SYMPOSIUM

HOMELAND SECURITY, LAW, AND POLICY THROUGH THE LENS OF CRITICAL INFRASTRUCTURE AND KEY ASSET PROTECTION

Joe D. Whitley, George A. Koenig, and Steven E. Roberts*

ABSTRACT: Homeland security continues to be one of the principal priorities of government at all levels. Homeland security, however, is not static. What gets protected, how resources are allocated, and the manner in which threats are identified continue to evolve. In particular, critical infrastructure and key asset protection are fundamental components of homeland security greatly influenced by developments in law and policy.

CITATION: Joe D. Whitley, George A. Koenig, and Steven E. Roberts, Homeland Security, Law, and Policy Through the Lens of Critical Infrastructure and Key Asset Protection, 47 Jurimetrics J. 259–279.

*Joe D. Whitley was the first General Counsel of the Department of Homeland Security and is now an attorney and part of the Global Security and Enforcement Team in the Washington, D.C., office of Alston & Bird L.L.P. George A. Koenig was former Counsel to the General Counsel of the Department of Homeland Security and is now an attorney and part of the Global Security and Enforcement Team in the Washington, D.C., office of Alston & Bird L.L.P. Steven E. Roberts is an attorney specializing in homeland security matters in Boca Raton, Florida.

I. HOMELAND SECURITY: NOT A POST 9/11 PHENOMENON

The escalation of terrorist activity throughout the 1990s suggests that the end of the Cold War ushered in a new era of conflict.[1] The terrorist enemies in this war neither maintain standing armies nor subscribe to the laws of war. To the contrary, they fight in the shadows, target civilians, and seek weapons of mass destruction.[2] Physical destruction, economic harm, and social unrest are their ends. To accomplish them, terrorists frequently target critical infrastructures and key assets, such as rail networks, power plants, and hotels.

Critical infrastructures may be defined as the "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, or any combination of those matters."[3] As such, there are twelve identified critical infrastructure sectors in the United States: 1) defense industrial base, 2) food and agriculture, 3) public health and health care, 4) emergency services, 5) energy, 6) transportation systems, 7) banking and finance, 8) information technology, 9) telecommunications, 10) drinking water and water systems, 11) chemicals, and 12) postal and shipping.[4] For important sites either not classified directly as critical infrastructures or for which additional, independent security considerations must be addressed, the federal government has defined five categories of key assets: national monuments and icons; nuclear reactors, materials, and waste; dams; government facilities; and commercial key assets, such as prominent commercial buildings, hotels, and sports stadiums.[5]

Arguably, the defense (and, if necessary, the rapid reconstitution) of these critical infrastructures and key assets sectors *is* homeland security. Understanding their vulnerabilities and dependencies is the "heavy lift" necessary to

---

1. *See* NAT'L COMM'N ON TERRORIST ATTACKS UPON THE U.S., THE 9/11 COMMISSION REPORT (2004) [hereinafter THE 9/11 COMMISSION REPORT]; *see also* STEVE COLL, GHOST WARS: THE SECRET HISTORY OF THE CIA, AFGHANISTAN, AND BIN LADEN, FROM THE SOVIET INVASION TO SEPTEMBER 10, 2001 (2004) (outlining the rise of jihadi terrorists in Afghanistan and U.S. policy in the region).

2. Former CIA Director Porter Goss told a Senate panel in 2005 that "it may be only a matter of time before al-Qa'ida or another group attempts to use chemical, biological, radiological or nuclear weapons." *Current and Projected National Security Threats to the United States: Hearing Before the S. Select Comm. on Intelligence*, 109th Cong. 8 (2005) (statement of Porter Goss, Director of Central Intelligence); *see also Annual Threat Assessment of the Director of National Intelligence: Hearing Before the S. Select Comm. on Intelligence*, 109th Cong. 11 (2006) (statement of John D. Negroponte, Director of National Intelligence) ("Although an attack using conventional explosives continues to be the most probable scenario, al-Qa'ida remains interested in acquiring chemical, biological, radiological, and nuclear materials or weapons to attack the United States, U.S. troops, and U.S. interests worldwide.").

3. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act), Pub. L. No. 107-56, § 1016, 115 Stat. 272, 275–76 (2001).

4. *See* U.S. DEP'T OF HOMELAND SEC., NATIONAL INFRASTRUCTURE PROTECTION PLAN 3 (2006).

5. *Id.*

make the United States safer from terror. Thus, it is not coincidental that many of America's homeland security efforts are largely variations on, or extensions of, critical infrastructure and key asset protection.

Long before 9/11, the federal government recognized the escalation of terrorist activity and took steps to confront it. Two incidents—the 1995 bombing of the Alfred P. Murrah Federal Building in Oklahoma City and the 1996 bombing of the Khobar Towers Military Complex in Dhahran, Saudi Arabia—left little doubt that terrorism represented a new and growing threat to U.S. national security. Consequently, in 1997, President Clinton issued Executive Order 13,010[6] which created the President's Commission on Critical Infrastructure Protection (PCCIP) to examine terrorism through the prism of critical infrastructure.

Recognizing the importance of electronic networks and systems, the PCCIP asked not only how terrorists might exploit the physical vulnerabilities of critical infrastructures and key assets, but also their digital vulnerabilities.[7] The Commission also investigated novel issues of critical infrastructure and key asset protection, including the use of emergency declarations such as the Stafford Act,[8] and how such exceptional executive powers might be employed.[9] The PCCIP delivered its *Report of the President's Commission on Critical Infrastructure* to President Clinton in October 1997.[10] It left no doubt that the threat of terrorism was real.

PCCIP's warning did not fall on deaf ears. Largely as a result of the Commission's final report, the president issued a national security order—Presidential Decision Directive 63 (PDD-63)—in May 1998.[11] PDD-63 recognized that future adversaries would be unable to confront America on the battlefield and would turn to new technologies and methods to wage asymmetrical war.[12] It stated that enemies

> may seek to harm [the United States] in non-traditional ways including attacks within the United States. Because our economy is increasingly reliant

---

6. Exec. Order No. 13,010, 61 Fed. Reg. 37,347 (July 15, 1996).

7. The Commission's attention to cyber security was informed, in some measure, by worries of computer malfunctions following the millennium computer rollover on December 31, 1999.

8. Robert T. Stafford Disaster Relief and Emergency Assistance Act of 1974, 42 U.S.C. §§ 5121–5206 (2000) [hereinafter Stafford Act].

9. PRESIDENT'S COMMISSION ON CRITICAL INFRASTRUCTURE PROTECTION, CRITICAL FOUNDATIONS: PROTECTING AMERICA'S INFRASTRUCTURE 80–82 (1997) (citing the Defense Production Act of 1950, Pub. L. No. 81-774, 64 Stat. 798 (1950), and the Stafford Act—statutes intended for use primarily during national emergencies).

10. *Id.*

11. Presidential Decision Directive No. 63 (May 22, 1998), *available at* http://www.fas.org/irp/offdocs/pdd/pdd-63.htm; *see also* Press Release, White House, Fact Sheet: Protecting America's Critical Infrastructures PDD-63 (May 22, 1998), *available at* http://www.fas.org/irp/offdocs/pdd-63.htm (stating that PDD-63 "builds on the recommendations of the President's Commission on Critical Infrastructure Protection"). The president issued a complementary presidential decision directive, PDD 62, to be interpreted in conjunction with PDD 63. Press Release, White House, Fact Sheet: Combating Terrorism PDD-62 (May 22, 1998), *available at* http://www.fas.org/irp/offdocs/pdd-62.htm.

