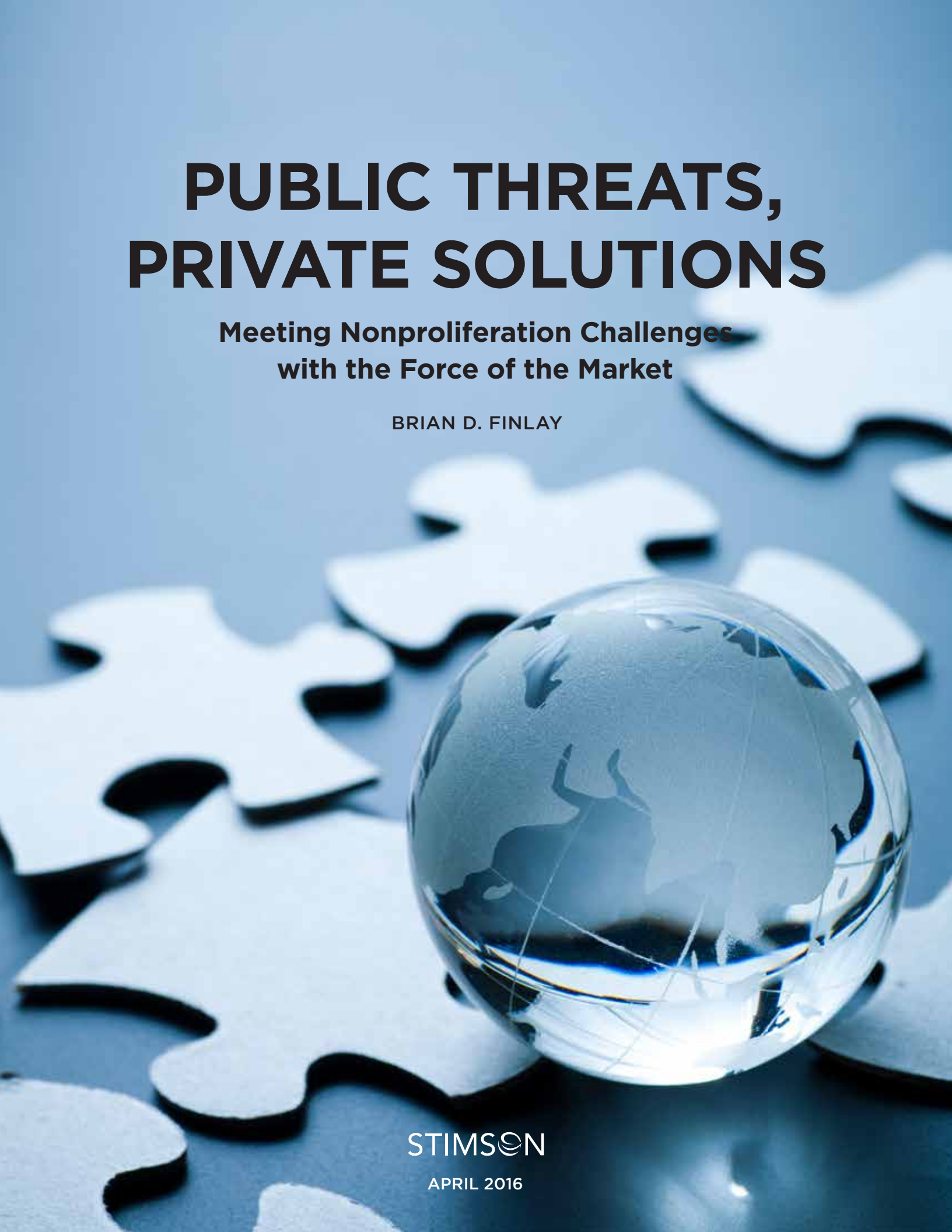


PUBLIC THREATS, PRIVATE SOLUTIONS

Meeting Nonproliferation Challenges with the Force of the Market

BRIAN D. FINLAY

STIMSON

APRIL 2016

Stimson Center
1211 Connecticut Avenue, NW
8th Floor
Washington DC 20036
www.stimson.org

CONTENTS

Acknowledgements

I am pleased to present this report encapsulating the cutting-edge work being undertaken by my colleagues at the Stimson Center in the field of proliferation prevention.

Stimson was founded on the principles of innovation and pragmatism. More than a quarter-century later, that unique brand of addressing the grand global challenges of our time is alive and well, and is reflected in the thinking that has informed this study. It proceeds from the notion that governments alone cannot meet the global spread of weapons of mass destruction nor related technologies. Thus, the report takes a bold approach to better aligning governments' interest in ensuring nonproliferation with industry's imperative to build market value. By better defining "shared value," complementary and sustainable new approaches to proliferation prevention can and have been engendered. Three discrete case studies are presented. Each is eminently scalable and replicable to the global scale and has been demonstrated to be effective in the private marketplace.

Financial support for this project was provided by the John. D. and Catherine T. MacArthur Foundation, the Carnegie Corporation of New York, the Government of Finland, and the US Department of State. We are particularly indebted to Emma Belcher, Theo Kalionzes, Carl Robichaud, Vanamo Sannamaaria, and Ryan Taugher, who have all made important conceptual recommendations and contributions to our work.

Among the staff at Stimson, I am grateful for the substantive contributions to this study made by Johan Bergenas, Debra Decker, and Nate Olson. Their individual research and practical efforts in the field are reshaping the nonproliferation landscape as they redefine how governments and private industry collaborate to address global challenges. Additional thanks go to Nakia Bell, Oksana Bellas, Jim Baird, Miles Abadilla, Ariella Knight, Shannon Dick, Grace Mahoney, and Rose Morrissy. More broadly, I am grateful to all of my colleagues at Stimson who make the organization a vibrant, unique, and intellectually stimulating place to spend the workday.

Brian Finlay
April 2016

For security analysts, the conclusion is clear: globalization has made the world a far less safe and predicable place.

The rapid pace and geographic breadth of technology innovation; the rapidity and volume of international trade; globalized business practices from outsourcing to offshoring and supply-chaining; the atomization of government interests and bureaucratic organization; and the inherent inability of governments to act at the speed of 21st-century commerce: these are but a few factors negatively influencing our ability to manage the lengthening global proliferation supply chain. The net result has been the global diffusion of the "means of production" of weapons of mass destruction (WMD) at the very moment that the traditional instruments of control are being challenged by downward budgetary pressures in government, complex cost-benefit calculations by political leaders, and a rapid evolution of the nature and modalities of the proliferation threat.

These realities necessitate the advent of new approaches that better match and ultimately defeat emerging avenues for proliferation threats. Governments can no longer be solitary nonproliferation activists.

The end of the last millennium brought with it a host of challenges that transcend national borders and institutional and conceptual boundaries: 9/11 and the rise of non-state actors, global disease pandemics, economic crises, and climate change. Globalization has clearly yielded a more uncertain and potentially dangerous world. A rapid increase in the movement of goods and people around the world has fueled a concomitant rise in illicit trade and a surge in profits to global gray and black markets. In 2012 the United Nations (UN) Secretary General's report noted that while over 500 million maritime containers move around the world every year, accounting for 90 percent of international trade, only 2 percent of these containers are physically inspected for contraband on an annual basis.[1] In 2009, the UN Office on Drugs and Crime (UNODC) estimated that transnational organized crime generates $870 billion a year, an amount equal to 1.5 percent of the global gross domestic product and six times the amount of official development assistance.[2] More recent estimates put this number even higher, at closer to $3 trillion annually.[3] Cybercrime, for which private industry bears most of the cost, is also surging. Cyber activities have increased by 26 percent since 2012, and reportedly now cost victims $11.56 million per year.[4] And successive reports by the UN Sanctions Committees on North Korea and Iran demonstrate the widespread exploitation of private industry as both a witting and unwitting facilitator of proliferation.[5]

For security analysts, the conclusion is clear: globalization has made the world a far less safe and predicable place. Yet these grand challenges resulting from globalization have also yielded heretofore unimagined technological, economic, and development opportunities in virtually every corner of the globe. For instance, thanks in large measure to globalization, extreme poverty has declined significantly over the last two decades. In 1990, nearly half of the population in the developing world lived on less than $1.25 a day. Today, that proportion has dropped to just 14 percent – the largest mass migration from poverty in human history.[6] For most of the planet's population, globalization and technology diffusion are rightly celebrated as truly life-changing – and in many cases life-saving – phenomena.

Of course, it is not merely a change in access to the spoils of globalization that has, to varying degrees, revolutionized life in virtually every corner of the planet. We have also witnessed a fundamental evolution in the character and drivers of these trends. Today, the engine of opportunity and prosperity no longer depends on government action. A central defining aspect of globalization is the diversion of power away from the nation-state and into the hands of a wider range of actors. Among these, and in the modern economy, the growth and influence of private industry cannot be understated. Consider that:

- In the 1960s, nearly 70 percent of all money flowing from the United States to the developing world was official development assistance; today, more than 80 percent comes from private sources.[7]
- Globally, private investment flows to developing countries are more than five times higher than formal government aid.[8]
- More than 90 percent of jobs in the world are now in the private sector,[9] a significant change from several decades earlier when public-sector employment constituted almost half of all employment in certain regions.[10]
- Walmart, the world's most profitable company in 2015, ranks as the 28th-largest economy in the world, behind Norway and above Austria.[11]

Private industry can become an overwhelming force for good in the modern economy – provided we can more effectively identify this overlap between government objectives and corporate interests.

The breadth of industry influence demonstrates that without harnessing the wealth of interests, capabilities, and resources of the private sector, governments will inevitably lose the struggle against criminal elements which more dexterously exploit the seams of the global economy for their own political or self-interests. Here, the field of critical infrastructure development is instructive: Macroeconomic reports indicate that the international marketplace in critical infrastructure protection is expected to grow to more than $105 billion by 2018.[12] Overall, global infrastructure investment needs, most of which are in developing countries, will total upwards of $57 trillion.[13] In the coming decades, therefore, decisions made by corporations in the infrastructure, technology, security, and defense sectors will dominate developed and emerging regions' ability to flourish by building resilient societies that can withstand the pressures from a wide range of security and development challenges – including climate change, transnational crime, disease, terrorism, and the proliferation of dangerous technologies. Depending upon their flavor, those decisions will make governmental security and development objectives easier or more difficult.

Even as nefarious private actors exploit the opportunities afforded by globalization, virtually no challenge that transcends international borders can be solved by any government in isolation – nor by any like-minded consortium of governments. Likewise, legitimate companies also see that the dark side of globalization not only threatens broad social values, but challenges corporate interests. This provides for the easy alignment of governmental and corporate objectives. If harnessed appropriately, private industry can become an overwhelming force for good in the modern economy – provided we can more effectively identify this overlap between government objectives and corporate interests.

In short, the scale and complexity of the global drug trade, transnational organized crime, cyber-insecurity, and, perhaps most distressingly, the proliferation of WMD necessitate new approaches that eschew the traditional mechanisms of prevention with more flexible engagements and an entirely new consortium of public and private interests. By better aligning social value with corporate interests, potent new mutually beneficial instruments can be developed that build and sustain a more peaceful and prosperous world.

Public-Private-Sector Partnerships: Then and Now

Over the course of the last decade, the US government rhetoric regarding the need to build a cadre of business partners to promote American interests around the world has proliferated. Recognizing the limitations of government's reach in the modern era, the president's National Security Strategy explicitly calls upon the executive branch to work with industry in developing new so-called public-private partnerships – a voluntary interaction between governments and nongovernment entities where one or both parties draw upon the expertise of the other. The influence of the private sector has grown, and the need for industry to play a key role in meeting global challenges has increased, but despite these efforts the relationship between the private and public sectors has become more distant and contentious.

This is a very different narrative compared to the Cold War era, during which American industry tailored business models to support key US strategic objectives. For example, following World War II, the aerospace, defense, and security sectors, along with other segments of private industry, intensified their relationships with government clients to jointly identify national security needs and design profitable operational plans to address them. These innovative partnerships not only built up the US military to global supremacy, they helped to put humans on the moon, and they generated game-changing technological spinoffs to the civilian sector by connecting the world through the Internet, promoting the development of semiconductors, and introducing GPS technologies.

