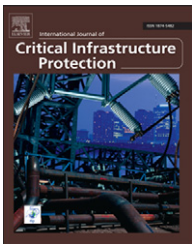
Available online at www.sciencedirect.com

SciVerse ScienceDirect

www.elsevier.com/locate/ijcip



Realizing the promise of public-private partnerships in U.S. critical infrastructure protection

*Austen D. Givens**, *Nathan E. Busch*

Department of Economic Crime and Justice Studies, Utica College, 1600 Burrstone Road, Utica, New York 13502, USA

ARTICLE INFO

Article history:
Received 5 July 2012
Received in revised form
22 February 2013
Accepted 22 February 2013
Available online 27 February 2013

Keywords:
Critical infrastructure protection
Public-private partnerships
Resilience
Effectiveness

ABSTRACT

To date, much attention has focused on the advantages of public-private partnerships for critical infrastructure protection in the United States. These include reducing the duplication of effort, enhancing cross-sector communication, increasing efficiency, and ultimately achieving the protection objectives better than government or business acting independently. The benefits suggest that public-private partnerships will be a significant and enduring part of critical infrastructure protection initiatives in the United States. However, we argue that a pattern is emerging that may lead to a fracture between the appearance and the reality of public-private partnerships in U.S. critical infrastructure protection. Although some research has focused on specific challenges in this domain of U.S. homeland security, comparatively little attention has been paid to thinking through the issues facing critical infrastructure protection as a whole. We maintain that unless concrete steps are taken to bolster public-private partnerships in critical infrastructure protection, they will be much less effective than hoped for by U.S. homeland security analysts.

1. Introduction

Since the terrorist attacks of September 11, 2001, great progress has been made in fostering public-private sector partnerships for U.S. critical infrastructure protection. These public-private partnerships—which we define as collaboration between a public sector (government) entity and a private sector (for-profit) entity to achieve a specific goal or set of objectives—have increasingly been incorporated into critical infrastructure protection initiatives at all levels of government, from the local through the federal (see, e.g., [1–7]). At the local level, grassroots organizations such as ChicagoFIRST (Financial Industry Resilience and Security through Teamwork) have been formed to enhance public-private emergency preparedness, evacuation planning, and credentialing in the Chicago-area financial sector [8]. The All Hazards Consortium, a non-governmental organization, has hosted numerous workshops and meetings on critical infrastructure protection to bring together government agencies and businesses at the state level [9]. Within the U.S. federal executive branch, new Department of Homeland Security (DHS) advisory groups such as the Critical Infrastructure Partnership Advisory Council (CIPAC) are made up of public sector and business representatives who meet regularly to exchange information of mutual interest [10].

Overarching these local, state, and federal-level initiatives, the White House embraces the private sector as an essential part of the United States National Security Strategy [11]. The National Security Strategy conceptually shapes how government and non-governmental organizations should work together to achieve security objectives; its scope transcends the local, state, and federal levels of government. And in two key areas of critical infrastructure—the operation of commercial facilities and energy production—recent disasters demonstrate the prominence of

*Corresponding author. Tel.: +1 315 557 6615; fax: +1 315 223 2456.
E-mail address: adgivens@utica.edu (A.D. Givens).

1874-5482/$ - see front matter © 2013 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.ijcip.2013.02.002

public-private partnerships. The responses to Hurricane Katrina and the Deepwater Horizon oil spill, for instance, required thousands of public and private sector employees to cooperate and coordinate their actions [12,13]. Thus, from the local level to the federal level, public-private partnerships are now an indispensable part of critical infrastructure protection.

Despite this progress, public-private partnerships related to U.S. critical infrastructure protection are now at an important crossroads. To date, much attention has focused on the advantages of public-private partnerships in critical infrastructure protection. These include reducing duplication of effort, enhancing public-private sector communication, increasing efficiency, and ultimately achieving objectives better than government or businesses acting independently [14–18]. The benefits suggest that public-private partnerships will be a significant and enduring part of critical infrastructure protection initiatives. However, we argue that a pattern is emerging that may lead to a fracture between the appearance and reality of public-private partnerships related to critical infrastructure protection. Although some research [19–21] has focused on specific challenges, comparatively little attention has been paid to thinking through the issues facing critical infrastructure protection as a whole. We maintain that, unless concrete steps are taken to bolster public-private partnerships in critical infrastructure protection, they will be much less effective than hoped for by homeland security analysts.

This article begins by briefly summarizing the evolution of critical infrastructure protection in the U.S. national security context since 1997—an evolution that we argue has come to emphasize public-private partnerships directly and prominently. The article proceeds to analyze four challenges to public-private partnerships in critical infrastructure protection—public-private sector coordination, information sharing, promoting private sector engagement, and cybersecurity—and argues that there is the potential for a gap between their apparent and actual success. The article also offers some recommendations and discusses the need for further research in the area.

2. Evolution of critical infrastructure protection

In 1997, U.S. government and private sector leaders took the first steps in changing the nation's approach to critical infrastructure protection. Prior to that time, the importance of critical infrastructure protection was recognized, but only for its commercial impact rather than national security implications. The Clinton administration first saw the need to re-examine the critical infrastructure in other contexts [22]. This led to the formation of the President's Commission on Critical Infrastructure Protection (PCCIP). By today's standards, the PCCIP's final report appears remarkably understated:

> [W]e have to think differently about infrastructure protection today and for the future....*We found that the nation is so dependent on our infrastructures that we must view them through a national security lens*....We also found the collective dependence on the information and communications infrastructure drives us to seek new understanding about the Information Age. Essentially, we recognize a very real and growing cyber dimension associated with infrastructure assurance [22].

The PCCIP membership also foreshadowed the proliferation of public-private partnerships in critical infrastructure protection; representatives from AT&T, IBM, the Association of American Railroads, and Pacific Gas and Electric Company all sat on the Commission alongside government representatives. Of course, in the fifteen years since the Commission's report, much has changed—in large part prompted by the terrorist attacks of September 11, 2001.

2.1. *Aftermath of 9/11*

The devastating attacks of September 11, 2001 reinforced the PCCIP's findings on the importance of the critical infrastructure to national security, profoundly underscoring the value of the PCCIP being composed of public and private sector officials. As Abou-Bakr [23] notes, 9/11 represented a catastrophic breach of national security that involved the use of private resources (commercial aircraft) in one critical infrastructure sector (transportation sector) to attack multiple public and private sector resources, including The World Trade Center, part of the commercial facilities and banking/finance sectors; Pentagon, part of the government facilities and defense industrial base sectors; and associated critical infrastructure components in lower Manhattan, including electricity and steam distribution systems, telecommunications equipment, and components of the New York City subway system. Thus, 9/11 highlighted the importance of critical infrastructure protection to confront threats to the public and private sectors, and it sparked a series of historic changes in government.

