

Journal of Homeland Security and Emergency Management

Volume 3, Issue 4

2006

Article 5

Marshalling the Great Arsenal of Democracy: Engaging the Private Sector to Secure the Public Good

Ian Siperco*

*London School of Economics and Political Science, I.Siperco@lse.ac.uk

Copyright ©2006 The Berkeley Electronic Press. All rights reserved.

Marshalling the Great Arsenal of Democracy: Engaging the Private Sector to Secure the Public Good

Ian Siperco

Abstract

More than sixty years have passed since Franklin Roosevelt forecast a victory over tyranny that could only be won with the unprecedented voluntary efforts of industry. Today the mobilization of the private sector under the banner of national defense is no longer guided by the rhetoric of mass production, but rather the emergence in the past five years of terrorism-related planning as a corporate governance issue. Whether it is possible to secure adequate private sector investment in best-practice continuity and resiliency strategies depends on the will of government to use the stick of regulation sparingly and the carrot of statutory incentives liberally.

KEYWORDS: terrorism, corporate governance, risk assessment, homeland security

INTRODUCTION

In December 1940, as the yoke of Nazi tyranny descended over Europe, President Franklin Delano Roosevelt delivered a fireside sermon intended to rouse the slumbering giant of American industry in preparation for war. Elaborating on a theme of “splendid cooperation” between the government and industry, Roosevelt stressed that it was not the American politician, but the American people who had the power to turn the tide of the war. Sixty years later the mobilization of industry under the banner of national defense is no longer guided by the rhetoric of mass production, but rather the emergence in the past five years of terrorism-related planning as a corporate governance issue.

The September 11th terrorist attacks in New York and Washington introduced a new dynamic into the logic of boardroom risk assessment methodologies. In the time it took for the tragedies of that day to register worldwide, security had gained unprecedented salience on the corporate agenda. Accordingly, the North American private sector - which exercises control over 85% of critical infrastructure¹ - undertook unprecedented good-faith initiatives to increase corporate threshold investments in voluntary security-related best practices to secure infrastructure from terrorist attack.²

To promote networked solutions for business continuity and resiliency in the wake of the attacks, many companies found that it was in their interest to support operational mutual-aid agreements with other industry partners. Today these initiatives have been expanded to include sector-specific coordinating mechanisms that facilitate sharing of information on physical and cyber threats, as well as vulnerabilities, incidents, recommended protective measures, and security-related best practices.³ Unfortunately, these developments have not sufficiently changed corporate security strategies. Plans have yet to go beyond the lip service paid to the benefits of a resilient security strategy and into the C-suite and boardroom. Security is simply not viewed as a core business function.⁴

¹ National critical infrastructure is made up of material assets that are essential for the functioning of a society and economy including, but not limited to, electricity generation and distribution, telecommunication, water supply, and transportation systems.

² The National Strategy for the Physical Protection of Critical Infrastructure and Key Assets, Office of Homeland Security, February 2003. Pg. xi

³ Department of Homeland Security. “National Infrastructure Protection Plan,” 2006, p. 19.

⁴ Robert Housman and Timothy Olson, “New Strategies to Protect America: A Market-Based Approach to Private Sector Security,” Center for American Progress, July 28, 2006.

COMPETITIVE DISADVANTAGE AND VOLUNTARY SECURITY PRACTICES

Industries, including commercial aviation and nuclear power, which feature regulatory or statutory frameworks that govern private sector security operations are consistently measured ahead of the curve in North American - and indeed global - security preparedness. By contrast, privately regulated sectors, including finance, communications, and energy, are guided by voluntary security regimes. This arrangement ensures that efforts to secure our critical infrastructure will be plagued by corporate aversion to counter-competitive policies and the increased liability exposure associated with voluntary security investment.⁵

Any company that includes security upgrades in the normal cycle of capital expenditures when industry competitors do not follow suit and the costs are not readily offset or recoverable in the form of reduced insurance premiums, for example, faces a potentially debilitating competitive disadvantage on the free market.⁶ Moreover, purely voluntary protective efforts can expose companies to claims that they were aware of their vulnerabilities, but were negligent in taking sufficient measures to address them. Without the blanket protection of sector-specific legislation, companies that make a good-faith effort to undertake antiterrorist measures risk open-ended liability issues should terrorists succeed at defeating those measures.⁷ Lacking the statutory implementation of liability safeguards, executives will thus increasingly face pressure to limit company efforts to acknowledge and address security concerns.⁸ At the same time, there are options available to government that can raise (or reduce) the threat and viability of such lawsuits. For example, the legislature can statutorily reduce the burden of proof on plaintiffs.⁹

GUIDANCE FOR COLLABORATION WITH THE PRIVATE SECTOR

Non-regulatory approaches should always be favored as a means of diffusing the impact of pervasive state controls that could overburden the private market economy. However, when voluntary efforts do not achieve adequate levels of security, lawmakers and regulators may need to take action. In any free market economy, governments unavoidably remain prominent players with regulatory

⁵ Stephen E. Flynn and Daniel B. Prieto, "Neglected Defense: Mobilizing the Private Sector to Support Homeland Security," Council on Foreign Relations, CSR No. 13, March 2006, p. 18.