Project Apollo, carried out by the US National Aeronautics and Space Administration (NASA), is a case in point. The enormous scale of this national initiative, as well as the novel technological challenges associated with it, meant that the government had to rely heavily on private-sector innovation for its implementation from 1969-1972. The result was that with few exceptions, much of the flight hardware was built by private-sector companies. Private companies even operated missions. The government's role was geared toward program planning, preparing guidelines for execution, and overseeing the work accomplished. In short, the public and the private sector leveraged one another's strengths as NASA's relationship with industry was oriented toward a mutually beneficial partnership serving the greater public interest.[14] At least in the case of space exploration, the need for a renewed public-private partnership was recognized.[15]

Examples of sustainable public-private partnerships that yield mutual benefit extend well beyond the immediate realm of international security. The US Green Building Council, a not-for-profit organization, successfully established a set of standards for environmentally friendly building projects termed LEED, or Leadership in Energy & Environmental Design. To use the LEED brand, building projects must satisfy the prerequisites for one of nine different rating systems, and earn credits, or points, toward certification. The nine different categories of ratings represent different types of building projects, allowing LEED standards to be accessible to a wide range of construction projects. A varying level of points increases a building's LEED certification level from "certified" to "silver," "gold," and "platinum," incentivizing continuous efforts for improvement beyond basic certification.

In order for programs such as LEED to be successful, they need to have a strong brand name and awareness. The LEED team has marketed the brand with enormous success, and today LEED certification is globally recognized as a mark of green building. Additionally, investments in LEED buildings pay back over the years because those buildings are less costly to operate, increase property value, and may qualify for tax rebates and zoning allowances. This back-end appeal to what matters most to industry is essential. The LEED brand combines a set of implicit and explicit incentives to create a desirable brand for the market, yielding broad social and environmental benefits as well as meaningful corporate value.[16]

Key to the success of the LEED brand is that it was created out of an industry-led nonprofit. As such,

buy-in from industry was nearly guaranteed, as was the industry-specific knowledge necessary for designing a program that could integrate into existing industry standards. This is a useful example for national security partnerships. Industries involved in national security are often solely on the receiving end of regulations, and thus the relationship between industry and regulators is one of "push and pull" around specific regulations. If an industry body were to lead the conversation on formulating mutually agreed-upon regulations, much of this tension and time – and thus money – could be saved.

It is also the case that the force of the market can be leveraged by industry for social value even in the absence of government action.

The LEED brand also was marketed so effectively that it became publicly recognizable to consumers, and this greatly incentivized companies to invest in the accreditation process – thus it was the consumer who placed the pressure on the company rather than on the government or a regulatory body. The national security space, while it faces specific challenges due to the confidential and serious nature of the products and their regulation, could certainly learn from the LEED example in the areas of brand recognition (e.g., a "National Security Gold Standard"), tax rebates, and the importance of effective marketing.

It is also the case that the force of the market can be leveraged by industry for social value even in the absence of government action. Here again, the environmental sector has been a pioneer. For example, according to a recent study, 65 percent of car owners in the United States overpay for insurance because they do not drive enough to warrant the level of coverage offered by insurers, and thus are subsidizing those 35 percent who drive the most. MetroMile, a new pay-per-mile insurance company that rewards consumers for spending less on fuel and shortening commutes, was founded in response to this market discrepancy. The company developed a technology application that attaches to a plug-in device inside of cars in order to track consumer mileage. Driving less than 10,000 miles per year can yield cost savings of up to $400 for individual consumers through this mileage-based, transparent pricing of insurance. Use of the application benefits all parties by promoting tangible environmental benefits, reducing risk for insurers, and incentivizing good behavior via the private insurance market.[17]

This model rewards consumer self-reporting that exceeds the levels required by regulation. Rewards match behavior, encouraging maximum self-reporting and improved behavior. Furthermore, the simple process and affordable technical application decreases consumer risk for participation, and the transparency in direct mileage-based pricing builds consumer trust. The national security industry could benefit from this model. Given the industry's seemingly onerous regulatory workload, the relationship between industry and regulators tends to be terse and resentful. By giving industries the opportunity to report more frequently, and with supplementary information through a streamlined process, regulators could offer companies tangible benefits such as tax rebates, fewer or faster audits, or a "fast lane" for import processing or export licensing.

With insufficient resources to achieve their missions, members of the global development community have long seized upon the force-multiplying power of private industry. In 2013, for instance, President Obama launched the program Power Africa with the goal of bringing together technical and legal experts, the private sector, and governments from around the world to work in partnership to increase the number of people on the continent with access to affordable power. Recognizing that government investment alone is incapable of providing the nearly $300 billion in investment needed to achieve universal electricity access to sub-Saharan Africa by 2030, Power Africa leverages private-sector investments, beginning

Traditional "technology denial" strategies enforced by committed governments will no longer hold the line against a growing tidal wave of technology diffusion and trade liberalization that is forcing proliferation-sensitive ideas into more hands in more corners of the globe than ever before.

with more than $9 billion in initial commitments from private-sector partners to support the development of more than 8,000 megawatts of new electricity generation on the continent.[18] Such partnerships not only satisfy the mandate of the US Agency for International Development (USAID), they do so by promoting corporate interests in sustainable energy partnerships that yield mutual benefit.

As noted, public-private partnerships in the security realm have proven to be far more elusive – and with respect to nonproliferation, nearly nonexistent. As committed proliferators have morphed to take advantage of the modern economy, the international community has largely responded by doubling down on past practices that have proven effective at preventing proliferation in the past. Yet in a globalized world, traditional "technology denial" strategies enforced by committed governments will no longer hold the line against a growing tidal wave of technology diffusion and trade liberalization that is forcing proliferation-sensitive ideas into more hands in more corners of the globe than ever before.

To the limited extent that private industry has been drawn into public-private security partnerships, the record of the nonproliferation community has been spotty. Driven in part by national security budgets that once grew reliably year after year, the nonproliferation policy community has had little need for mutually beneficial partnerships with industry. Industry partners could either be bullied into cooperation through rigorous regulation, or induced to collaborate through direct contracting with government procurement agencies. Few examples of successful and sustainable partnerships – where government and industry work for common nonproliferation cause, even in the absence of a direct financial transaction – are evident.

This is not to suggest that governments have failed to recognize or make tentative efforts to develop effective partnerships with private industry for the purpose of proliferation prevention. Perhaps the best example of national security engagements involving industry in cooperative nonproliferation began with the end of the Cold War, when the US government initiated programming that was focused on redirecting erstwhile Soviet weapons scientists, engineers, and technicians to nonweapon enterprises. These efforts included the cooperative biological research program at the Department of Defense, the Department of State's Global Threat Reduction Program, and the Department of Energy's Global Initiatives for Proliferation Prevention programs. The stated objective of each of these programs was to permanently and sustainably redirect former WMD specialists. Yet with the exception of those programs that sought to systematically create sustainable job opportunities for the targeted scientists within private industry, few of these efforts yielded sustained security results – largely because of a lack of engagement with the private sector.

Where private industry was involved and saw commercial benefit from engagement, sustainable opportunities were created for former Soviet weapons specialists. This led to both durable nonproliferation and corporate profit. The case of QED Technologies is a textbook example of a successful and sustainable project of technology transfer leading to successful commercialization and the permanent and sustainable redirection of scientists. Byelocorp Scientific Inc. (BSI), a privately held American company established to

develop business opportunities in the former Soviet Union, identified magnetorheological finishing (MRF) as a promising new technology at a state-owned laboratory in Belarus. The company surveyed the US for potential markets, which led to a collaborative relationship with the University of Rochester's Center for Optics Manufacturing (COM). COM had previously received substantial funding from the federal government to develop new optics manufacturing technologies that would ensure that the United States did not fall behind, or become dependent upon, foreign countries for specialized optics in defense applications. This partnership offered a potential go-to-market opportunity for the research of the former Soviet weapons scientists.

In an era of dramatically tightening budgets and changing global realities, the national security enterprise must learn to better pool resources with industry over shared objectives – and learn and live the true meaning of partnership.

Initial collaboration with COM soon produced a patented application of the technology. BSI then set up a new enterprise, QED Technologies, to develop a commercially viable machine using the technology that could be sold to commercial optics manufacturing companies worldwide. Additional government support was then secured through the US Department of Defense Small Business Innovation Research program, which funds staged defense technology development at small businesses throughout the United States. The Civilian Research and Development Foundation, a nongovernmental organization established by Congress to facilitate a variety of basic science, nonproliferation, and threat-reduction activities in the former Soviet Union, also provided funding for travel grants and exploratory research to assess the ability of former weapons scientists to contribute to new innovations in QED's optics manufacturing technology.

Within two years, BSI, COM, and the former weapons laboratory in Belarus developed a patented application for magnetically controllable fluid for optics finishing. Two years later, QED developed a commercially viable machine for optics manufacturers. In the end, Soviet scientists' former experience in basic research in magnetically controllable fluids helped them, in another industry, to develop a commercially viable optics finishing technology for the private marketplace.

A 2007 study by the Stimson Center found that sustainable nonproliferation engagement ultimately necessitated a transition from government investments in redirecting scientists to private-sector investments in business development.[19] To ensure employment beyond the funding horizon of US nonproliferation programming, new models of engagement must be based on long-term partnerships with the private sector. The example of QED Technologies could not have been achieved without short-term incentives that motivate private-sector interests and mitigate risks in the near term and also help secure financial investments in the long-term. In the end, modest government investments led to long-term sustainable engagement of the "target" community of weapons researchers, along with other economic development dividends pursued by the United States government. Similarly, the partnership yielded significant financial dividends for industry partners that incentivized their ongoing participation, even absent government funding.

Government regulation will, of course, remain central to preventing proliferation for the foreseeable future. But recent history demonstrates that it will no longer suffice. In an era of dramatically tightening budgets and changing global realities, the national security enterprise must learn to better pool resources with industry over shared objectives – and learn and live the true meaning of partnership.

The Role of Industry in Proliferation

As noted above, the decentralization of the modern economy has given rise to criminal actors who prey upon these trends to market their illicit wares. This is not simply the case for the global trade in narcotics, or counterfeit items such as T-shirts and pharmaceuticals, but extends similarly to those intent on profiting from the proliferation of WMD knowledge and technologies. Aligning the social objective of nonproliferation with corporate interests necessitates a better understanding of the marketplace for dual-use goods and know-how.

While there are many different actors that require dual-use technology, a typical customer rarely exists. Ranging from friendly states to nefarious individuals and corporations, customers exist within a complex global system that exists to fulfill these orders. Beginning with the manufacturers and moving through to retailers, supply-chain companies, and then to proliferators, each stage of the process offers up a great deal of information regarding the customer. Bad actors do not just include nefarious individuals or known criminal organizations or companies; they can also include state actors who then market this technology to sell to companies or individuals.

There are currently a great deal of state and supranational mechanisms to curb the illicit diversion of proliferation-sensitive knowledge and technologies, yet they often fall short because of a lack of information, enforcement, or political will. While many national control systems are in place around the globe, they are often viewed as being in direct competition with higher national economic priorities. For instance, the mistaken belief that enhanced nonproliferation controls will reduce competitiveness in the global supply chain has been a core challenge to the implementation of strategic trade controls. If governments conclude that enhanced regulation at their borders or in the export process will result in a competitive disadvantage, the politics of developing a rigorous control regime can be daunting and even insurmountable. And even when legal regulation and political commitments exist, many governments lack the requisite resources to enforce these standards across a growing industry.

Even the most cursory glance at the proliferation environment suggests that these widening bureaucratic trade-offs and capacity gaps have proven to be meaningful. Despite international efforts against the spread of weapons-usable material, proliferation networks have been able to illicitly transfer dual-use technologies to military and civilian weapons programs in several countries. Iran has been able to obtain dual-use goods even through international sanction regimes. In late 2012, an Iran-bound ship from China was intercepted and found to be carrying carbon fiber made by Toray Industries Inc., which was believed to be intended for use in Iran's nuclear program.[20] Materials used for biological warfare technology in Iran have also been linked to two Chinese companies, Oriental Scientific Instruments Corporation and Zibo Chemical Equipment Plant (both of which have been sanctioned independently).[21] Three recent cases of export control violations in Germany resulted in the shipment of dual-use materials with applicability to Iranian missile and WMD programs.[22] A businessman from the United Kingdom was also fined £68,000 after he exported £3 million worth of banned dual-use items – alloy valves, which are useful in WMD construction – to Iran in defiance of a UK export ban.[23]

Pakistan is another case study for failures in governmental nonproliferation controls. The A. Q. Khan network helped to spur the acquisition of nuclear weapons capabilities through a network of global exporters. Over a 10-year period, the A. Q. Khan network successfully exported nuclear centrifuge technologies and other sensitive knowledge and materials to Iran, North Korea, and Libya, and possibly to other countries and non-state actors that have not yet been realized.[24] Prior to the formation of Khan's own network, the Pakistani nuclear weapons developer likely received dual-use industrial equipment

from Henk Slebos, a Dutch national who was able to evade prosecution several times until he was finally convicted of illicit exporting of restricted goods in 2005.[25] In addition, the British firm A. M. Castle & Co. successfully shipped a consignment of dual-use alloy metals to Pakistan in 2001.[26] More recently, the owner of Trexim Corporation was sentenced to two years in a United States federal prison for attempting to export a dual-use item without proper licensing – and the investigation revealed that he had successfully shipped several other items with dual usability for military and civilian applications in the past.[27]

For every illegitimate firm there exist hundreds or even thousands of companies that are making the right decisions to help identify and disrupt the activities of committed proliferators.