A new idea—U.S. homeland security—began to rapidly alter the organization of government and the national approach to critical infrastructure protection. Less than a month after 9/11 attacks, the White House created the Office of Homeland Security headed by former Pennsylvania Governor Tom Ridge [24]. In 2002, DHS was established [25]. This new cabinet-level department brought 22 disparate agencies together under one administrative umbrella. It represented an extraordinary realignment of public sector resources to confront natural and man-made threats to the United States. Among its new responsibilities, DHS became the lead federal agency for coordinating critical infrastructure protection activities [26]. However, as time passed, it became increasingly clear that the idea of "protection" itself needed to evolve. This gave rise to two important changes that continue to impact public-private partnerships in critical infrastructure protection today.

First, the idea of "protection" was transformed into an ethos of "resilience." This broad concept suggests a more integrated role for the private sector in protecting the critical infrastructure. Second, public-private sector collaboration became the "new normal" for this activity. There is recognition that joint action by government and business is needed to achieve resilience. For the public and private

sectors, each of these shifts further developed and clarified the understanding of how to effectively protect the critical infrastructure.

2.2. *From protection to resilience*

The evolution from protection to resilience can be described as follows. In its original post-9/11 form, government protection of critical infrastructure narrowly focused on the events and circumstances that came before an incident occurred. Targets were hardened; walls were built; armed guards were posted; surveillance equipment and intrusion alarms were installed; the focus was on stopping an incident before it occurred. In short, protection concerned the "before" rather than the "after." This was viewed as a largely governmental responsibility—which we refer to as the "government protects" model of critical infrastructure protection.

But the "government protects" model was shown to be insufficient. One of the most significant deficiencies was that it neglected the vital role of public-private partnerships in critical infrastructure protection. For example, dams, nuclear power plants, and commercial manufacturing facilities are remarkably complex systems. They make use of a host of private sector products and services. The notion that government alone could effectively protect the wide array of facilities ignores the complexities of the systems. Thus, a new, more inclusive approach—resilience—replaced the outmoded "government protects" model with an "everybody protects" model of critical infrastructure protection [27].

Resilience places critical infrastructure protection within an immense network of public, private, non-profit, civic, and individual actors. The burden of protection is spread among these stakeholders and, most significantly, to businesses themselves, which own or operate some 85% of the U.S. critical infrastructure [28]. The general public also participates in activities to enhance resilience. The New York City Metropolitan Transportation Authority (MTA), for example, launched a public awareness campaign in 2003 called *If You See Something, Say Something*. The campaign placed colorful posters on subway cars—which the DHS has designated as a part of the critical infrastructure—that encouraged citizens to report suspicious behavior to police and MTA employees [29]. The *If You See Something, Say Something* campaign demonstrates the importance of public engagement in activities to promote critical infrastructure resilience. The U.S. Federal Emergency Management Agency (FEMA) also actively encourages the public to prepare for disasters. Its advertisements stress the importance of having an emergency kit, preparing a family emergency plan, and being informed about ongoing emergencies [30]. Individual preparedness can translate into societal preparedness, which can help promote critical infrastructure resilience. By engaging multiple segments of society, including the private sector and the general public, resilience represents a conceptual improvement on the idea of critical infrastructure protection.

Resilience also advances the idea of critical infrastructure protection in a temporal way. Whereas the "government protects" model of critical infrastructure protection focuses on pre-incident prevention, resilience incorporates the idea of pre-incident prevention and post-incident response. It concerns both the "before" and the "after." In the abstract, resilience is generally helpful for both the public and private sectors—it means more comprehensive safety. But resilience also introduces difficult fiscal constraints. Someone has to pay for resilience to move from rhetoric to reality.

The current global financial crisis impacts U.S. critical infrastructure protection measures, including the adoption of resilience. Businesses are making painful choices about how to trim spending in all areas, including on security controls. Fiscal constraints are further compounded by the rarity of major disasters, because large-scale emergencies have a way of concentrating the attention of public policymakers and freeing up money for protection initiatives [31]. But reduced budgets and infrequent major disasters mean that the attention of policymakers and business executives is less attuned to critical infrastructure protection. Without this attention, critical infrastructure protection can become marginalized. Diminished importance means reduced budgets, which translate into eroding effectiveness; it is a classic example of a vicious circle.

Multiple forces are working against the move from protection to resilience, despite governmental and corporate recognition of the importance of the move. It is in the interest of the public sector and the private sector to embrace resilience despite fiscal tightening. But under the current circumstances, there is the potential for a split between the appearance and the reality of public-private partnerships, undermining the value of public-private partnerships in critical infrastructure protection.

Unless government and business actually deliver on their commitments to resilience, the actual value of public-private partnerships will remain in doubt. As things stand now, rewards come from a hollow commitment to resilience rather than genuine changes that could achieve true resilience.

3. Challenges threatening the effectiveness of public-private partnerships

Public-private sector coordination and information sharing are foundational in U.S. critical infrastructure protection. Since 9/11, there has been a remarkable surge in this activity across the public and private sectors. For example, the CIPAC mentioned earlier provides a federal-level mechanism for public-private sector information sharing [32]. InfraGard is a Federal Bureau of Investigation (FBI)-led initiative dating back to 1996 that now brings together more than 50,000 public and private sector representatives working in the area of critical infrastructure protection [33]. The All Hazards Consortium, a not-for profit organization, hosts public-private sector workshops on critical infrastructure protection [9]. These are all positive signs that the public and private sectors recognize the importance of coordinating and sharing information, and that they are taking action to achieve mutually beneficial goals. However, there remain a number of challenges that government and business still need to overcome. Without greater attention from policymakers, these challenges will reduce the long-term value of public-private partnerships.

3.1. *Obstacles to cross-sector coordination*

Effective public-private sector coordination in critical infrastructure protection continues to face challenges. The challenges result from imprecise contracts that create a mismatch in expectations, a lack of centralized mechanisms for coordinating integrated actions, a tendency on the part of the actors in a partnership to act out of self-interest, and the prospect of public and private sector actors relying on the other to bear the costs of the partnership. These obstacles are present in many areas of critical infrastructure protection. To better analyze the obstacles, we focus on specific concerns related to contracts and the agricultural sector.

While useful, contracts are imperfect instruments for defining public-private sector roles and facilitating coordination. Unanticipated issues can arise that extend beyond the scope of a specific contract, prompting the government to demand products and services from a firm beyond those defined in the original contract [34]. This leaves the firm with a range of choices. The firm can reluctantly accept the extra work without requiring payment, negotiate for extra payment for the extra work, or it can refuse to do the work. In certain situations, laws or regulations might compel the firm to deliver the additional products or services.

But if the firm chooses to reluctantly accept extra work without negotiating for additional payment, this can lead to cost overruns, impacting overhead expenses. Representatives of the firm may also push back against increasing demands from public sector clients. This is understandable—a firm must protect its financial interests. But private sector pushback can then sour relationships between business and government. This can hamper coordination by temporarily slowing or reducing cross-sector communication. Repeatedly delivering goods and services beyond the original contract terms can lead to contract renegotiation. This process requires time and effort, and it risks delaying or preventing the fulfillment of contractual obligations.