⁶ Council on Foreign Relations, "Neglected Defense: Mobilizing the Private Sector to Support Homeland Security," p. 19

⁷ *Ibid.*, p. 27

⁸ *Ibid.*, p. 31.

⁹ Center for American Progress, "New Strategies to Protect America: A Market-Based Approach to Private Sector Security"

oversight capacity that can help to bound market uncertainties, making it easier for markets to work and for the private sector to make investment decisions. For example, by helping to establish and enforce uniform standards, the federal government can provide a predictable environment which will better allow companies to invest in security without fear that such efforts will be undercut by competitors that do not follow suit, or that investments will be rendered obsolete because the government later ends up standardizing a different set of technologies or practices.¹⁰

The issues surrounding the particular modes of speculative government intervention and private sector compulsion are somewhat involved and are set out more fully and formally elsewhere.¹¹ For the purposes of this paper, it is enough to only briefly review the three forms of intervention that can compel the private sector to adopt requisite security improvements. In the first instance, government can impose standards through laws and regulations, though this comes with a high potential cost of freezing innovation. Secondly, government can offset the costs of security improvements via direct subsidies (grants) or tax incentives targeted at high risk sectors. Because it is not practical or feasible to protect all assets, systems, and networks against every possible terrorist attack vector, this solution requires developing a hierarchy of security priorities for resource allocation based on sector business characteristics, risk landscape, protection authorities, requirements, and maturity.¹² For example, nuclear power plants have sophisticated security systems that are designed to protect against willful disruption by anticipating hostile action as well as accidental phenomena.¹³ Conversely, chemical facilities continue to suffer from serious deficiencies in facility security and basic vulnerability analyses despite having been universally assigned a high-risk designation by legislators.¹⁴ To address inconsistencies in the protective landscape, tax credits could be made available to companies that make investments to improve chemical security (for example), since voluntary investments by chemical manufacturers are acknowledged to be insufficient,¹⁵

¹⁰ Council on Foreign Relations, "Neglected Defense: Mobilizing the Private Sector to Support Homeland Security," p. 4

¹¹ Stephen E. Flynn and Daniel B. Prieto, "Neglected Defense: Mobilizing the Private Sector to Support Homeland Security," Council on Foreign Relations, CSR No. 13, March 2006

¹² Department of Homeland Security. "National Infrastructure Protection Plan," p. 11

¹³ In a study conducted by the Center for Strategic and International Studies, a prominent Beltway think tank, research supported the observation that while under very specific conditions it may be possible for a large (767-equivalent) aircraft to penetrate the pressure vessel, only a modest release of radiation would be expected and would trigger safe shutdown procedures. ("Silent Vector: Issues of Concern and Policy Recommendations," September 2003, p. 7)

¹⁴ *Ibid.*, p. 7

¹⁵ Council on Foreign Relations, "Neglected Defense: Mobilizing the Private Sector to Support Homeland Security," p. 38

while maintaining current levels of support for nuclear facilities and other industries already regulated by government.

In the final option for government intervention, the state might choose to establish market-based measures enabling companies to more efficiently allocate resources and correct market failures. Market-based measures offer greater flexibility and act as strong behavioral drivers that support innovation, while companies seek to meet mandates with a positive return on investment.¹⁶ For example, the application of disclosure requirements under existing securities laws would not require legislative action and could be done with little or no new federal dollars.¹⁷ Requiring disclosure would compel companies to treat homeland security matters not as non-revenue producing costs, but as core corporate matters.¹⁸ The problem with this solution lies with redefining homeland security matters as “material” in influencing a reasonable investor’s investment decisions with respect to a particular company (the standardized litmus test for compelling disclosure requirements). Expanding securities laws to redefine information sharing baselines would ensure market support for a new standard of security.

These advantages notwithstanding, market-based measures have their own limitations. Markets would require constant feedback, oversight, and management to ensure that they serve the ends desired. This task is made all the more onerous in a dynamic and unsettled bureaucratic landscape, where government agencies find it difficult to share anything but the most general threat information with private companies out of fear that it will be leaked or that intelligence sources and methods will be compromised.¹⁹

Lacking sufficient access to reliable threat information, companies find it difficult to make informed cost-benefit decisions that might justify greater security investments. This, in turn, deprives the market of an important transmission mechanism to convey signals that might compel companies to increase investments in security.²⁰ That said, in general, market-based measures present strong, flexible, and efficient solutions to a non-responsive private sector.