Wittingly or not, these cases indicate the negative contribution that companies can make to the global proliferation supply chain. Of course, for every illegitimate firm there exist hundreds or even thousands of companies that are making the right decisions to help identify and disrupt the activities of committed proliferators. Enlisting their support and rewarding that behavior can yield a powerful and essential set of new allies to government.

In each of the proliferation incidents described above, opportunities existed for legitimate private enterprise to have taken a stronger role in identifying and disrupting illicit transactions. Yet our failure to better recognize and adapt to industry motivations has impeded our ability to establish more meaningful cooperation with industry. In short, technology denial strategies have yielded a culture of compliance over one of cooperation.

The Challenges of Public-Private Cooperation

The lessons learned from previous efforts, particularly in the global development realm, as well as the changing market realities related to proliferation demonstrate the potential benefits of innovative engagement with private industry. Our common failure to develop such sustainable public-private partnerships to help prevent the proliferation of WMD is not the result of unenlightened thinking or a lack of effort on the part of government or industry. Political leaders have called for the development of public-private partnerships.[28] Business leaders have recognized the shared concern over the proliferation and potential use of WMD.[29] And at least in the case of the US government, tentative efforts have been made to develop cooperative approaches that leverage mutual interests even beyond immediate security imperatives.

A 2014 task force convened by the Stimson Center identified numerous cases where government-industry cooperation would have been mutually beneficial but failed to materialize for reasons related to legal prohibitions, competitive risks, or an unconvincing cost-benefit calculus. The impediments to public-private cooperation in general are numerous – and in the case of security cooperation, are particularly plagued by a lack of understanding between government and industry around their respective capabilities, resources, and interests; a lack of joint decision-making and operational capacity between government and industry that would otherwise ensure mutual benefit; a lack of clarity on regulatory regimes and enforcement practices; and a lack of a regulatory environment that promotes innovation in service of both security and economic competitiveness.[30] Perhaps most importantly, the national security community has systematically failed to comprehend and design against the motivating incentives

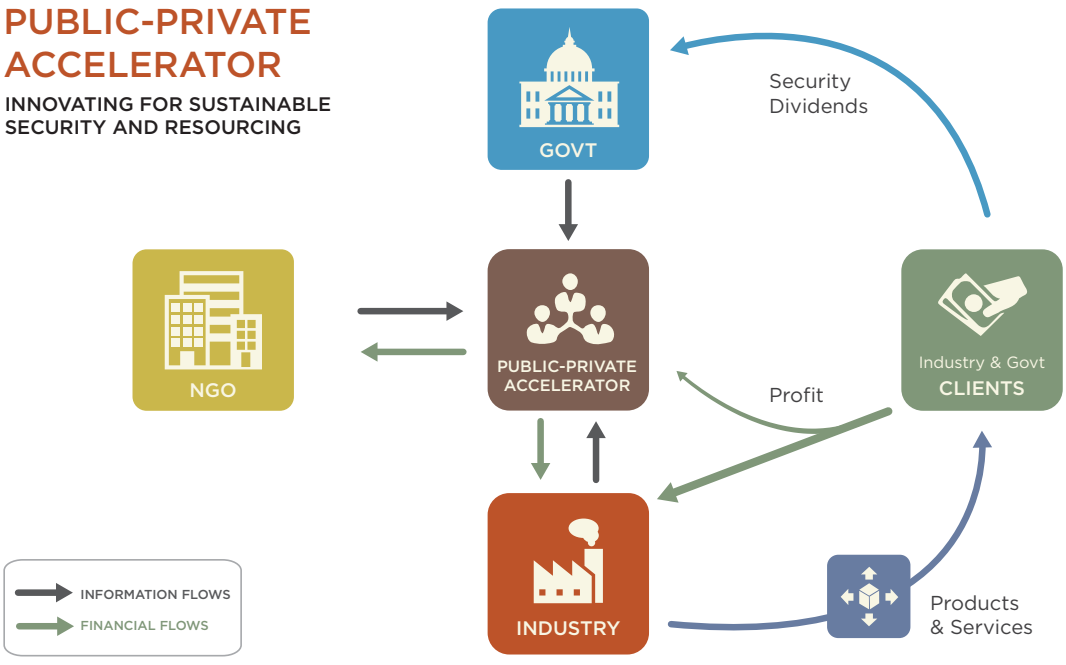
that yield sustained industry engagement of nonproliferation. Any future public-private partnership must correct for these previous shortcomings and essential requirements.

The Nonproliferation Accelerator

An approach to nonproliferation that builds upon the convergence of business opportunity and social value must go beyond traditional philanthropy or even corporate social responsibility. Unfortunately, while governments and the nonproliferation community are especially adroit at identifying threats and wider social needs, they are less well placed to assess business value. An innovative new organization – a nonprofit Nonproliferation Accelerator (see Figure A) – could advance nonproliferation objectives *and* produce financial value for industry stakeholders and the policy community, which could provide mutual dividends for both government and the private sector. This Nonproliferation Accelerator would enable government, industry, and nongovernmental organization (NGO) stakeholders to jointly develop an array of products (including, for instance, new insurance products, risk-management tools, investment instruments, new technologies, and data collection, analytics, and dissemination products) that would advance nonproliferation while responding to market demand for sensors and scanning equipment, information-sharing mechanisms, analytic and risk management services, and insurance and standards development.

The Accelerator would pool the knowledge of government, the nongovernmental expert community, and private industry to incubate relevant products and services designed to address 21st-century proliferation threats. The financial returns from these products would be returned to industry, with a portion of that yield recapitalizing the Accelerator. The wider security or social dividends would accrue to all actors, but would ultimately help satisfy government nonproliferation objectives.

FIGURE A

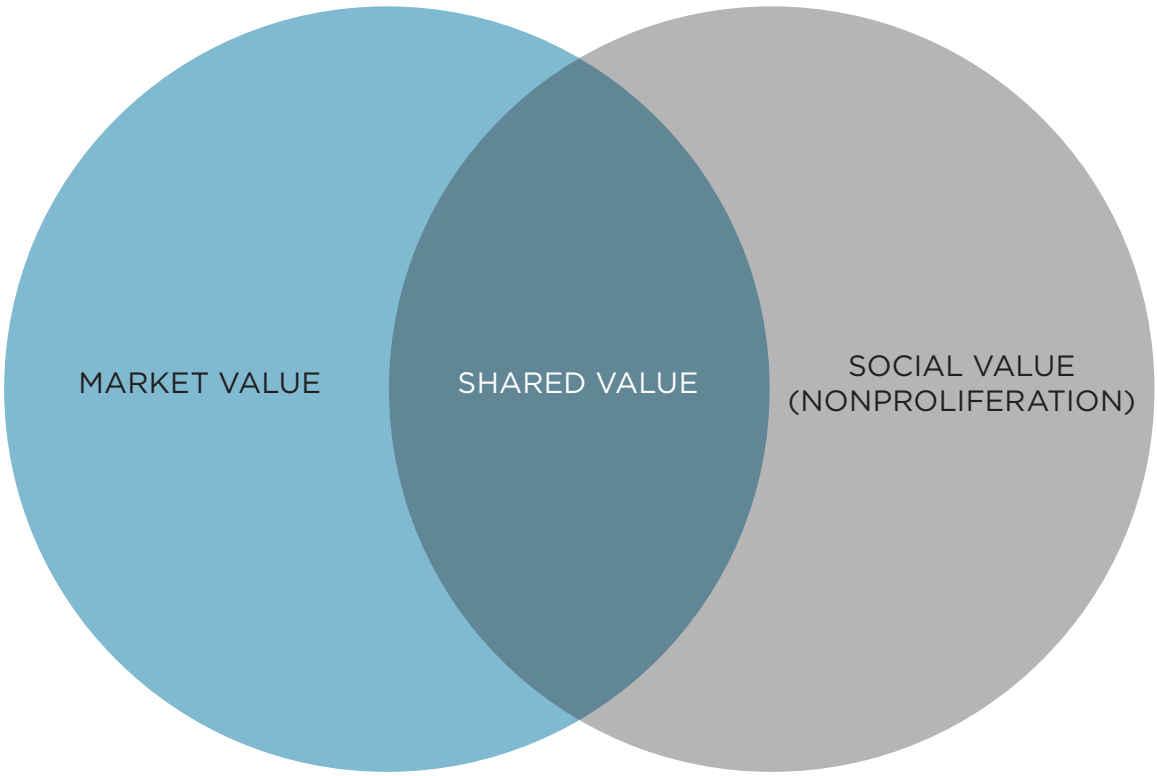


Building the Strategy

The entrepreneurial process of starting a business is straightforward: (1) Identify a need; (2) Identify a customer; (3) Develop an operational plan; (4) Identify how to make money through those operations; and (5) Identify the team necessary to execute that strategy. This process, at a micro level, is used to start one company. That company will work only when it knows and understands the problem it wants to solve, for whom it is solving the problem, how it will solve the problem, how it will make money solving the problem, and who will make the plan to solve the problem tangible. This straightforward logic can be coopted by governments to help achieve durable solutions to societal challenges—including the threat of proliferation.

The objective of the Nonproliferation Accelerator should be to develop new, authentic public-private partnerships that involve voluntary interactions between governments and nongovernment entities where one or both parties draw upon the expertise of the other. The Accelerator could help incubate new companies where there is a market gap, or work with existing firms to build new products. Either way, these efforts must go beyond corporate social responsibility and appeal to the vested self-interest of both public- and private-sector stakeholders (see Figure B). This approach to building shared value will create new nonproliferation instruments in a self-sustaining manner that homes in on market-driven solutions.

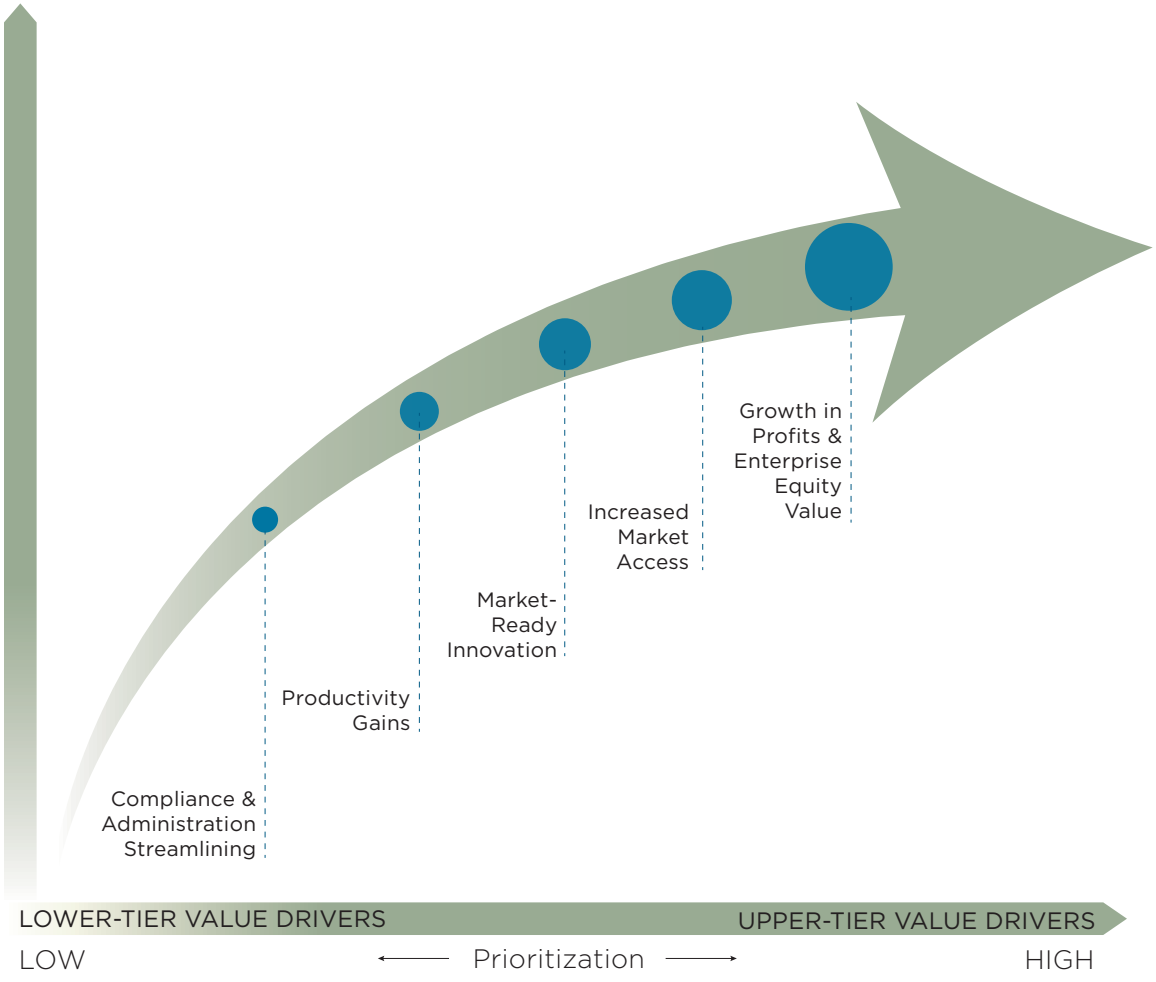
FIGURE B: DEFINING SHARED VALUE



Defining Shared Value

Each output of the Accelerator should result in an instructive demonstration of the social value of security for governments while better addressing the value-creation objectives of industry. These incentives can range across a broad spectrum (see Figure C), and are best defined by industry partners in collaboration with government. The benefits of cooperation for industry could range from streamlined regulatory measures that promote the core business to direct financial value through enhanced profits via new products or growth in overall enterprise equity value.