Failures to clearly delineate roles and responsibilities for public and private sector actors have also led to challenges in protecting a vital area of U.S. critical infrastructure: the agricultural sector. The U.S. food supply is recognized as critical to national security, yet the basic challenge of coordinating security efforts for the food supply remains unsettled [35]. A 2011 Government Accountability Office (GAO) report notes that there is no centralized coordination mechanism for protecting the U.S. food and agriculture sector [36]. At the federal level, the responsibility for food and agriculture security is primarily spread among DHS and the U.S. Department of Agriculture (USDA), Department of Health and Human Services (DHHS) and Environmental Protection Agency (EPA) [36]. Against this backdrop, the USDA is charged under Homeland Security Presidential Directive (HSPD)-9 with developing a mass zoonotic disease vaccination program. The reasoning behind this initiative is that terrorists could deliberately introduce diseases to kill substantial numbers of farm animals, or an ordinary zoonotic disease not introduced by humans could infect American livestock [36]. Either scenario would harm the U.S. food supply. This would overwhelm the public sector, which is responsible for the response, as well as the private sector, which produces the vaccines [36].

Major coordination challenges in this area of critical infrastructure protection remain unresolved. Certain vaccines have not been produced for cost or logistical reasons. There are vaccine distribution problems at the state level. There is confusion about the vaccines stockpiled for agricultural purposes as opposed to the Strategic National Stockpile (SNS), the national cache of medical supplies for large-scale public health emergencies [36]. All this underscores the importance of having centralized coordination mechanisms in critical infrastructure protection initiatives, and especially where public-private partnerships are concerned. The diverging interests of government and businesses can sometimes create role conflicts and confusion. Having a centralized coordination mechanism to navigate these issues can help alleviate the challenges by managing the needs of public and private sector actors.

This type of centralized coordination of critical infrastructure protection initiatives is important because there is a general tendency for each participant in a partnership to act out of pure self-interest and without regard for the partnership, resulting in what has been called the "tragedy of the commons" [37]. When public and private sector actors partner with each other—even with the best intentions to work collaboratively—each actor retains a need to look out for its own interests. These circumstances create an ongoing tension between individual goals and collective goals [38]. The tension can affect the choices made by the public and private sector partners in critical infrastructure protection.

There is also a tendency for individual participants in a public-private partnership to let others in the partnership absorb the costs of the partnership. The phenomenon is similar to what economists call the "free rider" problem [39]. Specifically, the parties in a public-private partnership naturally tend to invest less in the partnership, because doing less helps the individual actors to maximize their net gains from the partnership. This tendency also influences the choices of the individual actors in the context of the partnership. It means that, all things being equal, an individual actor in a public-private partnership will put in the minimum amount of investment required to sustain the partnership.

For example, persistent challenges in protecting the agricultural sector point to a potential disconnect between the appearance and the reality of public-private partnerships. Agricultural security is an important homeland security priority for government, and billions of dollars hang in the balance for agricultural firms [40–43]. But basic coordination of public-private sector efforts to produce animal vaccines and plan for agricultural emergencies is clearly uneven. Individual participants in a public-private partnership may display a commitment to the partnership, but they also face a tension between individual and collective goals, and they tend to invest as little as possible in the partnership in order to increase their own gains from the partnership. A false sense of security can emerge from this environment, and lead to organizational apathy over time. The reason is simple: government and business have few incentives to enhance coordination if it appears that coordination is already taking place. This perpetuates the *status quo*, which means continuing coordination difficulties. The appearance of cross-sector coordination carries at least two interrelated negative effects.

First, it can lead to stagnation in true coordination levels. Second, the stagnation has a way of "locking in" lower collective levels of security. Both these pathologies harm critical infrastructure protection efforts.

3.2. Gaps in information sharing

There is also an "expectations gap" in information sharing between the public and private sectors. Neither sector appears to be satisfied with the information it receives from the other. Also, there exists a mutually acknowledged reluctance to exchange sensitive information. A 2010 GAO report [44] noted that many private sector representatives feel that the information they receive from the government is generic and, therefore, not actionable. Additionally, the report noted that business executives expect to have access to sensitive government information related to critical infrastructure protection, but are not receiving it from the government. How can we explain these findings?

Multiple variables conspire to hinder effective cross-sector information sharing [45]. An unsettled organizational landscape exists in critical infrastructure protection. Personnel turnover and reorganizations can diminish or erode relationships between public and private sector actors. When one's colleagues and counterparts change, new working relationships must be forged with new colleagues and new counterparts. This process takes time and can hinder communication. Moreover, fundamental questions of trust persist. It is extremely difficult to share sensitive information absent trust. This is true whether the trust comes in the form of something tangible such as a security clearance, or something less concrete like a feeling of mutually-shared confidence. Also, information sharing rarely provides an immediate payoff for businesses. Prieto [45] labels this the *quid pro quo* problem, in which private firms expect measurable benefits from information sharing, but do not receive them. This is all further complicated by a sense in the business community that government holds back information and does not provide the "whole story." Putting aside the value of information, these issues illustrate the basic challenges of actually sharing information.

It is useless to talk about public-private sector commitments to information sharing if the sharing cannot occur in a meaningful way. Over the long term, a false front of robust information sharing can hide dysfunction and poor results. After all, government can take satisfaction knowing that, in the eyes of its stakeholders (i.e., the public), it is sharing information—even when the information is generic, useless, and dated in the eyes of the business community. Similarly, businesses can relax, knowing that they are good stewards of national security, simply by providing the government with minimal data pertaining to their own security vulnerabilities. These approaches can entrench low levels of public-private sector engagement. Additional information sharing beyond this low standard is unlikely if it requires increased overhead spending for businesses, longer hours for government employees, and barely noticeable benefits. This has the potential to stunt the growth of public-private partnerships and jeopardize homeland security.

3.3. Shortfalls in private sector engagement in critical infrastructure protection

Businesses need incentives to spend on their own protection measures. To date, DHS has instituted a number of initiatives to boost the ability of businesses to enter the general homeland security arena, including the critical infrastructure space [46,47]. But it is important to distinguish these projects from how businesses spend money on protecting their own operations. Since these ideas are conceptually close to each other, it is easy to confuse the efforts of a business focused on developing critical infrastructure technologies as investing in self-protection.

Telling businesses that they must protect or perish may not be good enough any longer. In 2005, Lewis and Darken [20] stated that firms will voluntarily opt-in to robust critical infrastructure protection measures. They maintain that the notion that critical infrastructure protection is prohibitively expensive for the private sector is a kind of false choice [20]. Businesses, the argument goes, have a vested interest in the continuity of operations. Citing the effects of Hurricane Katrina in the Gulf, Lewis and Darken point out that severe disruptions can force businesses into bankruptcy [20]. In effect, they maintain that there is a built-in incentive for businesses to invest in the continuity of operations—not doing so risks a complete shutdown. While reasonable on its face, this argument does not hold up to scrutiny. In theory, businesses are indeed motivated toward self-preservation. But this ignores the sometimes illogical, non-linear decision-making patterns of human beings that operate and patronize the businesses.

