the private sector will remain crucial. Moreover, governments must take a fuller view of their industry partners' strategic environment, operational processes, and value-creation opportunities. That in turn requires engaging companies across corporate functions and affiliated communities of interest. Simply giving industry a seat at the proverbial table is not enough. All too often, the industry players that government has sought out have fallen into a narrow range of functional roles and subject matter expertise. The results have been too inflexible, leading to a mantra of "one size does not fit all" among industry observers.

Three Public-Private Best Practices

Potential Nonproliferation Value-Add in Select Issue Areas

	BEST PRACTICE		
SELECT ISSUE AREAS	Stakeholder engagement	Information sharing	Targeted incentives
Cybersecurity			
Critical infrastructure protection			
"Responsible business conduct"			

To mitigate the perverse effects of "derisking," officials also must improve coordination at the national and international levels on relevant regulatory and enforcement actions – and they must bring the private sector into the process. Streamlined communication and enhanced industry feedback would better enable them to tackle related challenges, such as limiting legal entanglements that firms could face and harmonizing regulatory and enforcement actions. While priorities might change over time, this coordination would remain crucial. In all likelihood, its benefits would extend to how many other enforcement regimes could function effectively.

Ideally, one or more existing institutions could lead these efforts. One candidate would be the Financial Action Task Force, whose 36-member governments and regional organizations develop standards to combat money laundering and terrorist financing. To its credit, the task force recognizes industry disengagement as a serious concern. But its private-sector outreach – essentially, occasional meetings with financial services firms – is not adequate. While finance companies are a key weapon of entrepreneurial policy architects, the disengagement issue demands more regular consultation with a more diverse set of international commercial players. In addition, the task force is not equipped to handle

the broader set of problems against which emerging enforcement strategies are being deployed today.

Finally, cybersecurity is an area that could have a number of beneficial "spinoff" effects for other agendas. For instance, governments could do more to leverage cybersecurity's inherently enterprise-wide relevance to advance public-private coordination on a larger scale. The issue's complexity, and its material consequences for the bottom line, has opened a window for unconventional cooperation. Corporate boards recognize the imperative of a modernized risk-management paradigm that blends existing business models with new technological variables.

CONCLUSION

Recent history is replete with examples of how the trade-security nexus can undermine both the public security interest and legitimate commerce. Massive volumes in trade and investment, moving rapidly across multiple jurisdictions with the aid of the latest technologies, have opened many seams for illicit networks to move various forms of contraband, including items that can support WMD capabilities. It is imperative that stakeholders, including the nonproliferation community, turn this dynamic on its head. Complementing sound regulations and direct government enforcement tools with industry-driven countermeasures is essential to keep pace with today's proliferation threats.

The ideas elaborated here demonstrate how to do just that, while ensuring that all stakeholders see a compelling value proposition for the longer term. For government, they represent a natural starting point in building a broader public-private portfolio of tools for managing contemporary security challenges. It is vital that industry remain engaged to ensure that the actual implementation of these more innovative governance tools remains consistent with profitability in global business operations. That, in turn, will help make implementation – and the nonproliferation dividend – sustainable.

In the coming years, as investors and export-minded players in industry and governments ramp up overtures to the next wave of emerging markets, the challenges brought by global value chains will multiply – and traditional countermeasures will only be further outpaced. It will be crucial to strengthen cross-border governance mechanisms and find more effective ways to harness the private sector's expertise, resources, and reach. A focus on trade network transparency will go far in ensuring that these multistakeholder approaches stand up to the daunting challenges of 21st-century proliferation threats.

Acknowledgements

Stimson is deeply 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 providing keystone support to the industry engagement efforts of the Center's Managing Across Boundaries Initiative. The author is also grateful to Stimson colleagues Matt Ellison, Ben Brown, and Li Ma for assisting with this report's research and editing, and to Lita Ledesma for its design and layout.