FIGURE C: DEVELOPING INDUSTRY INCENTIVES

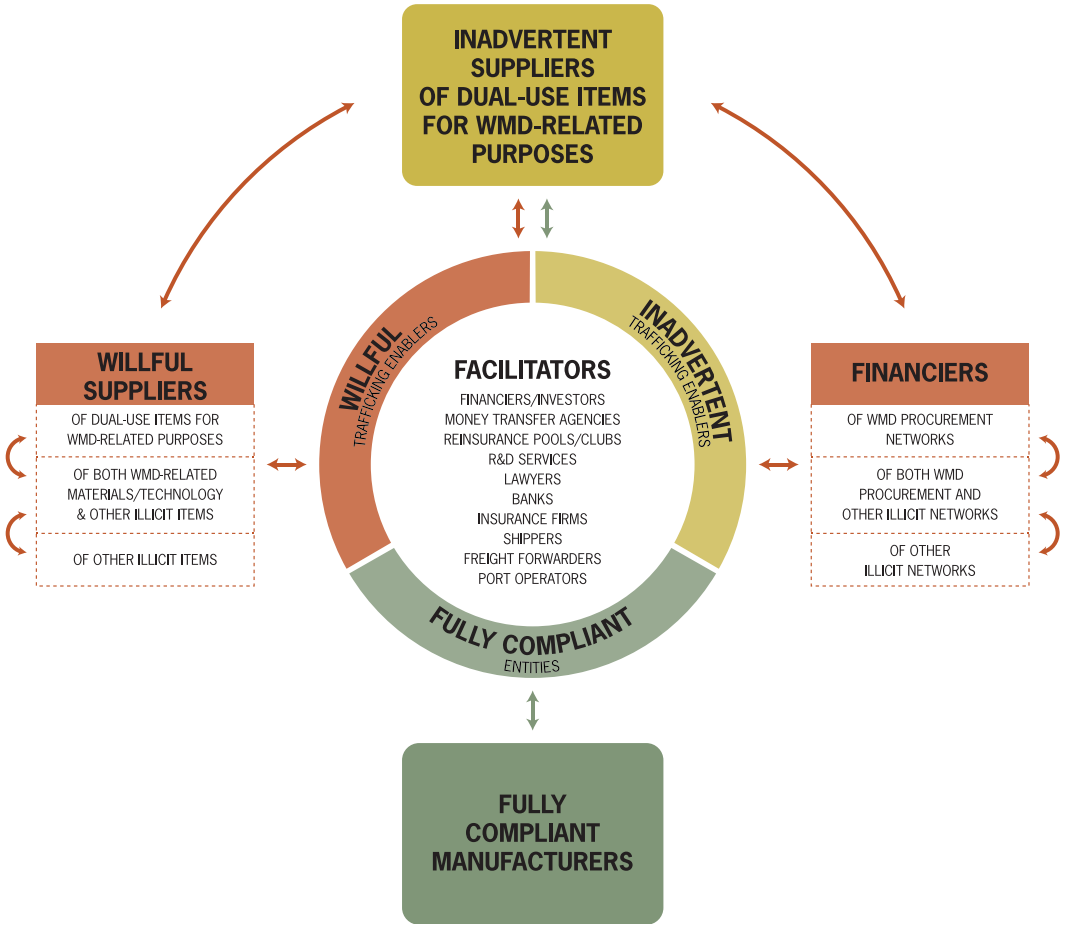


Adapted from Nate Olson and Brian Finlay, Market Power: Adapting Public and Private Roles for Transnational Commerce and Transnational Threats (Washington, DC: Henry L. Stimson Center, 2013), http://www.stimson.org/images/uploads/research-pdfs/Market_Power_Sep2013.pdf.

Identifying Private Partners

Recent state efforts to engage private industry have focused on the extreme ends of the proliferation supply chain: technology innovators and manufacturers at one end, and end users at the other. Yet modern supply chains are a complex system of interlocking actors and processes that span the globe and involve not only businesses that physically move products, but financial and communications firms, insurers and reinsurance companies, standards-development organizations, private security firms, money transfer agencies, and a host of other operational service providers critical to the smooth operation of the global supply chain (see Figure D). Each of these industries has a potential role to play in the nefarious transit of WMD materials and know-how – or preferably in a networked response to proliferation. Similarly, all have a potential stake in the benefits of a Nonproliferation Accelerator.

FIGURE D: COMPONENTS OF THE PROLIFERATION SUPPLY CHAIN



Adapted from Nate Olson and Brian Finlay, Market Power: Adapting Public and Private Roles for Transnational Commerce and Transnational Threats (Washington, DC: Henry L. Stimson Center, 2013), http://www.stimson.org/images/uploads/research-pdfs/Market_Power_Sep2013.pdf

An overlay of current market trends in the proliferation arena with an assessment of industry interests yields some low-hanging fruit for the nonproliferation sector. Early efforts should be focused on third-party mechanisms whose functional roles are oriented to:

1. Development of robust mechanisms for information-sharing between government and industry on real-world proliferation challenges;
2. Development and dissemination of best practices for compliance with trade controls and other controls that could provide public and private benefits;
3. Creation of new specialty insurance products including "compliance insurance," and other "dual-benefit" products such as surety bonds on sensitive materials for end-of-life disposal; and
4. Technology development and application of products that can help identify and ultimately address proliferation, particularly related to border security, countertrafficking, and trade efficiency.

With the goal of developing viable pilot ventures that would operationalize discrete proofs of concept, the Stimson Center launched three demonstration projects using the force of the market itself as motivation for enhanced nonproliferation activities. The working theory throughout those efforts was that if capacity-building connections across security and development areas could be found, new resources from the private and public sector could be generated for the mutual benefit of the WMD nonproliferation regime, as well as for broader security and development capacity-building efforts. Ultimately, this would usher in a new model for bringing on board private-sector actors not on the basis of legal regulation, or even as government clients, but rather based upon their own assessment of corporate interest in the private market.

Case Study 1: Border Security through Public-Private-Sector Partnership – Project Ngulia

In April 2004, the 15 members of the United Nations Security Council voted unanimously to pass Resolution 1540 (2004).[31] The measure mandated an array of global supply-side controls over sensitive weapons, materials, technologies, and know-how. Three years after the events of September 11 – and on the heels of astonishing revelations that rogue Pakistani scientist A. Q. Khan had shared WMD technologies with North Korea, Iran, Libya, and potentially even Al Qaida – the resolution sought to rectify the inadequacies of the existing control regime, and the particular challenge of WMD proliferation to non-state actors.

Yet even as each of the 15 Security Council members cast a vote in favor of the resolution, for the 80 percent of the world's population living on less than $10 a day, far more immediate security and development threats were rightly being prioritized.[32] For instance, in the same month that Resolution 1540 was promulgated by the Security Council, more than 100 suspected Jemaah Islamiah militants were killed during attacks on security outposts in Thailand's Muslim-dominated southern provinces. In Damascus, Syria, a bomb explosion and gun battle between security forces and a terrorist group killed four people and left a UN building badly damaged. In a village in southern Kyrgyzstan, a landslide left 33 people dead and a nation struggling to recover. That year in sub-Saharan Africa, 1 in 12 adults was newly infected with HIV/AIDS, as life expectancy trends continued to plummet.[33] Also in 2004, Colombia retained its rank as the largest producer of cocaine, and homicide rates across the country remained among the highest in the world – upwards of 490,000 deaths resulted from armed violence in that year alone.[34]

Amid pervasive economic deprivation, human insecurity, deteriorating public health, lack of access to basic education, poverty, hunger, and environmental degradation, it was little wonder that Resolution 1540 was met by much of the world with a significant measure of disinterest bordering on disdain. Two full years after enactment of the resolution, 62 countries had failed to fulfill even the most basic requirement by submitting an initial progress report to the 1540 Committee in New York – the entity responsible for monitoring implementation of the 2004 resolution.[35] Unsurprisingly, the vast majority of non-reporting states were countries of the Global South – often the same countries with the weakest preventive measures and enforcement capacities.

In response to this burgeoning North/South divide on the full and effective implementation of the resolution, and to the global nonproliferation regime more generally, the Stimson Center developed an innovative approach that would build more pragmatic and durable engagement on the nonproliferation issue. What was clear was that a modernized nonproliferation strategy that successfully built buy-in among governments of the developing world needed to begin by changing the terms of the then-current debate. A range of approaches, from the continued (and often sanctimonious) appeals by economically more advanced governments to legal mandates, along with the stark facts of the dire human and financial costs that a WMD incident could yield – and even tangible evidence of proliferation itself – had systematically failed to inculcate more robust adherence to the nonproliferation regime across much of the developing world. A new approach that inspired sustained and pragmatic engagement with these new proliferation-capable actors was necessary. In short, only by appealing to the higher-priority interests of countries in the Global South – on both sides of the security/development divide – could countries be transformed from recalcitrant "targets" of nonproliferation policy into sustained advocates for effective nonproliferation engagement.

Fortuitously, when it is considered more innovatively, much of the generous assistance offered by wealthy industrialized governments in the name of nonproliferation is directly applicable to the more immediate challenges facing countries of the Global South. For instance:

- Assistance provided to enhance border and export controls can also aid the prevention of small-arms or drug trafficking and promote efficiencies at transit hubs for legitimate commodities. These, in turn, facilitate trade expansion, business development, and national competitiveness within the global supply chain.
- The same resources and capacities necessary to detect the illicit movement of terrorists across borders can also help address human trafficking – a growing moral priority for many governments across the Global South.
- Detecting and responding to biological weapons requires a functional disease-surveillance network and a public health infrastructure.
- Assistance proffered to develop pre- and post-WMD incident response enhances governments' capacity to detect an earthquake or respond to a tsunami.
- Governments' pursuit of energy diversification through nuclear power can be aided and accelerated with technical and capacity-building assistance from nonproliferation accounts, all while reinforcing global confidence in a government's adherence to the regime.[36]

In 2012, together with a Kenyan research organization and in collaboration with the Office of the President of the Kenyan government, Stimson conducted an 18-month analysis of security and development challenges in Kenya, and by extension, across Eastern Africa. The project rationale was driven by growing concern that East Africa had the potential to become an entrepot for the transshipment of technologies associated with the proliferation of weapons of mass destruction.

By building common capacity at the border, multiple trafficking streams could be disrupted, economic security could be enhanced, and corporate value could be demonstrated.

During this research phase, it became clear that the government of Kenya, and others in the region, were increasingly concerned with the emergence of terrorists and transnational organized criminals, and the convergence of illicit trafficking in small arms, drugs, people, and wildlife – with the networks capable of facilitating proliferation. An interministerial network of Kenyan authorities participated throughout the analysis, identifying national border priorities, border strategies, and capacity shortfalls. The research team and government stakeholders recognized that Kenyan "border insecurity" – broadly defined not only as threats to external national borders, but to the internal boundaries that surround a wide range of important societal functions and resources including ports, airports, critical infrastructure, and even national wildlife parks – posed a threat to the country's national interests. Inadequate border security challenges Kenyan economic, social, and political objectives as laid out in the nation's development blueprint, Vision 2030.[37]

For other stakeholders within the Kenyan government, border insecurity challenged the country's strategies to combat terrorism; piracy; the influx of refugees; and the proliferation of illicit trafficking in small arms, drugs, and people; as well as wildlife poaching and the smuggling of a wide range of consumer goods. Insecure borders were also seen to promote criminality related to armed conflict, which in turn negatively impacts national development and economic prosperity. This convergence of threats across the country's economic, development, and security interests became tragically evident with the 2014 attack on the Westgate Shopping Center.[38] The activities of al-Shabab had been financed, at least in part, from the proceeds of wildlife poaching.