- First, this idea brushes aside the notion of consumers gravitating toward the most affordable products and services regardless of their reliability. A certain proportion of the population will always choose the cheaper option. Businesses that invest less in security pass on fewer security-related costs to consumers. This can provide a relative price reduction, making a less reliable firm the more affordable option towards which consumers gravitate. In this case, a business has an incentive to remain competitive and therefore not to invest in additional protection.
- Second, pointing to business failures in the wake of Hurricane Katrina is hardly sufficient to prompt businesses to take protective actions. People tend to be optimistic and forget negative evidence over time. This tendency impacts the emergency preparedness efforts of businesses and government entities. It leads to enduring, well-documented disaster preparedness fallacies that plague individuals and organizations. These include historical precedence (e.g., "It has not happened yet, so it likely would not happen"); fallacies of improbability (e.g., "That kind of thing does not happen here"); cost (e.g., "We just do not have the funding for it this year"); cognitive biases (e.g., "There have been no disasters recently, therefore, I am not actively thinking about emergency preparedness, so preparedness is unimportant"); cultural norms (e.g., particular populations are statistically less inclined to

trust government authorities or prepare for emergencies); and prioritization schema (e.g. "In the big picture, emergency preparedness is not that important right now"). Simply stating that it is in the best interest of business to invest in protection is not enough to overcome these fallacies.

- Third, the return-on-security-investment for a business ultimately comes from the ability of the business to continue to generate revenue in the midst of a crisis. This reality can make it difficult to initially justify the cost of emergency preparedness measures—a business can only fully understand the need to spend money on emergency preparedness measures when it is in the midst of an emergency. Thus, while the value of investing in emergency preparedness measures is clear, connecting the initial expense of the measures to potential revenue can be a challenge.
- Fourth, the argument flies in the face of overwhelming evidence that individuals and organizations continue to be woefully unprepared for disasters, despite major disasters affecting businesses year after year [48,49].

Thus, the argument that businesses are naturally motivated to invest in protection overlooks important subtleties. Businesses are supposed to keep their operations humming even in the midst of disruptions. They should be self-motivated to do this and not require government intervention. In a competitive market, however, ensuring the long-term continuity of operations may take a backseat to generating short-term revenue. This dynamic can also be exacerbated by other policy conditions, including a hands-off approach by government with regard to critical infrastructure protection.

The George W. Bush administration took a market-driven stance on critical infrastructure protection, with little government intervention or regulation entering into the equation. Survey data reveals that this strategy failed to spur firms to action [21]. This is largely due to the need for businesses to keep costs low in order to be competitive. Commercial pressure is compounded by the general belief that enhanced security elevates costs, degrades efficiency, does not guarantee reliability, and limits consumer access to goods and services [21]. This belief provides little incentive for business leaders to invest in additional security measures. It also suggests that there is a key role for government in promoting business engagement in critical infrastructure protection.

But, as DeBruijne and Van Eeten [19] observe, U.S. government appeals based on morality, patriotism, or civic responsibility quickly lose their luster when they eat into a firm's bottom line. They point out that, while government and business both agree on the importance of critical infrastructure protection, the consensus can be remarkably shallow. Schneier [50] notes that a business executive who suddenly announces a 25% increase in security spending for the good of the country would almost certainly be fired. Businesses may publicly promote their commitment to security but, behind closed doors, there are limits to their security expenses. Beyond these limits, genuine (rather than rhetorical) investment in security is difficult to come by. A 2008 Congressional hearing on private sector compliance with a government advisory underscores the challenges involved in promoting business investment in critical infrastructure protection.

Threats to the national power grid—technically known as the Bulk Power System (BPS)—are well-documented [51,52]. Less known is the persistent tension between regulators and firms related to BPS security. A 2007 DHS test demonstrated the ease with which a hacker could compromise the BPS. In the test, technicians were able to remotely break into electrical grid components and deliberately cause them to malfunction [53]. As a result of the test, the North American Electric Reliability Corporation (NERC)—a non-profit umbrella group of power companies—issued an advisory to national electricity producers [54]. The advisory provided specific information on the vulnerability exploited by the test. It also included information on how to remedy the vulnerability. However, it was up to the individual producers to comply with the recommendations.

The timeline set for implementation of the guidance was 180 days. More than a year later, the Federal Energy Regulatory Commission (FERC)—a government agency—audited 30 electricity producers to check their voluntary compliance with the advisory. Of the 30 producers audited, only two or three had fully complied with the advisory and the accompanying guidance [54]. The Congressional testimony [54] focused on this gap in compliance—the prohibitively high cost to implement the guidance may have been why the corrections were not implemented more widely.

This instance of non-compliance with clear guidance for critical infrastructure protection shows why effective incentives are essential. Absent a clear business motivation for investing in security, it is unrealistic to expect businesses to spend on increased security measures, especially if the adjustments also impact overhead expenses. However, there is also a second, related issue here, which is connected to the ongoing global economic crisis.

Short-term spending on security and protection reduces the availability of funds for other needs. Today, this is a difficult prospect for firms to consider. Layoffs are increasing; production is slowing; revenues are shrinking [55]. Businesses are faced with the difficult choice of spending on short-term survival or making longer-term investments in protection. Businesses that are in dire straits must gamble—they can choose to maintain what remains of their operations or cut into core business activities in the name of improved critical infrastructure protection. Only the most security-conscious businesses can be expected to choose the first option. It does not make sense to worry about security cameras when the financial core is melting down.

This trend does not bode well for public-private partnerships in critical infrastructure protection. It means that businesses that are focusing on survival are spending less on security. Over time, and particularly as the economy begins to recover, this pattern of low spending may become "sticky." A new norm of not expending budgets on protection may emerge. Of course, the public sector cannot shoulder the lion's share of critical infrastructure protection. But this is the logical outcome of long-term reductions in business spending

on security. After all, someone has to pay for protection. Therefore, for the short and medium terms, it is important to institute incentives that promote private sector engagement in critical infrastructure protection.

Dunn Cavelty and Suter [56] have proposed a basket of incentives and penalties to help build public-private partnerships. It is up to the government, they argue, to choose between regulation, financial incentives, definitions of liability, contracts, subsidies, loans, deficit guarantees, issuing licenses, state insurance, tax relief, and fines. Of course, some of these tools could present a conflict for government itself. For example, the government is a large consumer of electricity, but if these policy tools result in the government being charged more by electrical companies, then the government has helped to achieve one goal (i.e., better cooperation from the private sector) at its own expense. Nevertheless, this range of options provides tools for the government to spur the development of public-private partnerships. It also opens up a way to increase private sector involvement in critical infrastructure protection that is more consistent with business interests. Rather than appealing to good citizenship or other values, these choices simply make good financial sense. Of course, they come with some caveats: it is far from certain if the list of policy tools is as comprehensive as it could be, or if its elements could potentially be implemented in an effective manner. Despite these shortcomings, there is a pressing need to create workable incentives for private sector engagement in critical infrastructure protection.