About Stimson

Founded in 1989, the Stimson Center is a nonprofit, nonpartisan think tank devoted to addressing transnational challenges in order to enhance global peace and economic prosperity.

The grand challenges faced by humanity yield both troublesome new complexities and unprecedented new opportunities. Terrorism, population shifts, conflict, trafficking, inadequate health, environmental degradation, resource scarcity, cyber-insecurity are only a partial list of threats that increasingly confound the traditional instruments of policy. Through rigorous research, analysis and outreach, the solutions Stimson offers operate at the intersection of security, development, and sound economic policy. Our approach is pragmatic – geared toward providing policy alternatives, solving problems, and overcoming obstacles to a more prosperous and secure world. By engaging policymakers, policy implementers, private industry and nongovernmental institutions, Stimson crafts recommendations that are non-partisan, actionable, and effective. The MacArthur Foundation recognized Stimson in 2013 with its "institutional genius" Award for Creative and Effective Institutions, and the organization consistently ranks among the world's top think tanks.

Endnotes

1. US Department of Justice (DOJ). "Summary of Major U.S. Export Enforcement, Economic Espionage, Trade Secret and Embargo-Related Criminal Cases." January 23, 2015. Accessed August 26, 2015. http://www.justice.gov/sites/default/files/nsd/pages/attachments/2015/01/23/export-case-list-201501.pdf.

2. SEMI. "Traceability Committee." Accessed June 25, 2015. http://www.semi.org/en/node/41831.

3. Consolidated and Further Continuing Appropriations Act of 2013. Public Law 113-6. Section 560. 113th Cong., 1st sess. March 26, 2013. Accessed January 27, 2016. https://www.gpo.gov/fdsys/pkg/PLAW-113publ6/pdf/PLAW-113publ6.pdf.

4. US Department of Homeland Security (DHS) and US Customs and Border Protection (CBP). "Reimbursable Fee Agreements: Fourth Semiannual Report." June 23, 2015. Accessed February 25, 2014. https://www.dhs.gov/sites/default/files/publications/OCFO/Customs%20and%20Border%20Protection%20(CBP)%20-%20%20Reimbursable%20Fee%20Agreements%20-%20Fourth%20Semiannual.pdf.

5. Wagner, John. "A New Approach to Increase Trade and Security: An Examination of CBP's Public Private Partnerships." Statement before U.S. Congress. House. 114th Cong., 2nd sess. November 4, 2015. Accessed January 27, 2016. http://docs.house.gov/meetings/HM/HM11/20151104/104132/HHRG-114-HM11-Wstate-WagnerJ-20151104.pdf.

6. Olson, Nate. "Making Public-Private Security Cooperation More Efficient, Effective and Sustainable." Staff Report. Washington, DC: Stimson Center, December 2014. 80. Accessed January 27, 2016. http://www.stimson.org/images/uploads/research-pdfs/PIP_Staff_Report_FINAL.pdf.

7. "Making Public-Private Security Cooperation More Efficient, Effective and Sustainable." Recommendations of the Partners in Prevention Task Force. Washington, DC: Stimson Center, May 19, 2014. 22. Accessed January 27, 2016. http://www.stimson.org/images/uploads/research-pdfs/Stimson_Partners_in_Prevention_Task_Force_Report_May_2014.pdf.

8. DHS. "National Planning Frameworks." March 19, 2015. Accessed January 27, 2016. http://www.fema.gov/national-planning-frameworks.

9. Olson, "Public-Private Security Cooperation" (Staff Report), 82.

10. DHS. "The Strategic National Risk Assessment in Support of PPD 8: A Comprehensive Risk-Based Approach toward a Secure and Resilient Nation." December 2011. Accessed January 27, 2016. http://www.dhs.gov/xlibrary/assets/rma-strategic-national-risk-assessment-ppd8.pdf.