Porous national boundaries and inadequate security at ports and airports are also, of course, a threat to the proliferation and spread of WMD. In short, enhanced border security is a bridge to both development and security, none of which can be achieved without the other. For the government of Kenya, the proliferation of weapons of mass destruction is, in essence, a border management issue that impacts not only upon Kenya's global nonproliferation obligations, but also upon its wider security challenges and long-term prospects for economic development.

Piloting a Public-Private-Sector Partnership for More Integrated Capacity Building

Under the premise that increased border capacity is a priority for the public sector's security and development communities, and that shared value can be found with the private high technology and telecommunications sectors, Stimson set out to assemble a consortium of Kenyan and international stakeholders from both the public and private sector that could participate in a demonstration project in Kenya related to border security. The objective was to develop a pilot effort whereby coordinated border security could yield benefit at the intersection of multiple trafficking flows. In other words, by building common capacity at the border, multiple trafficking streams could be disrupted, economic security could be enhanced, and corporate value could be demonstrated. The government of Kenya invited the initiative to conduct this pilot project to build capacity against a wide variety of countertrafficking challenges, and entered into a memorandum of understanding (MoU) with Stimson.

Under this agreement, the project team concluded that by building countertrafficking capacity around one high-priority objective for the Kenyan government – in this case, the prevention of wildlife poaching – a scalable and replicable strategy could be expanded to better manage security at national borders and ultimately help to also prevent the cross-border flow of proliferation-sensitive items that remain a core concern for the international community.

Per the invitation of the Kenya Wildlife Service, a public-private-sector partnership was formed to build a border-security capacity-building program in southern Kenya at the Tsavo West Ngulia region near the Tanzanian border. The project was initiated in light of rising levels of environmental crime, including poaching of elephants and rhinoceroses, and increasing connections to broader security and development challenges, including the financing of terrorist organizations in sub-Saharan Africa.

Consider the following dynamics around the poaching and wildlife crime challenge:

- More than 140,000 elephants and upwards of 3,600 rhinoceros have been killed in recent years, and Kenya's black rhino population has gone from 20,000 to 650 since the 1970s.
- Approximately 15 percent of Kenya's GDP comes from tourism – a sector driven by the country's popular wildlife.
- The illegal wildlife trade generates between $7 billion and $23 billion in revenue every year – more than the illicit trafficking of small arms, diamonds, gold, or oil – and the UN Secretary General, national governments, and independent NGO analyses all have drawn direct and indirect links between poaching/wildlife crime and transnational criminal organizations, insurgencies, and terrorist organizations in Africa.
- This illicit trade promotes a culture of corruption at the border that, in turn, facilitates the cross-border flow of all manner of contraband – including, potentially, WMD items.

Building the Case for Private-Sector Participation

Over the course of 12 months, Stimson engaged more than a dozen private-sector technology firms seeking their participation in the project. To date, about half of the companies approached by Stimson have made direct contributions to the execution of the field project in Kenya, while others have engaged in various different ways in our technology test arena in Sweden.[39] Two specific phases were essential to protecting the integrity of the project and rallying the support of industry to make investments in the project, which subsequently led to a public-private-sector partnership in executing the initiative. The objective of these firms went beyond the protection of animals, and reflected their direct business interests in demonstrating a wider applicability of their technologies to a growing global problem – and hence, a growing global market.

Phase 1: Build a Project Free of Private-Sector Bias

In order for the project not to be associated with any given company or product, Stimson worked with a technology university that designed, together with the Kenyan government, a technological action plan for the border security efforts at Ngulia. This plan became foundational for negotiating the MoU with the Kenyan government. With an established baseline for our efforts, the plan of action (and not the private-sector interests) drove the selection of the technology solutions that were implemented on the ground.

Phase 2: Building a Multifaceted Pitch to Industry

In seeking to identify sustainable and long-term partnerships with industry, Stimson project managers surveyed a wide variety of pressure points that we thought would positively impact private-sector partners to join our efforts. In no particular order, they included:

- The project would identify new value and user-areas for products that industry already had in their product portfolio.
- Industry could leverage the pilot project as a case study that moved away from development aid toward more business-oriented agreements with government actors and other businesses.
- Organizations from developed nations would identify and capitalize on new markets through participation in a demonstration project in an emerging market.
- Through the partnership with the technology university, companies would receive inexpensive system integration, thought leadership, and information for their products.
- New products and spinoffs would emerge from the project.
- The project would represent a platform where peer industry representatives could find new opportunities for collaboration.
- The project would assist companies with public affairs and corporate social responsibility activities throughout the project period.
- Corporations would sustain their involvement through direct market incentives.

Project Execution

The project plan, in short, included designing, developing, and deploying a command, control, and communications (C3) system followed by the integration of radar and other sensors. Following several visits to the pilot site by the technology university and Kenyan information and communications technology professionals to collect information from commanders, rangers, and researchers, a smartphone-based C3 software was designed and developed by project partners who invested their own resources.

The C3 system is an input device with which rangers can note their observations regarding security and wildlife matters. Photo documentation is available, as is automatic geotagging. The app is also a navigation tool, whereby park rangers can view their position overlaid on a map. The interface includes local landmarks such as waterholes, roads, trails, bunkers, borders, patrol routes, and the like. The commander app includes the same functionality as the ranger app, but is foremost an administrative tool and platform for officers. The map interface shows the position and trajectories of all rangers and vehicles, security alerts, and animal observations. The data can be accessed in real time or analyzed in retrospect. Commands are issued by secure-broadcast voice or text messages, and patrolling routes or ambush positions are defined for individual rangers.

A Kenyan telecommunications company agreed to support the pilot project with SIM cards, airtime, and data, while improving connectivity at the wildlife sanctuary through a partnership with another global telecommunications firm. A dozen additional partners came together to participate in this pilot project, bringing goods, services, and capacity-building knowledge.

Within months, the C3 platform was launched in the field, including smartphones to rangers, tablets to commanders, as well as hardware to improve connectivity. These investments were made by the technology university with support of the public-private-sector consortium.

As the C3 platform was being rolled out in Ngulia, additional sensor systems were simultaneously tested in Kolmården Wildlife Park in Sweden to evaluate their applicability to the Ngulia project. The technology tested includes sensor systems and radar for border and intruder detection. Training and educational activities ran concurrently. Project partners were asked to make contributions on as-needed basis, and to date the team has secured the following core components to an integrated border management response at the park:

- Project management support;
- Product design, user experience, and development support for the C3 system;
- System integration support;
- Radar under a lease agreement;
- Sensor solutions to be tested in controlled environments before deployment in the field;
- Tests of unmanned vehicles; and
- Market analysis.

Project partners believe that a phased approach to technology development and deployment is important. During the successful execution of previous phases, partners will continue to secure the relevant stakeholders and hope to deploy additional technology at Ngulia. The testing at Kolmården will be critical for additional technological steps, as well as ensuring that the solution remains cost-effective.

At the end of the pilot phase, the park rangers, commanders, and the research team will take full advantage of the technological platform that makes their jobs easier, advances their mission, and cuts costs for the Kenya Wildlife Service (KWS). This will provide an opportunity for the KWS and other partners to scale and replicate the system in Ngulia and other parks, and ultimately apply this low-cost coordinated approach to all manner of border-related threats at the national borders. Other law and security organizations in the region and beyond will be able to scale and replicate the model and technological system to benefit their top-priority considerations – from wildlife crime to counterterrorism and the spread of WMD.

Identifying Shared Value

The following benefits have been identified for each sector that is actively or indirectly involved in the project:

- ***The Kenyan government*** is the partner in implementing programs and technology (to which it otherwise would not have access) to help achieve national wildlife preservation, national security, and regional development priorities. Throughout this project a wide range of knowledge is being transferred, including a better understanding of technology and service specifications to solve problems in a cost-effective manner.
- ***Donor governments*** are leveraging limited resources, skills, and technologies, and finding shared value with the private sector. Particularly important is that development-focused government agencies have gained access to companies and technology that traditionally operate in the defense and security arenas. Defense- and security-related actors interact with organizations outside their immediate areas of interest, driving innovation and new business models against a broader range of issues that span the security/development divide in emerging economies.
- ***Multilateral organizations*** from the United Nations to the World Bank are offered a replicable case study on how to build cross-sectorial capacity building in emerging and developing regions that can be scaled and replicated to benefit a wider range of security and development initiatives.

Stimson has successfully been able to incubate cost-sharing by bringing together organizations in the public and private sector that otherwise would not have been cooperating on border and security capacity building.

• ***High technology and telecommunications sector players*** showcase their wares in a real-world environment, demonstrating their effectiveness to new markets and building market opportunities across a wider customer base. Participating firms educate their prospective customers about what products can help solve discrete challenges while also exercising pragmatic corporate social responsibility. In addition, the companies prove that their sectors and products can be partners with donor countries that are executing capacity-building projects in other regions across the security and development continuum. Finally, the pilot project is a launching platform from which to participate in larger capacity-building projects where a more traditional business model is in place.

This pilot venture indicates that Stimson has successfully been able to incubate cost-sharing by bringing together organizations in the public and private sector that otherwise would not have been cooperating on border and security capacity building. In short, organizations that did not know they had a role to play in national and regional security in East Africa are now working together from a public policy point of view while identifying durable new business opportunities. This model is eminently replicable to the national borders of Kenya to better identify and disrupt all manners of illicit trafficking, including in proliferation-sensitive items.

Case Study 2: Nuclear Power – Building the Benefits of Voluntary Consensus Standards

In 2014, Stimson launched a second pilot effort to apply the Accelerator concept to the field of nonproliferation. Here again, Stimson sought to identify risks and existing "market failures," then identify potential customers who could be serviced through an ongoing mechanism that would yield both long-term security value and nearer-term profit or risk mitigation.

The risks associated with the proliferation of civilian nuclear power are significant. Nuclear power has garnered increased interest internationally as a way to meet growing baseload energy demands while limiting greenhouse gas emissions.

With the global population expected to reach 8.5 billion in 2030, demand for energy is growing rapidly.[40] Astonishingly, and according to the World Nuclear Association, electricity demand is increasing twice as fast as overall energy use.[41] Developed and rising middle-income countries are increasingly looking to nuclear energy as an ideal source of clean, affordable energy production to meet their growing energy needs.

Nuclear energy facilities hold many advantages over other methods of electricity supply. Coal and natural gas have high fuel costs and contribute to air pollution; wind and solar energy, while they have low carbon emissions, cannot produce sufficiently high levels of energy to meet global energy needs. In contrast, nuclear energy production does not produce greenhouse gases, has stable fuel costs, and can generate large amounts of electricity required to meet the growing demand. Developing countries, with quickly growing middle classes and increasing energy demands, need the large-scale stability and cost-effective energy production that nuclear power plants can provide.

This international increase in nuclear power demand is expected to reach across countries, including those with limited or no experience in the nuclear field. While the extension of civilian nuclear power will have doubtless benefit to global development objectives, these realities pose potentially significant new security challenges as technologies and materials are introduced to regions with little experience in stringent nuclear security standards development and enforcement. Furthermore, as the Nuclear Security Summits draw to a close and US leadership on, and investment in, international nuclear security likely declines both in real terms and as a percentage of civilian power operations, the nonproliferation community is being forced to identify ways to sustain interest and investment in nuclear security.

While the extension of civilian nuclear power will have doubtless benefit to global development objectives, these realities pose potentially significant new security challenges as technologies and materials are introduced to regions with little experience in stringent nuclear security standards development and enforcement.

In 2014, in an attempt to operationalize the Accelerator concept, Stimson launched a new effort that considered how to incentivize a sustainable model for building nuclear security in new nuclear power countries. The objective was to provide a solution that not only was cost-neutral to governments, but could be reinforced by the private marketplace. Moreover, where possible, the objective was to circumvent insufficient regulatory authority or enforcement by appealing to nuclear power operators' vested interests, irrespective of their legal obligations.

Stimson undertook research and extensive discussions with multiple stakeholders to uncover where agreement could be reached on risk areas of concern to industry stakeholders that intersected with governments' interest in improving nuclear security to reduce the likelihood of sabotage or diversion of materials, technology, or knowledge. Based on concepts and contacts developed from earlier efforts, Stimson conducted extensive interviews to identify stakeholder interests and educate stakeholders to the possibility of a positive return on a security investment. This alignment of interests was the first step in galvanizing industry and government into a mutually beneficial partnership.