A framework of incentives must support commitments to cross-sector collaboration. Without incentives, the growth of public-private sector partnerships will be stymied, because no business executive interested in maximizing profit would spend more on protection than what is perceived to be the minimum necessary to sustain business operations. Businesses need more than appeals to emotion or goodwill to meaningfully engage with the government in critical infrastructure protection. The government must institute effective incentives to help ensure the long-term private sector commitment to critical infrastructure protection.

3.4. *The cyber problem*

Effective cybersecurity requires a cultural shift toward close and continuing public-private sector cooperation. This has been occurring with increasing effectiveness since the terrorist attacks of 9/11. One example is the National Cyber Security Alliance (NCSA), an organization focused on raising public awareness about cybersecurity issues [57]. Public-private partnerships are at the center of the NCSA mission. The NCSA board includes representatives from well-known technology companies such as Cisco Systems, Microsoft, Google, and Facebook [58]. Demonstrating substantial public-private sector cooperation, the White House and DHS in 2010 promoted National Cyber Security Awareness Month (NCSAM), the most visible NCSA initiative [59].

A 2011 hacking incident highlights the importance of strong working relationships between public and private sector representatives in the area of cybersecurity. In June 2011, Google disclosed that unknown individuals from China had illegally accessed the personal email accounts of several senior U.S. government officials [60]. This was done via "phishing," a method of fraudulently obtaining a user's information through fabricated emails. Google alerted the FBI about the incident. The White House National Security Council (NSC) and DHS followed up with Google to assess the impact of the incident [60]. The national security implications of the incident underscore why strong working relationships between public and private sector entities are so essential in critical infrastructure protection. The relationships can help foster closer cooperation and information sharing between the public and private sectors; also, they enable the public and private sectors to work together more efficiently.

The examples above demonstrate that government agencies and businesses must view collaborative cybersecurity as an integral part of their daily operations. Despite the positive steps, challenges remain to effectively address cybersecurity considerations. Government cybersecurity recommendations to private industry as well as other government agencies are often implemented inconsistently. The unresolved challenges risk the erosion of the value of public-private sector partnerships in cybersecurity initiatives.

Challenges also exist to implementing cybersecurity best practices. In a survey of industrial control system operators, Permann et al. [61] observed that common security procedures were not being followed consistently. Indeed, Permann et al. highlighted an important gap between appearance and reality in the area of cybersecurity. While government agencies and businesses may appear to use relatively uniform cybersecurity standards, this is not necessarily the case. This pattern is also visible in the context of the U.S. electrical grid.

The 2008 House of Representatives hearing on the BPS mentioned in Section 3.3 underscores the difficulty of integrating cybersecurity into other critical infrastructure protection initiatives [54]. Teams of government scientists identified a clear electronic vulnerability in the BPS. The officials drafted a list of remedies to address the vulnerability, distributed the list to electrical utilities, and provided a timeline for implementation. Despite these proactive steps, compliance with the recommendations remained low [54]. This gap suggests that, despite the appearance of public-private sector cooperation on cybersecurity initiatives, actual cooperation may be less common than expected [62].

A 2009 GAO report [63] also adds weight to the idea that effective public-private sector coordination in cybersecurity may not be as common as it might seem. The GAO report noted that, while significant efforts are underway to integrate cybersecurity planning throughout DHS, sector-specific plans are not being updated with cybersecurity information to the degree that they should [63]. Tellingly, these plans also continue to focus primarily on physical threats rather than cyber threats. The situation persists despite a steady drumbeat of electronic crimes and attacks on public and private sector information systems [64]. Like the deficiencies in addressing BPS vulnerabilities, the GAO report shows a widening gap between public and private sector approaches to cybersecurity. Government and businesses inadvertently undermine public-private partnerships by publicizing their mutual commitment to cybersecurity initiatives, but they cooperate in the initiatives and/or adopting their measures in a minimal way.

Government emergency management documents highlight a similarly uneven approach to cybersecurity. Emergency managers will be increasingly needed to handle "cyber disasters," but important U.S. emergency management documents do not reflect this new reality.

Despite the increasing number of cyber incidents, the 2008 National Response Framework (NRF) and National Incident Management System (NIMS) documents [65,66]—core doctrinal publications for emergency managers—hardly addressed cybersecurity. The NRF briefly describes a cyber attack scenario as part of a broader discussion related to emergency planning [65]. NIMS does not mention cyber issues at all. In contrast, the 2009 National Infrastructure Protection Plan (NIPP) comprehensively integrates the discussion of cybersecurity [14]. Focused tactical documents, such as *Configuring and Managing Remote Access for Industrial Control Systems* from DHS [67], also show concern for cybersecurity issues. The gap existing between the emergency management and infrastructure protection documents is curious and deserves further exploration.

It is reasonable to suppose that the gap between the NRF/NIMS and NIPP reflects differences in disciplinary focus. Emergency managers and those with otherwise strong connections to incident response may not yet view cybersecurity as a front burner issue, although this is changing. By contrast, the NIPP authors, clearly concerned about critical infrastructure protection, recognize that information and communications technology is an essential facet of modern life.

This gap is arguably the crux of the cyber problem in critical infrastructure protection. Effective cybersecurity requires a shift in culture. It is not enough to consider cybersecurity in an emergency management context; instead, it must be viewed as a unifying thread that transcends the operations of all organizations. Researchers and practitioners working in the area of critical infrastructure protection (vis-à-vis emergency management) already recognize the importance of this cultural change [68,69]. The reason is simple: information and communications technology is itself a critical infrastructure sector. But it is actually emergency managers and other practitioners who do not normally focus exclusively on critical infrastructure protection that need to make cybersecurity part of their organizational cultures. Fortunately, future releases of the NRF and NIMS will likely integrate additional discussion of cybersecurity. These updates will help place government and corporate emergency managers in a better position to understand the relevance of cybersecurity to their respective operations. Public-private sector approaches to cybersecurity may become more integrated as a result. This can lead to greater cross-sector uniformity in planning and incident response, ultimately benefiting all critical infrastructure protection activities.

Solving the cyber problem thus involves several overlapping areas of concern. It is a given that basic cybersecurity principles need to be followed by businesses and government agencies. But emergency managers and other specialists that do not typically focus on critical infrastructure are in the best position to actually benefit from the changes. After all, information and communications technology experts do not need to be convinced of the importance of cybersecurity. Rather, non-experts could benefit the most from greater knowledge of cybersecurity threats. Unless there is alignment between experts and non-experts in information and communications technology from both government and business, public and private sector approaches related to cybersecurity will be out of sync and lose their effectiveness.