11. Kshemendra, Paul. "White House Releases New National Strategy for Information Sharing and Safeguarding." Program Manager for the Information Sharing Environment. December 19, 2012. Accessed January 27, 2016. http://www.ise.gov/blog/kshemendra-paul/white-house-releases-new-national-strategy-information-sharing-and-safeguarding.

12. Olson, "Public-Private Security Cooperation" (Staff Report), 83..

13. Olson, Nate, and Finlay, Brian. "Market Power: Adapting Public and Private Roles for Transnational Commerce and Transnational Threats." Washington, DC: Stimson Center, September 2013. 25. Accessed January 27, 2016. http://www.stimson.org/images/uploads/research-pdfs/Market_Power_Sep2013.pdf.

14. Olson, "Public-Private Security Cooperation" (Staff Report), 79.

15. Olson and Finlay, "Market Power," 25.

16. Olson, "Public-Private Security Cooperation" (Staff Report), 141.

17. Ibid., 76.

18. Ibid.

19. "NCFRP Report 25: Freight Data Sharing Guidebook." Washington, DC: Transportation Research Board, February 2013. 8. Accessed January 27, 2016. http://onlinepubs.trb.org/onlinepubs/ncfrp/ncfrp_rpt_025.pdf.

20. Transportation Research Board, "Freight Data Sharing Guidebook."

21. Olson, "Public-Private Security Cooperation" (Staff Report), 142.

22. CBP. "C-TPAT: Customs-Trade Partnership against Terrorism." Accessed January 27, 2016. http://www.cbp.gov/border-security/ports-entry/cargo-security/c-tpat-customs-trade-partnership-against-terrorism.

23. CBP, "C-TPAT."

24. Smith, Gordon B. "The Politics of East-West Trade." In *Law and Politics of East-West Technology Transfer*, edited by Oda, Hiroshi, 53. Martinus Nijhoff/Graham & Trotman, 1991.

25. Olson, "Public-Private Security Cooperation" (Staff Report), 83.

26. DHS. "National Infrastructure Protection Plan." October 27, 2015. Accessed January 27, 2016. http://www.dhs.gov/national-infrastructure-protection-plan.

27. DHS. "NIPP 2013: Partnering for Critical Infrastructure Security and Resilience." Accessed January 27, 2016. http://www.dhs.gov/sites/default/files/publications/NIPP%202013_Partnering%20for%20Critical%20Infrastructure%20Security%20and%20Resilience_508_0.pdf.

28. CBP. "FY2013 - FY2015 COAC Recommendations." Accessed January 27, 2016. http://www.cbp.gov/sites/default/files/documents/COAC%20Recommendations%2013th%20Term.pdf.

29. CBP. "Advisory Committee on Commercial Operations to U.S. Customs and Border Protection (COAC): Statement of Work for the Subcommittee on Trusted Trader Programs." April 17, 2015. Accessed January 27, 2016. http://www.cbp.gov/sites/default/files/documents/06%20Trusted%20Trader%20Subcommittee%20Pre-Decisional%20Statement%20of%20Work.pdf.

30. CBP, "FY2013 - FY2015 COAC Recommendations."

31. US Department of Commerce (DOC). International Trade Administration. "Advisory Committee on Supply Chain Competitiveness." Accessed January 27, 2016. http://trade.gov/td/services/oscpb/supplychain/acscc/about.html.

32. DOC. Advisory Committee on Supply Chain Competitiveness (ACSCC). Letter to Secretary of Commerce Penny Pritzker. May 2015. Accessed January 29, 2016. http://trade.gov/td/services/oscpb/supplychain/acscc/documents/May%2021%202015%20Conf%20Call/ACSCC%20trade%20ltr%20to%20SPP%20TC%20Subcomm.pdf.

33. Ibid.

34. Ibid.

35. DOC. Bureau of Industry and Security. "Charter of the President's Export Council Subcommittee on Export Administration." October 21, 2011. Accessed January 27, 2016.

http://www.bis.doc.gov/index.php/licensing/28-technology-evaluation/151-presidents-export-council-subcommittee-on-export-administration.