A Stimson publication in January 2016, *Nuclear Energy: Securing the Future, A Case for Voluntary Consensus Standards*, highlighted the overlapping areas of concern to industry and governments. Areas of mutual concern ranged from cybersecurity to export controls to human reliability issues. These were all areas where agreed good standards of performance had both real security dividends for government as well as the potential to reduce the likelihood, frequency, or magnitude of losses for corporations and power operators.[42] In sum, the customer base was being built through the identification of shared value.

Identifying Shared Value

The customers were thought initially to be the insurance industry, including insurers, reinsurers, and brokers who were rightly concerned over potential losses in new nuclear countries as a result of insufficient security enforcement at facilities. Their concerns, however, turned out to be broader than anticipated, and extended not only to new entrants in the nuclear field but to existing nuclear power countries, where security risks are deemed higher than previously recognized. Nonetheless, Stimson found that industry's ability to be a lead change agent in effecting better practices was constrained

Standards – developed by multiple stakeholders working together – would ultimately give greater clarity to how much security is enough, and what that security in and around a facility should look like.

by limited resources to invest in the proactive assessment of risks in this insular market (with fewer than 450 currently operational reactors), and singularly imposing controls. Cooperative discussions with private industry led to the conclusion that insurance and reinsurance incentives would be too narrow to capture the totality of the nuclear security challenge. Because the insurance that underwrites the operation of nuclear facilities is a massive globalized industry, elevated standards introduced by one actor, or even one consortium of actors, would invariably provide competitive pricing advantages to competitors. What was clear, however, was that insurance firms could be important partners in the creation and development of industrywide standards. Because such standards could be enforced by the market and would ultimately help mitigate risk to their business, the industry has been eager to support the concept.

Unlike the insurance industry, financiers became even more important than initially anticipated. For example, export credit agencies (ECAs) of nuclear power plant exporting countries hold great sway because new-build costs are so high and ECAs provide valuable long-term financing. A few basis points on a loan and a loan performance requirement can drive better operator behavior to the direct benefit of all involved. Leveraging this market mechanism based upon industry-agreed standards has the potential to ensure far more rigorous compliance to elevated security standards than traditional regulatory efforts, precisely because such standards are in the direct business interests of power facilities.

Regulators also support voluntary consensus standards because meeting them demonstrates compliance and provides assurances that can save regulators some additional oversight.

The above benefits all get translated to owners, whether public or private, as well as to facility operators. Each of these constituencies wants efficient, safe, secure, high-performing operations, but the challenges of making tradeoffs in the face of limited resources is daunting. Standards – developed by multiple stakeholders working together – would ultimately give greater clarity to how much security is enough, and what that security in and around a facility should look like. Third-party verification for that standards compliance would translate into benefits from insurers, financiers, regulators, and facility operations, and benefits to governments. In this case, the shared value is risk mitigation and enhanced nonproliferation and nuclear security.

Developing an Operational Plan

Moving beyond wider stakeholder engagement, Stimson identified an array of market prerequisites that must exist for such an incentivized nuclear security effort to germinate and succeed. These include:

- Risks must be identified that are of sufficiently high concern to multiple stakeholder groups, including operators.
- An agreed-to set of reasonable and quantifiable nuclear security standards must be developed.
- These standards must be verifiable against quantifiable metrics.
- Those providing market benefits must agree to recognize the standards and the process for verification, and to provide concomitant benefits to those who are found to be in compliance.

- Operators must consider the benefits to be sufficiently compelling to comply with these nonregulatory standards.
- A champion is needed to coordinate across stakeholders, and the International Atomic Energy Agency, although an important stakeholder, is not sufficiently agile to lead the effort.

Stimson found that the areas of risk on which multiple stakeholders – "the customers" – would be willing to consider working together in order to reduce overall risks and possible future expenses include: cybersecurity, integrated safety and security culture, human factors such as insider threats, supply chain/contracting security, export controls, and small reactor security. Stimson also found that existing standards have not been well developed, much less operationalized by the market.

How the standards would be developed would depend on the champion for the effort, which is still being identified. One logical potential leader is the World Institute for Nuclear Security (WINS), along with international NGOs whose missions include professional development and certification for nuclear security management. The next step is to develop the appropriate champions. Perhaps the most logical stakeholders to provide meaningful incentives are those with the most vested interests: the countries borrowing and lending funds for nuclear power developments (i.e., the ECAs of nuclear power vendor states). Many of these states are represented in the Organisation for Economic Cooperation and Development (OECD), and coordination could be pursued through the OECD's Nuclear Energy Agency. In addition, the borrowing states are well represented in the International Framework for Nuclear Energy Cooperation. These entities along with the insurers are those with vested financial interests. Additional stakeholder entities representing the public interest include the regulators, NGOs, and intergovernmental organizations like the International Atomic Energy Agency.

The group likely to make money from the operations of voluntary consensus standards would be the standards groups and certification entities. Standards development organizations like the ISO, American Society of Mechanical Engineers (ASME), and ASIS typically make money not from developing the standards, but from selling their standards, training to those standards, and in some cases providing certifications. Certifiers may be independent auditors or organizations, such as Bureau Veritas and Lloyds Register, which may or may not be the developer.

Recently, Bureau Veritas has been trying to develop a nuclear supply-chain standard based on an ISO standard that it is making available for free. It would make money on the auditing function. Lloyds Register has been engaged to develop standards for the new Chinese floating reactors, but it is unclear whether Lloyds Register would also be verifying compliance.

Next Steps

Stimson is working to engage with a likely champion or group of stakeholders who will agree to formally survey areas of risk where certification schemes could provide benefits. These are likely to include an integrated safety-security culture standard, a cybersecurity standard, and an export-compliance standard. Once these are surveyed, the best mechanisms for promoting such certifications development must be evaluated, via standards-development organizations or other ad hoc groups.

For example, for a safety-security integrated standard, an NGO such as WINS could participate in the standards development and auditor certification requirements, or could take a carried interest in their development – which might be outsourced to a third party via a public request for information or expression of interest. WINS could then develop or help develop the standard. It could earn income from selling copies of the standards but also, and more importantly, from training the plant auditors who

would provide the certifications. Such training would match well with WINS's work in training individuals in nuclear security. Essentially, WINS would be determining whether its training translated into performance at the plant operating level.

By leveraging the force of the market itself, this initiative promises to deliver a potent new rationale for the nuclear industry to engage more robustly in building a nuclear security culture across operations – not on the basis of legal or regulatory obligation, but rather in the interests of profitability.

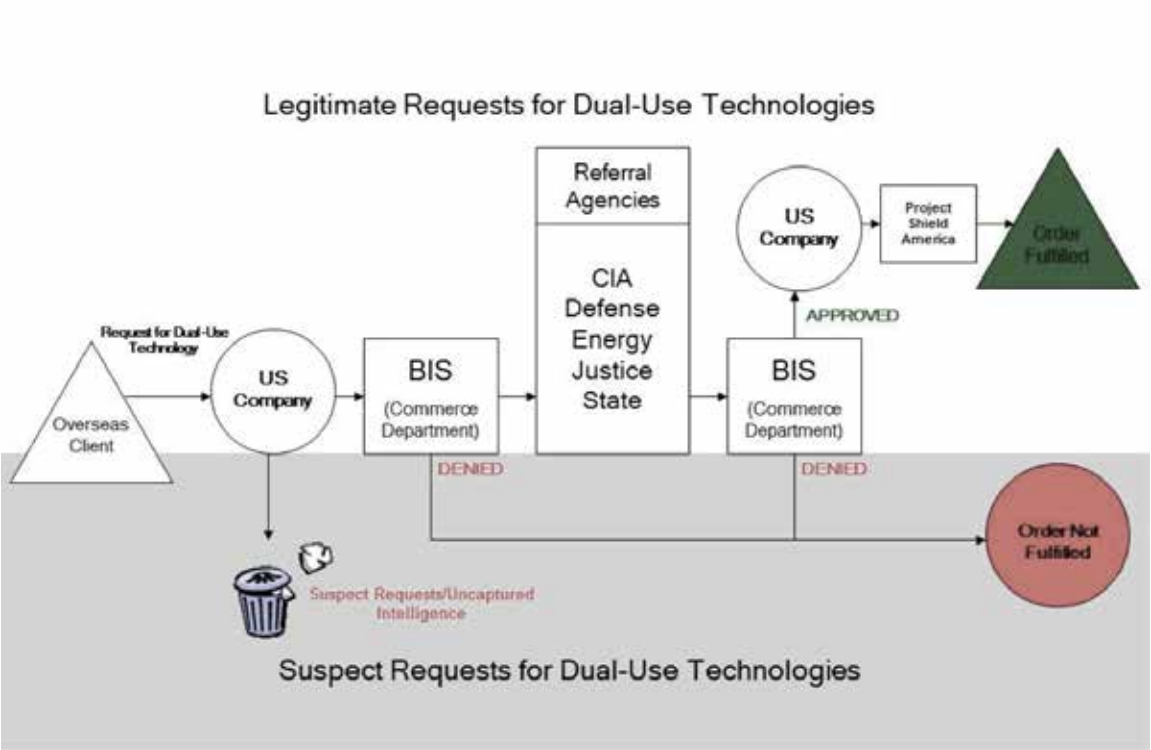
Case Study 3: The Black Box/Trash Can – Leveraging Lost Information for Mutual Benefit

Industry is central to the design, manufacture, transport, and sale of dual-use weapons-usable goods and technologies. Thus, information derived from these industrial transactions is inherently more accurate and timely than any other source of information related to proliferation intent, including government intelligence. Illicit requests for technologies, or strategies for their diversion, almost always originate with the private sector. Thus the connection between industry and the global supply chain gives technology firms and supply-chain companies an unrivaled ability to make judgments that can further government nonproliferation objectives, should they so choose.

Historically, companies manufacturing dual-use technologies have been subject to government regulations that dictate requirements to legally and legitimately export dual-use goods in the global marketplace. Individual companies' general due-diligence measures require significant resources to operate effectively within the bounds of government regulations, often leading to corporate complaints of financial burdens and unforeseen hardships. Here in the United States, these have included industry grievances over the stifling of innovation and the loss of market share to foreign competitors. These unintended side effects to proliferation prevention harm not only industry actors, but negatively impact the national economic interests. Thus the minimal necessary government regulation that engenders commitment to proliferation prevention is therefore ideal for industry exporters and governments alike.

Today, the export control process works as follows: When a United States exporter receives a purchase inquiry for a dual-use item, the company must verify the legitimacy of the actor. If the request is found inappropriate, it is discarded. If a prospective client is cleared through internal due diligence, or if red flags are raised during the review but suspicions are inconclusive, the exporter can submit an export request to the Department of Commerce Bureau of Industry and Security (BIS), which will, in turn, either deny the request or pass it on to the relevant government agencies and intelligence bodies for review, approval, or denial (see Figure E).

FIGURE E



While often cumbersome, the process is central to ensuring that sensitive items do not fall into the hands of would-be proliferators. Even as the US government works to enhance the efficiency of the export control process, current efforts and foreseeable improvements fail to capture a swath of prospective intelligence that could be gathered. If a company receives a suspicious inquiry from an overseas entity and determines not to pursue an export license, that information could be helpful to the intelligence community in identifying and ultimately disrupting proliferation networks. Yet the reporting of suspicious inquiries to government is entirely voluntary. A company, if it sees red flags in the course of due-diligence procedure, may simply decide to discard the request without submitting any information about the actor to BIS or other relevant agencies. This means that potential intelligence on proliferation networks is being summarily collected and discarded by private industry without ever being seen by government.

Additionally, government regulatory processes for dual-use technology occasionally hinder industry's ability to conduct business effectively and efficiently, as a result of the nature of bureaucracy itself. When industry chooses to report a suspect inquiry to BIS, the request must be transferred back and forth between agencies, where independent investigations into the purchaser's bona fides must be completed before BIS can deliver a verdict to the exporter. It is only after the full, time-consuming process has been completed and an approval has been issued that the company can start its additional export compliance procedures for the dual-use goods. While the process is essential to ensuring national security, it strains government resources and often unduly delays legitimate transactions. This, too, is neither in the interests of industry nor of the wider government.

One way in which industry can convince government to refrain from overly onerous regulation is to self-regulate beyond the strict mandates of existing regulations, adhering not only to the letter of the law but to the spirit of the regulations themselves.

In sum, multiple cross-cutting impediments have inhibited more effective information sharing between industry and government in this critical space. The industry resources to undertake due diligence and wait for government review of inquiries are finite. In addition, there are financial and legal barriers to the voluntary reporting of suspicious requests. Companies do not want to be held liable in the event that a government classifies an end user of dual-use materials as a proliferator, which may dissuade them from reporting suspicious inquiries to the Department of Commerce. Finally, many smaller companies may have difficulty completing rigorous due diligence, and may not want to risk inciting a costly and time-consuming "audit" by government regulators.