The lack of synchronization threatens to lower the potential value of public-private partnerships. Either the public sector or the private sector will be in a perpetual game of catch-up with the other. The process of catching-up and realigning cybersecurity strategies causes delays. These delays mean that vulnerabilities will persist for longer periods of time, increasing the possibility of them being exploited by malicious actors. This not only harms public-private partnerships, but also negatively impacts the electronic defenses of society as a whole.

4. Enhancing the effectiveness of public-private partnerships

As we have argued, public-private partnerships in critical infrastructure protection are at an important crossroads. Despite the potential benefits of public-private partnerships, there are numerous organizational pathologies that create the conditions for the partnerships to fall short of expectations. We suggest five initial steps that can help remove these pathologies.

- *Choose collaborative leadership, not regulation*: It is clear that the private sector must fully participate in critical infrastructure protection in order for both government and business to achieve the broader homeland security mission. The BPS vulnerability discussed above underscores the importance of private sector participation in critical infrastructure protection, even when the payoffs for that participation are not immediately obvious. Businesses are faced with a basic choice of resisting this participation, which may eventually lead to government regulation, or engaging in collaborative leadership with government, which involves jointly re-assessing mutually shared goals, strategies, and tactics. We support the latter. In fact, excellent research has been conducted to inform these efforts. Flynn [21] argues for collaborative leadership across the public-private sector divide. Government, his case goes, must directly engage with the private sector to promote critical infrastructure protection rather than rely on purely market forces to dictate solutions. Other research [70] extends this thinking further and proposes a spectrum of government engagement levels with the private sector. Values in this spectrum range from total state control of infrastructure, to a hybrid model of delegation and negotiation with businesses, to purely market forces dictating protection levels [70]. Using this research, government and business can develop a baseline understanding of what goal-oriented cooperation should look like, and how their respective roles can evolve in partnerships over time. This is helpful in bolstering public-private sector collaboration. It also provides a foundation for a shared understanding of what needs to be done to achieve the protection objectives.

- *Measure what is really happening—not what appears to be happening*: Government administrators and business executives should rigorously examine what is really occurring in public-private partnerships rather than what appears to be occurring. The current gaps in information sharing with regard to critical infrastructure protection demonstrate that there is the potential for public-private partnerships to appear to be more beneficial than they actually are. To help correct this, there must be consensus on what the public and the private sectors need from public-private partnerships to bolster critical infrastructure protection efforts. With this mutual understanding in mind, metrics can be developed to measure the genuine levels of cooperation and information sharing, as well as outcomes from cross-sector coordination. This basic re-examination of objectives will help confirm that public-private partnerships are oriented toward common goals. New measurements can then track if public-private partnerships are producing the intended results for both government and business.
- *Focus on quality, not quantity, of information*: The gaps in information sharing discussed above show that both government and business are dissatisfied with the information they receive from each another. The public sector generally seems to perceive that businesses are holding back data on their critical systems and facilities. Businesses find government-supplied information on critical infrastructure protection threats to be dated, watered-down, and of little use. This suggests that both government and business are following a process-oriented approach, meaning that they are sharing for the sake of sharing without paying much attention to what they are sharing. A goal-oriented approach, by contrast, emphasizes the quality of information. A "meeting of the minds" on the type, timeliness, and specific level of detail desired by government and business with regard to information related to critical infrastructure protection would go a long way toward reducing the mutual frustration.
- *Increase awareness of cybersecurity issues in the emergency management community*: The post-9/11 world is all about breaking down silos among disparate security functions. But it is clear that aspects of U.S. cybersecurity (one silo) have not fully made their way into important federal-level emergency management publications (another silo). This suggests that there may be an underdeveloped awareness in the U.S. emergency management community of the increasingly important role that cybersecurity plays in emergencies. Further integrating information on cybersecurity into emergency management training materials would help raise awareness and increase the commitment to protection efforts. This, in turn, could help increase the penetration of cybersecurity-related information into emergency management documents.
- *Understand resilience*: It remains to be seen if resilience will prove more than just a new buzzword in homeland security and critical infrastructure protection circles. While its use remains in vogue, important questions need to be considered by the public and private sectors, both individually and jointly. What precisely does resilience mean to us? What are the challenges we will face in embracing resilience? How will adopting resilience actually change the way we operate on a daily basis? And, perhaps most importantly, can this change be measured? Our analysis suggests that significant costs will be associated with the evolution from critical infrastructure protection to resilience. At this early stage, it would be helpful for government and business to determine exactly what the costs are and who will bear them.

The five steps listed above will not solve all the challenges facing public-private partnerships in critical infrastructure protection, but they hold promise. Public-private partnerships are indispensable to critical infrastructure protection and it is vital that policymakers do all that is possible to grow new partnerships and nurture existing partnerships.

5. Conclusions

Strong steps are being taken in all the critical infrastructure sectors to bolster coordination and information sharing across the government-business divide. Despite these steps, increased attention should be placed on growing and nurturing public-private partnerships in critical infrastructure protection. Certain structural challenges indicate that public-private partnerships focused on critical infrastructure protection may be on shaky ground. Cross-sector coordination efforts and information sharing are not delivering as expected. There is a frustrating lack of financial incentives that could promote businesses to invest in protection measures. Meanwhile, uneven public and private sector approaches to cybersecurity demonstrate that protection efforts are out of alignment. Left unchecked, these pathologies will promote organizational complacency. Researchers and policymakers must confront these challenges to unlock the full potential of public-private partnerships.

Three interesting research questions merit further examination:

- What measurable benefits do government and business leaders reap from public-private partnerships in critical infrastructure protection? The "tragedy of the commons," in which individual actors in a public-private partnership tend to behave in their self-interest, highlights the need for success stories related to public-private partnerships in critical infrastructure protection. The success stories—accounts of measurable benefits for all the participants in public-private partnerships—can help stimulate partnership-oriented behavior by the individual actors in public-private partnerships. In particular, participants in public-private partnerships must see how acting for the good of the partnerships can directly benefit themselves and their organizations. To generate success stories, focus groups with public sector officials and business representatives could be used to help explore the differences between the rhetorical and genuine benefits of public-private partnerships. These groups can also provide an excellent setting in which to examine the advantages and frustrations of cross-sector partnerships. Data about the measurable benefits of

public-private partnerships would be immensely useful to both researchers and practitioners.

- How do middle managers and front-line practitioners perceive public-private partnerships in critical infrastructure protection? Analyses of public-private partnerships in this article largely derive from high-level views of organizational activities. But workers at the middle and front lines of organizations tend to have a more detailed view of operational realities than senior leaders. Quantitative analyses of the relevant data could help identify emerging trends and challenges that may not be readily apparent to leaders in the public and private sectors.
- What metrics can be used to measure the success of public-private partnerships in critical infrastructure protection? The information sharing gaps highlighted in this article underscore the need for metrics to measure the progress of public-private partnerships in critical infrastructure protection. Research needs to be done to identify metrics for success in public-private partnerships. This challenge is distinct from the identification of success stories and benefits mentioned above. It is essential to define the particular advantages conferred on critical infrastructure protection activities by public-private partnerships. But to be truly meaningful, it is vital to actually measure the strength and effectiveness of the advantages.