Given the severity of the consequences associated with many potential attack scenarios, one might naturally assume that a combination of these solutions today colors the logic of private sector security investment. Unfortunately, government has largely taken a hands-off approach to the private sector, relegating to itself the limited role of “protector of last resort” – a backstop only

¹⁶ Center for American Progress, “New Strategies to Protect America: A Market-Based Approach to Private Sector Security”

¹⁷ Ibid

¹⁸ Ibid

¹⁹ Council on Foreign Relations, “Neglected Defense: Mobilizing the Private Sector to Support Homeland Security,” p. 15

²⁰ Council on Foreign Relations, “Neglected Defense: Mobilizing the Private Sector to Support Homeland Security,” p. 16

for those areas that meet the criteria for heightened risk, taking into account threat perception, vulnerability analysis, and consequence management.²¹

INNOVATION AND INFORMATION SHARING

There exists an enduring legacy of an often-adversarial relationship between the private sector and government stemming from government's regulatory oversight and enforcement roles that is only now beginning to change.²² Though there has been no open call for the private sector to throw its weight behind the new governance architecture of homeland security initiatives, the intellectual resources of this new discipline have fuelled a wave of developments that may provide the framework for a new approach to public-private interface in matters of homeland security.

The uniquely American innovation of voluntary participation in Information Sharing and Analysis Centers (ISACs) provides one such example of an effective (and discreet) private sector mechanism for information exchange. These Centers typically serve as the tactical and operational arms for sector specific information, sharing efforts designed to facilitate the free exchange of information on vulnerability data and protection strategies.²³ For example, the Financial Services Information Sharing and Analysis Center (FS/ISAC) gathers threat, vulnerability, and risk information about cyber and physical security risks faced by the financial services sector. Sources of information include commercial companies that gather this type of information, government agencies, academics, and other trusted sources. After analysis by industry experts, alerts are delivered to participants containing a description of the threat or vulnerability, its severity, and recommendations for solutions.

Today ISAC's exist for fourteen critical infrastructures, including Financial Services, Electric, Energy and Surface Transportation. But given the demonstrated vulnerability of networked systems of infrastructure to disruption (see the August 2003 East coast power outage), final responsibility for assuring resiliency and continuity in all sectors of our critical infrastructure must rest with the federal government.

²¹ Ibid., p. 7

²² Ibid., p. 10

²³ Department of Homeland Security. "National Infrastructure Protection Plan," p. 63

CONCLUSION

The United States emerged from the Second World War having created the conditions for productive postwar collaboration between the federal government and private enterprise - the parties whose partnership laid the foundation for an American victory in the Cold War. Today we stand on the precipice of a new generational war with the horrors of unimagined dangers coloring a dark future should we falter. Where the frontlines of this war encroach upon our cities and our way of life, we must ensure the collaborative efforts of all stakeholders to minimize or manage risk. Within this diverse protective landscape, private sector entities can better secure the infrastructure under their control by adhering to recognized industry best business practices and standards and by entering into operational mutual-aid agreements with other industry partners.²⁴ In many industries, threat perceptions and conducive market conditions have resulted in adequate voluntary investments in security. For industries in which voluntary investment has been insufficient, government intervention is necessary and desirable.²⁵ In these instances, the state must be permitted the latitude to drive our national protection priorities and inform the resource allocation process.

Whether the motivation for structural reform lies with a system of public policy incentives (grants for investment in protection, government underwriting of insurance, etc.) or in the specter of enhanced government regulation following the next attack, the performance of preventive security measures in a “new threats” agenda will unquestionably condition either our victory or our defeat at the hands of international terrorists.

²⁴ Department of Homeland Security. “National Infrastructure Protection Plan,” p. 27

²⁵ Council on Foreign Relations, “Neglected Defense: Mobilizing the Private Sector to Support Homeland Security,” p. 3

REFERENCES

Center for Strategic and International Studies. 2003. *Silent Vector: Issues of Concern and Policy Recommendations*. Washington, DC: Center for Strategic and International Studies.

Flynn, S. and D. Pietro. 2006. *Neglected Defense: Mobilizing the Private Sector to Support Homeland Security*. CSR No. 13 (Washington, DC: Council on Foreign Relations).

Housman, R. and T. Olson. 2006. *New Strategies to Protect America: A Market-Based Approach to Private Sector Security*. Washington, DC: Center for American Progress.

U.S. Department of Homeland Security. 2006. *National Infrastructure Protection Plan (NIPP)*. Washington, DC.

U.S. Office of Homeland Security. 2003. *The National Strategy for the Physical Protection of Critical Infrastructure and Key Assets*. Washington, DC.