Identifying Shared Value

One way in which industry can convince government to refrain from overly onerous regulation is to self-regulate beyond the strict mandates of existing regulations, adhering not only to the letter of the law but to the spirit of the regulations themselves. Ideally, the full spectrum of companies that manufacture dual-use technologies would adopt rigorous self-regulation in pursuit of nonproliferation goals by inculcating a culture of cooperation over compliance. Yet a single company on its own would not likely make a substantial impact, would incur additional costs, and would likely lose market share to less responsible competitors who can move more quickly to service foreign requests. On the other hand, widespread industry cooperation in export control would benefit the industry as a whole ***and*** benefit companies individually.

Governments and industry inherently find shared value in the prevention of dual-use technology proliferation, yet they fail to work together to a sufficient degree to systematically address this problem. Though governments may have intelligence regarding confirmed proliferators, only some of it is publicly available, and intelligence organizations are rightly unwilling to share classified data with private firms.[43] Thus the onus for due-diligence, "know your customer" evaluations rests with companies themselves – only some of which have established rigorous internal compliance programs in order to meet state licensing requirements for exporting dual-use goods abroad. With these programs in place, suspicious inquiries are screened by a company's purchase-request review process, and the vast majority of them may never be catalogued or investigated by the government. Security experts have posited that this trove of unclaimed intelligence on suspected bad actors could yield direct benefits to government in identifying and disabling proliferation networks, but relatively little attention has been paid to the market upsides for industry to make the requisite investments in such an information-sharing approach.

Solution: Industry Self-Regulation and Information Sharing

While governments set regulations and penalties, industry is the first line of defense for screening export requests for potential dual-use materials. Industry may refrain from exporting products to a suspected bad actor, but will rarely share that information with the government due to distrust of the government's speed and process for screening export requests and a lack of clarity around the consequences of reporting, as well as proprietary and confidentiality concerns. As noted, this information

about a suspected bad actor, potentially including actionable intelligence, often gets discarded. Though many industry exporters have created robust due-diligence programs to evaluate the legitimacy of dual-use inquiries, these efforts are often duplicative. Because many purchasers of dual-use materials send inquiries to several companies in the industry rather than to only one, all the companies who receive the order are completing similar request reviews and searching for the same red-flag warnings as their competitors, leading to sectorwide inefficiencies. Much like the government agencies who investigate the same bad actors without communicating information, dual-use exporters waste time and resources replicating each other's "know your customer" efforts. Sharing such information in an amicable and blinded way would allow for burden-sharing of due-diligence investigations and would streamline reviews for all participating companies.

It is now possible for companies producing dual-use technology to design, implement, and maintain a new technology platform capable of receiving suspect inquiries from a wide spectrum of private internal compliance programs and nongovernmental actors.

Even after the individual exporter's investigations are completed, the intelligence collected during the inquiry "background check" is wasted. The request, along with any suspicious or flagged information collected by the company, is often discarded, rather than transferred to the relevant governmental organization or with other industry actors who may find it useful. Stimson proposes, as others also have suggested, that it may be possible for such information to be catalogued and analyzed by industry in order to alleviate the risks of regulatory noncompliance and the financial burdens of the necessary due diligence involved in ensuring proper export licensing.

The emergence of big data capabilities holds particular promise in overcoming the challenge of creating an industrywide information-sharing mechanism. It is now possible for companies producing dual-use technology to design, implement, and maintain a new technology platform capable of receiving suspect inquiries from a wide spectrum of private internal compliance programs and nongovernmental actors. The collected data would be aggregated into a database that could be accessed by participating companies to help mitigate the risk of proliferation and to promote efficiencies in the export control process. Over time, and with a multitude of companies contributing information on suspect inquiries, this database would become richer with insights that would not only alleviate the expensive burden of due-diligence practices, but could help draw regulators into a partnership with industry with the goal of jointly disrupting illicit proliferation networks with the newly enhanced intelligence tapestry.

Equipping private industry with enhanced data analytics and other tools to tap into potentially illicit procurement networks will have the dual benefit of promoting business efficiencies while enhancing security through better identification of suspect actors and activities. Stimson proposes the creation of a "Black Box" or a wiki due diligence directory in order to allow companies selling dual-use products to become instrumental partners in identifying and disabling global proliferation networks. The risk-management analytical tool would take the form of a catalog or directory capable of holding and displaying relevant export information to private industry regarding suspect inquiries for proliferation-relevant goods and technologies.

The format of the data collected, whether text, numerical values, ranking metrics, or something else, would be at the purview of the participating companies. Information from the directory would be accessible to member or subscriber firms, and the storage of relevant information would likely require either physical servers or cloud-based storage. Necessary security measures such as encryption, secure login, and data-storage security would also be determined by the industry and technology partners.

Proper control of a data directory requires effective management in a clearly defined structure. Processes should be established to determine access controls for relevant sensitive information, and ownership of material must be specified. In addition, the organization governing the directory must have an established liability agreement in order to protect itself and participant companies from litigation.

The subject matter of the Black Box should reflect a variety of nonproliferation risks and realities. The macro-level design of the wiki should be tailored to the specific format of most companies' general due-diligence measures, and red flag warnings from BIS should be incorporated in order to accurately reflect the suspicions raised during the inquiry review. Of course, micro-level risk assessments should also be incorporated.

Although the initial research indicates that data will be only shared between one group of companies, companies from across the value chain of the industry may participate, and the data tool must be able to absorb, categorize, and interpret different kinds of information that could be acquired throughout the "know your customer" investigations of participant companies. Data should therefore be refined into a uniform output format for maximum impact across the supply chain.

Benefits to Industry

Perhaps the most obvious benefit to sharing information on suspect actors in dual-use technology acquisition is the potential for disrupting global proliferation networks. Companies would be able to not only depend on their own internal due-diligence programs, but also use the data tool to compare their findings with the results of other companies' general due-diligence measures, facilitating a more rapid identification of likely proliferators. Potential for intelligence sharing with government using such an industry-controlled tool could enhance domestic and international efforts to combat weapons proliferation and ensure a safer, more peaceful world.

Corporations that sell dual-use technology are held responsible by their governments if that technology knowingly falls into the hands of bad actors/proliferators. This can and will impact bottom lines, reputations, and licensing. These are costly blunders to reverse, and as such, prevention through comprehensive due diligence is both required and perfunctory.

Sharing information with each other and with government would also enable private companies to save substantial time, and therefore money, in their own due-diligence efforts. The opportunity to leverage information that both government and industry independently receive to maximize profit and security is currently underutilized. While the time and money required for proper due diligence is well spent, information-sharing platforms would allow individual corporations to pool their knowledge bases. These would likely lead to reduced costs for companies and much faster and more efficient ways to conduct searches for possible bad actors.

In addition to cutting costs and the likelihood of proliferation, the government could grant additional incentives to companies that are willing to share information. This could take many forms, including labeling

these companies as trusted traders, which could ease licensing restrictions or provide green lanes for imports and exports, making it easier to do business overseas. Companies could additionally be seen as responsible global citizens, which could provide rhetorical market advantage among socially responsible clientele.

Benefits to Government

From the perspective of the government, the information acquired from the Black Box could have significant national security implications at what amounts to very little cost for government regulators and those in the intelligence community. Labeling a company as a trusted trader, as well as streamlining the process for licensing, is a low-cost, high-yield strategy. At first, this may only be implemented on a company-by-company basis, but over time it could grow into an industry standard.

Challenges

Some challenges to the implementation of this process are obvious, while others are legally, financially, and technically nuanced. The first is the structure or management of this process. Who would be in charge? A third-party information aggregator must have as little interference in the process as possible. Nor should it have an immediate political or financial stake. An unbiased third party – such as an industry association – would thus be ideal, supplemented by extensive protocols regarding how, with whom, and what levels of participants (in either private industry or government) have access to the service.[44] This third-party aggregator could monetize the Black Box through a subscription-based service that would allow industry to share and access the database for a fee – capitalizing the service while reducing due-diligence costs on the part of the client.

Another challenge arises from the standard of care or accuracy, which, if proven false, would cause a myriad of problems both for industry and government. A mechanism for quality control is thus required, as information dumps would take a great deal of time and resources to sift through. Service operators must also be wary of misinformation, which could lead to dead-end investigations and hurt both these industries and potential clients, and waste valuable government resources.[45]

Profiling potential clients may also give rise to both false positives and negatives, through which the service may blacklist legitimate buyers or, more alarmingly, sell products to illicit buyers despite an extensive vetting process. Varying strengths among companies' vetting processes is also concerning. Even in a highly regulated industry, there could still be a great deal of fluctuation regarding research performed on potential clients and adherence to industry standards.

In summary, such a market-based information collection mechanism would not be a panacea for addressing the threats posed by would-be proliferators; however, operating in conjunction with the existing export control regime, such a system could, over time, help to better streamline limited government investigatory resources by identifying and regularly auditing those companies who are willing to adopt a more rigorous export standard and information-sharing practice. Supported by market value, such a plan could yield significant new public-private cooperation in the field of nonproliferation.

Conclusion

Threats to global peace and prosperity are more diverse and confounding now than at any other time in human history. The nature of threats that are interconnected and no longer respect traditional boundaries not only present immediate risks, they erode the tenets of the social contract, threatening prospects

for a peaceful and prosperous future. No public authorities or private entities operating in isolation can hope to bend the curve of history away from the transnational conflict and violence, deficient governance, religious and ethnic hostility, criminality, poverty, environmental degradation, resource depletion, and proliferation of technology that consort to threaten modern society. Meeting these transnational threats necessitates both a global reassessment of common objectives, and the implementation of pragmatic instruments of national policy and private-sector partnerships.

The security community has been delinquent in modernizing our nonproliferation efforts to keep pace with 21st-century commerce. The products generated by this "Accelerator" would not, of course, be a panacea for the proliferation threat. Stringent regulations by governments for the private sector will remain a critical element of a global prevention strategy. Yet, we find that we have systematically underexploited the use of positive market-based incentives to modify industry behavior.

Stimson Staff

Brian Finlay is the President and CEO at Stimson. 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 initiative focused on counterterrorism issues, a 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 Chairs the Board of Directors of iMMAP, an information management and data analytics organization focused on improving humanitarian relief and development coordination. He also serves on the Advisory Board of Black Market Watch, a Geneva-based NGO that works to raise awareness around illicit global trade. Finlay also sits on the Editorial Board of Global Security, a journal of health, science and policy published by Routledge, Taylor & Francis. Finlay has authored and co-authored numerous books, monographs and reports, and is widely published in academic and policy journals and magazines. He is frequently asked to provide expert analysis and commentary on transnational and development challenges to media outlets around the world. Finlay holds an M.A. from the Norman Patterson School of International Affairs at Carleton University, a graduate diploma from the School of Advanced International Studies, the Johns Hopkins University and an honors B.A. from the University of Western Ontario.

About the Stimson Center

Founded in 1989, Stimson is a nonprofit, nonpartisan "impact" tank that addresses transnational threats and seeks creative opportunities 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 nonpartisan, actionable, and effective.

Endnotes

1. United Nations Security Council, "Report of the Secretary-General on Illicit Cross-Border Trafficking and Movement," S/2012/777, October 19, 2012, http://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/s_2012_777.pdf.

2. United Nations Office on Drugs and Crime, "Estimating Illicit Financial Flows Resulting from Drug Trafficking and Other Transnational Organized Crimes," October 2011, https://www.unodc.org/documents/data-and-analysis/Studies/Illicit_financial_flows_2011_web.pdf.

3. Millennium Project: Global Futures Studies and Research, "Global Challenges Facing Humanity," 2011, http://www.millennium-project.org/millennium/Global_Challenges/chall-12.html.

4. Global Initiative Against Transnational Organized Crime, "Cybercrime and the Private Sector," http://www.globalinitiative.net/programs/cybercrime/cybercrime-and-the-private-sector/.

5. See, for instance, Louis Charbonneau and Michelle Nichols, "Sanctioned North Korean Shipping Firm Still Active, Renamed Ships – UN Panel," Reuters, February 25, 2015, http://www.reuters.com/article/us-northkorea-sanctions-un-idUSKBN0LT2EA20150225, or David Albright and Andrea Stricker, "Canada Prosecutes Company for Possible Nuclear Related Export to Iran," Institute for Science and International Security, April 24, 2014, http://www.isisnuclariran.org/assets/pdf/Canada_Prosecutes_Company_24Apr2014-final.pdf.

6. United Nations, "The Millennium Development Goals Report 2015," 2015, http://www.un.org/millenniumgoals/2015_MDG_Report/pdf/MDG%202015%20rev%20(July%201).pdf.

7. Elizabeth Frawley Bagley, "Remarks at Swearing-in Ceremony of Special Representative for Global Partnerships Bagley: Opening Our Doors to the Private Sector," US Department of State, June 18, 2009, http://www.state.gov/s/partnerships/releases/125074.htm.