Critical infrastructure protection is an enduring homeland security challenge. With some 85% of critical infrastructure in private sector hands, government-business partnerships are indispensable to protection efforts. While numerous gains have been achieved in public-private partnerships since the terrorist attacks of September 11, 2001, some inconvenient truths about the genuine effectiveness of the partnerships remain latent. It is vital that leaders from the public and private sectors critically examine the degree to which critical infrastructure protection partnerships are actually achieving their objectives.

REFERENCES

[1] N. Busch, A. Givens, Public-private partnerships in homeland security: Opportunities and challenges, Homeland Security Affairs 8 (1) (2012) 1–24.

[2] M. Bult-Splering, G. Dewulf, Strategic Issues in Public-Private Partnerships: An International Perspective, Blackwell, Oxford, United Kingdom, 2006.

[3] R. Beauregard, Public-private partnerships as historical chameleons, in: J. Pierre (Ed.), Partnerships in Urban Governance: European and American Experience, MacMillan, London, United Kingdom, 1997, pp. 52–70.

[4] P. Rosenau (Ed.), Public-Private Policy Partnerships, MIT Press, Cambridge, Massachusetts, 2000.

[5] P. Schaeffer, S. Loveridge, Toward an understanding of types of public-private cooperation, Public Performance and Management Review 26 (2) (2002) 169–189.

[6] B. Regan, Enhancing Emergency Preparedness and Response: Partnering with the Private Business Sector, M.A. Thesis, Department of National Security Affairs, Naval Postgraduate School, Monterey, California, 2009.

[7] S. Goldsmith, W. Eggers, Governing by Network: The New Shape of the Public Sector, Brookings Institution Press, Washington, DC, 2004.

[8] ChicagoFIRST, About us, Chicago, Illinois (〈www.chicagofirst.org/about/about_us.jsp〉), 2012.

[9] All Hazards Consortium, Critical Infrastructure Protection, Frederick, Maryland (〈www.ahcusa.org/criticalInfra.htm〉), 2012.

[10] U.S. Department of Homeland Security, Critical Infrastructure Partnership Advisory Council, Washington, DC (〈www.dhs.gov/files/committees/editorial_0843.shtm〉), 2012.

[11] The White House, National Security Strategy, Washington, DC (〈www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf〉), 2010.

[12] M. Barbaro, J. Gillis, Wal-Mart at forefront of hurricane relief, The Washington Post, September 6, 2005.

[13] National Commission on the BP Deepwater Horizon Oil Spill and Offshore Drilling, Deep Water—The Gulf Oil Disaster and the Future of Offshore Drilling: Final Report to the President, Washington, DC, 2011.

[14] U.S. Department of Homeland Security, National Infrastructure Protection Plan, Washington, DC, 2009.

[15] U.S. Department of Homeland Security, National Cyber Incident Response Plan (Interim Version), Washington, DC, 2010.

[16] U.S. Department of Homeland Security, Quadrennial Homeland Security Review Report: A Strategic Framework for a Secure Homeland, Washington, DC, 2010.

[17] P. Auerswald, L. Branscomb, T. La Porte, E. Michel-Kerjan (Eds.), Seeds of Disaster, Roots of Response: How Private Action Can Reduce Public Vulnerability, Cambridge University Press, New York, 2006.

[18] S. Eckert, Protecting Critical Infrastructure: The Role of the Private Sector, in Guns and Butter: The Political Economy of International Security, in: P. Dombrowski (Ed.), Lynne Rienner Publishers, Boulder, Colorado, 2005.

[19] M. de Bruijne, M. Van Eeten, Systems that should have failed: Critical infrastructure protection in an institutionally fragmented environment, Journal of Contingencies and Crisis Management 15 (1) (2007) 18–29.

[20] T. Lewis, R. Darken, Potholes and detours in the road to critical infrastructure protection policy, Homeland Security Affairs 1 (2) (2005) 1–11.

[21] S. Flynn, The brittle superpower, in Seeds of Disaster, in: P. Auerswald, L. Branscomb, T. La Porte, E. Michel-Kerjan (Eds.), Roots of Response: How Private Action Can Reduce Public Vulnerability, Cambridge University Press, New York, 2006, pp. 26–36.

[22] President's Commission on Critical Infrastructure Protection, Critical Foundations: Protecting America's Infrastructures, Report of the President's Commission on Critical Infrastructure Protection, Washington, DC, 1997.

[23] A. Abou-Bakr, Managing Disasters Through Public-Private Partnerships, Georgetown University Press, Washington, DC, 2013.

[24] G. Bush, Executive Order Establishing the Office of Homeland Security, Washington, DC (〈georgewbush-whitehouse.archives.gov/news/releases/2001/10/20011008-2.html〉), 2001.

[25] U.S. Department of Homeland Security, Homeland Security Act of 2002, Washington, DC (〈www.dhs.gov/xabout/laws/law_regulation_rule_0011.shtm〉), 2002.

[26] G. Bush, Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization and Protection, Washington, DC (〈www.dhs.gov/xabout/laws/gc_1214597989952.shtm〉), 2008.

[27] U.S. Department of Homeland Security, National Infrastructure Advisory Council, Critical Infrastructure Resilience: Final Report