36. DOC. "About Export Control Reform (ECR)." October 7, 2015. Accessed January 27, 2016. http://www.export.gov/ecr/.

37. Obama, Barack. "Executive Order 13659: Streamlining the Export/Import Process for America's Businesses." *Federal Register* 79, no. 37 (February 19, 2014). www.gpo.gov/fdsys/pkg/FR-2014-02-25/pdf/2014-04254.pdf.

38. World Customs Organization (WCO). "WCO SAFE Package: WCO Tools to Secure and Facilitate Global Trade." Accessed January 27, 2016. http://www.wcoomd.org/en/topics/facilitation/instrument-and-tools/tools/safe_package.aspx.

39. WCO. "MRA Guidelines: Guidelines for Developing a Mutual Recognition Arrangement/Agreement." Accessed January 27, 2016. http://www.wcoomd.org/en/topics/facilitation/instrument-and btools/tools/~/media/29AC477114AC4D-1C91356F6F40758625.ashx.

40. Ibid.

41. CBP. "Unified Global Security: The Challenge Ahead." Accessed January 27, 2016. http://www.cbp.gov/sites/default/files/documents/mutual_recognition_3.pdf.

42. WCO, "MRA Guidelines."

43. Ibid.

44. World Trade Organization. "Technical Information on Technical Barriers to Trade." Accessed January 27, 2016. https://www.wto.org/english/tratop_e/tbt_e/tbt_info_e.htm.

45. Ibid.

46. CBP, "Unified Global Security."

47. CBP. "Customs-Trade Partnership against Terrorism Mutual Recognition." Accessed January 27, 2016. http://www.cbp.gov/border-security/ports-entry/cargo-security/c-tpat-customs-trade-partnership-against-terrorism/mutual-recognition.

48. CBP. "U.S., Dominican Republic Sign Work Plan aimed at Mutual Recognition." Last modified May 28, 2015. Accessed January 27, 2016. http://www.cbp.gov/newsroom/national-media-release/2015-05-28-000000/us-dominican-republic-sign-work-plan-aimed-mutual.

49. Froman, Michael. "The Geopolitical Stakes of America's Trade Policy." Foreign Policy, February 17, 2015. Accessed January 27, 2016. http://foreignpolicy.com/2015/02/17/the-geopolitical-stakes-of-americas-trade-policy-tpp-ttip.

50. Permanent Mission of the United States to the United Nations and Other International Organizations in Geneva. "US-AID Announces Global Public-Private Trade Alliance." July 1, 2015. Accessed August 12, 2015. https://geneva.usmission.gov/2015/07/01/usaid-announces-global-public-private-trade-alliance/.

51. Global Alliance for Trade Facilitation. "Global Alliance for Trade Facilitation." Accessed January 27, 2016. http://www.trade-facilitation.org/.

52. The White House. "Fact Sheet: The U.S. Global Anticorruption Agenda." Last modified September 24, 2014. Accessed January 27, 2016. https://www.whitehouse.gov/the-press-office/2014/09/24/fact-sheet-us-global-anticorruption-agenda.

TRADE NETWORK TRANSPARENCY

Trade network transparency entails two dimensions of global commerce: business relationships and chain of custody. Historically, most security programs, including those focused on nonproliferation, have focused on ensuring a proper chain of custody – that is, the physical protection and integrity of a good at various stages of its life cycle, such as during transport on a container vessel. In many areas of global trade and investment activity, however, regulators, experts, and advocates are also scrutinizing business relationships – and the diligence that companies perform to support those relationships. Increasingly, firms are being encouraged, or even forced, to assume some measure of accountability for the actions of their business partners. This report highlights near-term opportunities to advance a shared public-private agenda by leveraging trade network transparency in the domestic and international contexts. Such an approach would go far in ensuring that multistakeholder approaches stand up to the daunting challenges of 21st-century proliferation threats.

STIMSON

WWW.STIMSON.ORG