8. Organisation for Economic Cooperation and Development, "Aid to Poor Countries Slips Further as Governments Tighten Budgets," April 3, 2013, http://www.oecd.org/newsroom/aidtopoorcountriesslipsfurtherasgovernmentstightenbudgets.htm.

9. World Bank, "World Development Report 2013: Jobs," 2012, http://econ.worldbank.org/external/default/main?contentMDK=23044836&theSitePK=8258025&piPK=8258412&pagePK=8258258.

10. James Guseh, "The Public Sector, Privatization, and Development in Sub-Saharan Africa," ***African Studies Quarterly*** 5, no. 1 (2001), http://asq.africa.ufl.edu/files/Guseh-Vol-5-Issue-1.pdf.

11. Benjamin Snyder, "Nine Facts about Walmart That Will Surprise You," ***Fortune***, June 6, 2015, http://fortune.com/2015/06/06/walmart-facts/.

12. MarketsandMarkets, "Critical Infrastructure Protection Market by Security Technology (Network, Physical, RADARS, CBRNE, Vehicle Identification, Secure Communication, SCADA, Building Management) by Service, by Vertical, by Region - Global Forecast to 2019," March 2015, http://www.marketsandmarkets.com/PressReleases/critical-infrastructure-protection-cip.asp.

13. Richard Dobbs, et al., "Infrastructure Productivity: How to Save $1 Trillion a Year," McKinsey Global Institute, January 2013, http://www.mckinsey.com/insights/engineering_construction/infrastructure_productivity.

14. Henry C. Dethloff, ***Suddenly, Tomorrow Came: The NASA History of the Johnson Space Center*** (Washington DC: Dover Publications, 2012), 137.

15. NASA Office of the Chief Technologist, "Emerging Space: The Evolving Landscape of 21st Century American Spaceflight," 2014, http://www.nasa.gov/sites/default/files/files/Emerging_Space_Report.pdf; Partnership for Public Service, "Linking NASA and the Private Sector to Further Space Exploration," ***Washington Post***, January 22, 2015, https://www.washingtonpost.com/politics/federal_government/linking-nasa-and-the-private-sector-to-further-space-exploration/2015/01/22/d022b34e-a24b-11e4-9f89-561284a573f8_story.html.

16. US Green Building Council, "Why LEED," 2016, http://www.usgbc.org/leed/why-leed.

17. See MetroMile, "Insurance," 2015, https://www.metromile.com/insurance.

18. The White House Office of the Press Secretary, "Fact Sheet: Power Africa," June 30, 2013, https://www.whitehouse.gov/the-press-office/2013/06/30/fact-sheet-power-africa.

19. Brian Finlay, Elizabeth Turpen, and Frederick Kellett, "Manufacturing Possibility: Expanding Resources to Meet Global Challenges, Promote Economic Development, Support Innovation, and Prevent Proliferation," report no. 67, Henry L. Stimson Center, April 2008, http://www.stimson.org/books-reports/manufacturing-possibility/.

20. "Japanese Carbon Fiber Bound for Iran Seized: UN Report," ***Japan Times***, June 14, 2014, http://www.japantimes.co.jp/news/2014/06/14/national/japanese-carbon-fiber-bound-for-iran-seized-u-n-report/#.VZrkZRNViko.

21. Nuclear Threat Initiative, "Biological," Iran Country Profile, http://www.nti.org/country-profiles/iran/biological/.

22. Sibylle Bauer, "WMD Related Dual-Use Trade Control Offences in the European Union: Penalties and Prosecutions," ***EU Non-Proliferation Consortium Non-Proliferation Papers*** 30 (July 2013), http://www.sipri.org/research/disarmament/eu-consortium/publications/nonproliferation-paper-30; David Crawford, "Germany Charges

Two Over Iran Equipment Deal," ***Wall Street Journal***, April 8, 2010, http://www.wsj.com/articles/SB10001424052702303720604575169673566651884.

23. John Elworthy, "Cambridgeshire Company Boss Faces £68,000 Bill – Or Extra 15 Months in Jail – Following Illegal Exports to Iran Trial," ***Wisbech Standard***, November 22, 2014, http://www.wisbechstandard.co.uk/news/cambridgeshire_company_boss_faces_68_000_bill_or_extra_15_months_in_jail_following_illegal_exports_to_iran_trial_1_3858588.

24. David Sanger, "The Khan Network," paper presented at Conference on South Asia and the Nuclear Future, Stanford University, Palo Alto, California, June 4-5, 2004, http://iis-db.stanford.edu/evnts/3889/Khan_network-paper.pdf.

25. Georgetown University, "The Prosecution of Henk Slebos," Institute for Law, Science, and Global Security, https://lsgs.georgetown.edu/programs/nlp/slebos.

26. Bauer, "WMD Related Dual-Use Trade Control Offences in the European Union."

27. Barbara Vitello, "Owner of Schaumberg Company Sentenced to Federal Prison," ***Daily Herald***, May 15, 2015, http://www.dailyherald.com/article/20150514/news/150519211/.

28. The White House Office of the Press Secretary, "Presidential Memorandum – Expanding Public-Private Collaboration on Infrastructure Development and Financing," July 17, 2014, https://www.whitehouse.gov/the-press-office/2014/07/17/presidential-memorandum-expanding-public-private-collaboration-infrastru; see also UN Secretary General, "Public-Private Partnerships Hold Key to Advancing Inclusive, Sustainable Growth, Secretary-General Tells United Nations Forum on Industrial Development," July 2015, http://www.un.org/press/en/2015/sgsm16942.doc.htm; Warren Buffet, 2015 annual letter to Berkshire Hathaway shareholders, February 27, 2016, http://www.berkshirehathaway.com/letters/2015ltr.pdf.

29 See Nuclear Power Plant and Reactor Exporters' Principles of Conduct for one attempt to harmonize regulations and resolve safety and security threats from nuclear power plants, at http://nuclearprinciples.org/.

30. Barry Blechman and Jay Cohen, ***Partners in Prevention: Making Public-Private Security Cooperation More Efficient, Effective and Sustainable: Recommendations of the Task Force,*** Henry L. Stimson Center, May 2014, http://www.stimson.org/images/uploads/research-pdfs/Stimson_Partners_in_Prevention_Task_Force_Report_May_2014.pdf.

31. See Appendix A.

32. Martin Ravallion, Shaohua Chen, and Prem Sangraula, "Dollar a Day Revisited," World Bank Policy Research Working Paper Series no. 4620, May 1, 2008, available at Social Science Research Network, http://ssrn.com/abstract=1149123.

33. World Health Organization, "World Health Report, 2004: Changing History," May 4, 2004, http://www.who.int/whr/2004/media_centre/en/slides_en.pdf.

34. United Nations Office on Drugs and Crime, "Violence, Crime, and Illegal Arms Trafficking in Colombia," November 2006, http://www.unodc.org/pdf/Colombia_Dec06_en.pdf.

35. According to Chapter Seven of the UN Charter, the Security Council "shall determine the existence of any threat to the peace, breach of the peace, or act of aggression and shall make recommendations, or decide what measures shall be taken … to maintain or restore international peace and security." Shortly following the terrorist attacks on September 11, 2001, the UN Security Council passed Resolution 1373, requiring all UN member states to take steps to combat terrorism. The passage of Resolution 1373 marked the first time since the Security Council was formed in 1945 that it invoked its Chapter Seven authority to legislate a functional, rather than state-specific, threat to international peace and security. The passage of UN Security Council Resolution 1540 represented only the second time the council had taken this extraordinary action. (Department of Public Information, Charter of the United Nations, San Francisco, CA, 1985.)

36. Brian Finlay, Johan Bergenas, and Esha Mufti, ***Beyond Boundaries in the Andean Region: Bridging the Security/Development Divide with International Security Assistance***, Stanley Foundation, 2011, http://www.stimson.org/images/uploads/BB_Andean_Rpt_.pdf; Brian Finlay, Johan Bergenas, and Veronica Tessler, ***Beyond Boundaries in Eastern Africa: Bridging the Security/Development Divide with International Security Assistance,*** Stanley Foundation, 2011, http://www.stimson.org/images/uploads/research-pdfs/EArptcover.pdf; Brian Finlay, Johan

Bergenas, and Esha Mufti, ***Beyond Boundaries in South Asia: Bridging the Security/ Development Divide with International Security Assistance,*** Stanley Foundation, 2011, http://www.stimson.org/images/uploads/research-pdfs/SArpt5121_1.pdf; Brian Finlay, Johan Bergenas, and Veronica Tessler. ***Beyond Boundaries in the Middle East: Leveraging Nonproliferation Assistance to Address Security/Development Needs with Resolution 1540,*** Henry L. Stimson Center and Stanley Foundation, 2010, http://www.stimson.org/images/uploads/research-pdfs/MErpt910.pdf; Brian Finlay, ***WMD, Drugs, and Criminal Gangs in Central America: Leveraging Nonproliferation Assistance to Address Security/Development Needs with UN Security Council Resolution 1540***, Stanley Foundation, 2010, http://www.stimson.org/images/uploads/research-pdfs/CArpt710_1.pdf; Brian Finlay and Elizabeth Turpen, ***The Next 100 Project: Leveraging National Security Assistance to Meet Developing World Needs***, Stanley Foundation, 2009, http://www.stimson.org/images/uploads/research-pdfs/Next100Report2009.pdf.

37. Government of the Republic of Kenya, "Kenya Vision 2030: Popular Version," 2007, http://www.vision2030.go.ke/wp-content/uploads/2015/12/Vision2030_Abridged%20(Popular%20Version).pdf.

38. Catrina Steward, "Illegal Ivory Trade Funds Al-Shabaab's Terrorist Attacks," ***The Independent***, October 5, 2013, http://www.independent.co.uk/news/world/africa/illegal-ivory-trade-funds-al-shabaabs-terrorist-attacks-8861315.html

39. See Project Ngulia, http://projectngulia.org/.

40. United Nations Department of Economic and Social Affairs, Population Division, ***World Population Prospects: The 2015 Revision, Key Findings and Advance Tables***, working paper no. ESA/P/WP.241, 2015, http://esa.un.org/unpd/wpp/publications/files/key_findings_wpp_2015.pdf.

41. World Nuclear Association, "World Energy Needs and Nuclear Power," December 2015, http://world-nuclear.org/information-library/current-and-future-generation/world-energy-needs-and-nuclear-power.aspx.

42. Debra Decker and Kathryn Rauhut, ***Nuclear Energy: Securing the Future, A Case for Voluntary Consensus Standards***, Henry L. Stimson Center, January 2016, http://www.stimson.org/sites/default/files/file-attachments/Nuclear-Energy-web-122315.pdf.

43. Export.gov, "Consolidated Screening List," http://export.gov/ecr/eg_main_023148.asp.; Bureau of Industry and Security, "Lists of Parties of Concern," https://www.bis.doc.gov/index.php/policy-guidance/lists-of-parties-of-concern; Bureau of Industry and Security, "Denied Persons List," https://www.bis.doc.gov/index.php/policy-guidance/lists-of-parties-of-concern/denied-persons-list; US Department of State, A Resource on Strategic Trade Management and Export Controls, "Red Flags and Watch Lists," 2011, http://www.state.gov/strategictrade/redflags/.

44. Daniel Salisbury, "How the Private Sector Can Do More to Prevent Illicit Trade," Arms Control Association, July 2013, http://www.armscontrol.org/act/2013_0708/How-the-Private-Sector-Can-Do-More-to-Prevent-Illicit-Trade.

45. F. A. Morris, A. J. Kurzok, and A. M. Seward, ***A Nonproliferation Third Party for Dual-Use Industries – Legal Issues for Consideration***, US Department of Energy, PNNL-21908, October 2012.

PUBLIC THREATS, PRIVATE SOLUTIONS

Meeting Nonproliferation Challenges with the Force of the Market

From the standpoint of security, globalization has made the world a far less safe and predicable place. Yet the forces that have driven the darker side of globalization have also yielded heretofore unimagined technological, economic, and development opportunities to citizens in virtually every corner of the globe. It has also opened up new avenues to better integrate private industry as a force for global good.

Governments around the world have long struggled with the spread of weapons of mass destruction and the proliferation of related technologies. This report takes a bold approach to better aligning governments' interest in ensuring nonproliferation with industry's imperative to build market value. By better defining "shared value," complementary and sustainable new approaches to proliferation prevention can and have been engendered. Three discrete case studies are presented. Each is eminently scalable and replicable at a global scale and has been demonstrated to be effective in the private marketplace. Each has the potential to help reshape government-industry relations for the betterment of global peace and prosperity.

STIMSON
www.stimson.org