and Recommendations, Washington, DC (〈www.dhs.gov/xlibrary/assets/niac/niac_critical_infrastructure_resilience.pdf〉), 2009, pp.1–54.
[28] U.S. Department of Homeland Security, Critical Infrastructure Sector Partnerships, Washington, DC (〈www.dhs.gov/critical-infrastructure-sector-partnerships〉), 2011.
[29] Metropolitan Transportation Authority, If You See Something, Say Something, New York (〈www.mta.info/news/stories/?story=55〉), 2013.
[30] U.S. Federal Emergency Management Agency, Make a Plan, Washington, DC (〈www.ready.gov/make-a-plan〉), 2012.
[31] B. Lopez, Critical infrastructure protection in the United States since 1993, in Seeds of Disaster, in: P. Auerswald, L. Branscomb, T. La Porte, E. Michel-Kerjan (Eds.), Roots of Response: How Private Action Can Reduce Public Vulnerability, Cambridge University Press, New York, 2006, pp. 37–50.
[32] U.S. Department of Homeland Security, Council Members, Critical Infrastructure Partnership Advisory Council, Washington, DC (〈www.dhs.gov/files/committees/editorial_0848.shtm〉), 2012.
[33] InfraGard, About InfraGard, Washington, DC (〈www.infragard.net/about.php?mn=1&sm=1-0〉), 2012.
[34] D. Kettl, Managing indirect government, in: L Salamon (Ed.), The Tools of Government: A Guide to the New Governance, Oxford University Press, New York, 2002, pp. 490–510.
[35] U.S. Department of Homeland Security, Critical infrastructure, Washington, DC, (www.dhs.gov/files/programs/gc_1189168948944.shtm), 2010.
[36] U.S. Government Accountability Office, Homeland Security: Actions Needed to Improve Response to Potential Terrorist Attacks and Natural Disasters Affecting Food and Agriculture, Report to the Chairman, Subcommittee on Oversight of Government Management, the Federal Workforce, and the District of Columbia, Committee on Homeland Security and Governmental Affairs, U.S. Senate, Washington, DC, 2011.
[37] G. Hardin, The tragedy of the commons, Science 13 (162) (1968) 1243–1248.
[38] A. Saz-Carranza, S. Opsina, The behavioral dimension of governing inter-organizational goal-directed networks—Managing the unity-diversity tension, Journal of Public Administration Research and Theory 21 (2) (2011) 327–365.
[39] T. Kameda, T. Tsukasaki, R. Hastie, N. Berg, Democracy under uncertainty: The wisdom of crowds and the free-rider problem in group decision making, Psychological Review 118 (1) (2011) 76–96.
[40] U.S. Department of Agriculture, Homeland Security—Overview, Washington, DC (〈www.usda.gov/wps/portal/usda/usdahome?navid=HOMELANDSECU&navtype=CO〉), 2013.
[41] U.S. Department of Homeland Security, Food, Agriculture, and Veterinary Defense Division, Overview, Washington, DC (〈www.dhs.gov/xabout/structure/gc_1234195670177.shtm〉), 2013.
[42] A. Allen, A. Myles, P. Fuentes, S. Muhammad, Agricultural terrorism: potential economic effects on the poultry industry in Mississippi, presented at the Southern Agricultural Economics Association Annual Meeting, Tulsa, Oklahoma, 2004.
[43] J. Monke, Agroterrorism: Threats and Preparedness, Congressional Research Service, Washington, DC (〈www.fas.org/sgp/crs/terror/RL32521.pdf〉), 2007.
[44] U.S. Government Accountability Office, Critical Infrastructure Protection: Key Private and Public Cyber Expectations Need to be Consistently Addressed, Washington, DC, 2010.
[45] D. Prieto, Information sharing with the private sector: history, challenges, innovation, and prospects, in Seeds of Disaster, in: P. Auerswald, L. Branscomb, T. La Porte, E. Michel-Kerjan (Eds.), Roots of Response: How Private Action Can Reduce Public Vulnerability, Cambridge University Press, New York, 2006, pp. 404–428.
[46] U.S. Department of Homeland Security, SECURE Program, Washington, DC (〈www.dhs.gov/secure-system-efficacy-through-commercialization-utilization-relevance-and-evaluation-program〉), 2013.
[47] U.S. Department of Homeland Security, FutureTECH, Washington, DC (〈www.dhs.gov/futuretech〉), 2013.
[48] A. Loten, Most business owners unprepared for natural disasters, Inc. Magazine, April 24, 2006.
[49] C. Rubin, Why you should stop reading this and go get a data backup plan, Inc. Magazine, September 15, 2011.
[50] B. Schneier, Beyond Fear: Thinking Sensibly about Security in an Uncertain World, Copernicus Books, New York, 2003.
[51] Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, Hearing on Securing the Modern Electrical Grid from Physical and Cyber Attacks, Committee on Homeland Security, U.S. House of Representatives, 111th Congress: First Session, Washington, DC, July 21, 2009.
[52] North American Electric Reliability Corporation and U.S. Department of Energy, High-Impact, Low Frequency Event Risk to the North American Bulk Power System: A Jointly-Commissioned Summary Report of the North American Electric Reliability Corporation and the U.S. Department of Energy's November 2009 Workshop, Washington, DC, June 2010.
[53] SecurityFocus, DHS video shows potential impact of cyberattack (〈www.securityfocus.com/brief/597〉), September 27, 2007.
[54] R. Boucher, Subcommittee on Energy and Air Quality, Hearing on Protecting the Electrical Grid from Cybersecurity Threats, Committee on Energy and Commerce, U.S. House of Representatives, 110th Congress: Second Session, Washington, DC, September 11, 2008.
[55] P. Domm, Corporate layoffs increase as economy sputters, CNBC, (〈www.cnbc.com/id/43977352/Corporate_Layoffs_Increase_as_Economy_Sputters〉), August 1, 2011.
[56] M. Dunn Cavelty, M. Suter, Public-private partnerships are no silver bullet: an expanded governance model for critical infrastructure protection, International Journal of Critical Infrastructure Protection 2 (4) (2009) 179–187.
[57] National Cyber Security Alliance, About the National Cyber Security Alliance, Washington, DC (〈www.staysafeonline.org/about-us/about-national-cyber-security-alliance〉), 2013.
[58] National Cyber Security Alliance, Board Members, Washington, DC (〈www.staysafeonline.org/about-us/board-members〉), 2013.
[59] National Cyber Security Alliance, National Cyber Security Awareness Month 2010 Results in Brief, Washington, DC (〈www.staysafeonline.org/sites/default/files/resource_documents/NCSAM%202010%20Short%20Report011411.docx〉), 2011.
[60] C. Kang, E. Nakashima, Google says hackers based in China accessed U.S. officials' Gmail accounts, The Washington Post, June 1, 2011.
[61] M. Permann, J. Hammer, K. Lee, K. Rohde, Mitigations for security vulnerabilities found in control system networks, presented at the Sixteenth Annual Joint Instrumentation, Systems and Automation Society POWID/EPRI Controls and Instrumentation Conference, San Jose, California, 2006.
[62] U.S. Chamber of Commerce, Business Software Alliance, TechAmerica, Internet Security Alliance (ISA), Center for Democracy and Technology, Improving Our Nation's Cybersecurity through the Public-Private Partnership: A White Paper, Washington, DC, 2011.

[63] U.S. Government Accountability Office, Critical Infrastructure Protection: Current Cyber Sector-Specific Planning Approach Needs Re-Assessment, Washington, DC, 2009.
[64] M. Lennon, Threat from cyber attacks nearing statistical certainty, SecurityWeek, June 22, 2011.
[65] U.S. Department of Homeland Security, National Response Framework, Washington, DC, 2008.
[66] U.S. Department of Homeland Security, National Incident Management System, Washington, DC, 2008.
[67] U.S. Department of Homeland Security, Configuring and Managing Remote Access for Industrial Control Systems, Washington, DC, 2010.
[68] L. Coles-Kemp, M. Haridou, Insider threat and information security management, in: C. Probst, J. Hunker, D. Gollman, M. Bishop (Eds.), Insider Threats in Cyber Security, Springer, New York, 2010, pp. 45–72.
[69] D. Lohrmann, Five reasons cybersecurity should be a top priority, Governing, December 2010.
[70] D. Assaf, Conceptualizing the use of public-private partnerships as a regulatory arrangement in critical information infrastructure protection, in: A. Peters, L. Koechlin, T. Forster, G. Zinkernagel (Eds.), Non-State Actors as Standard Setters, Cambridge University Press, New York, 2009, pp. 61–83.