12. Presidential Decision Directive No. 63, *supra* note 11.

> upon interdependent and cyber supported infrastructures, non-traditional attacks on our infrastructure and information systems may be capable of significantly harming both our military power and our economy.[13]

Under PDD-63's authority, new agencies within the federal government were spawned and new responsibilities were created. The Directive ordered the Federal Bureau of Investigation to create a National Infrastructure Protection Center to "serve as a national critical infrastructure threat assessment, warning, vulnerability, and law enforcement investigation and response entity."[14] Perhaps more importantly, PDD-63 accurately reflected the significance of the private sector in critical infrastructure and key asset protection, and ordered the federal government to "consult with owners and operators of the critical infrastructures to strongly encourage the creation of a private sector information sharing and analysis center."[15]

As such, PDD-63 recognized the obvious sentiment: critical infrastructure protection represents a unique challenge that requires private sector support. With up to 90% of the nation's critical infrastructures and key assets in private hands, the federal government's ability to protect, respond, and remediate was (and remains) largely dependent upon the cooperation and participation of industry.[16] Industry is frequently in the best position to recognize vulnerabilities, recommend remediation strategies, and implement protection procedures.

The timing of PDD-63 was prophetic. Three months later, in August 1998, Osama bin Laden and his al Qaeda terror network attacked the U.S. embassies in Nairobi, Kenya and Dar es Salaam, Tanzania in near-simultaneous explosions.[17] The American response to the embassy attacks was, in retrospect, limited: President Clinton ordered cruise missile strikes at targets in Sudan and Afghanistan, and the Department of Justice issued indictments, most in absentia.[18]

Some critics—especially after 9/11—believe that the U.S. response to the 1998 embassy bombings was squandered. Rather than striking al Qaeda with the brunt of the American armed forces, the military response did little damage to the terror infrastructure.[19] Hardly crippled, al Qaeda continued to plan and successfully execute additional attacks—notably the October 2000 strike on the U.S.S. Cole in Aden, Yemen.[20]

---

13. *Id.*

14. *Id.*

15. *Id.*

16. Public-private partnerships for the purposes of critical infrastructure protection and homeland security have become even more important since September 11, 2001.

17. Karl Vick, *149 Confirmed Dead in Embassy Blasts*, WASH. POST, Aug. 9, 1998, at A1.

18. The Department of Justice indicted Osama bin Laden in November 1998. *See* Benjamin Weiser, *Saudi Is Indicted in Bomb Attacks on U.S. Embassies*, N.Y. TIMES, Nov. 5, 1998, at A1.

19. With regard to the issue of assassinating Osama bin Laden following the 1998 attacks, see RICHARD A. CLARKE, AGAINST ALL ENEMIES: INSIDE AMERICA'S SECRET WAR ON TERROR 204 (2004) ("I still to this day do not understand why it was impossible for the United States to find a competent group of Afghans, Americans, third-country nationals, or some combination who could locate bin Laden in Afghanistan and kill him.").

20. *See* COLL, *supra* note 1, at 532.

September 11, 2001, however, represents the climax of terrorist action that reshaped U.S. foreign and domestic policy. Action oversees—particularly in Afghanistan—began in parallel with legal changes at home. In near record time, Congress passed and the president signed sweeping legislation that transformed everything from the Bank Secrecy Act[21] to the domestic insurance market.[22] More than five years later, homeland security legislation continues to occupy significant attention on Capitol Hill—and will likely continue to do so for the indefinite future.[23] A domestic terror attack—or an attack against American assets overseas—would surely accelerate legislative activity.

Critical infrastructure and key asset protection has never been more important. Moving from plan to practice requires comprehensive national action. Toward this end, the Bush Administration issued Homeland Security Presidential Directive 7 (HSPD 7) in December 2003.[24] HSPD 7, by its terms, updates and supercedes PDD-63 and establishes "a national policy for federal departments and agencies to identify and prioritize U.S. critical infrastructure and key resources and to protect them from terrorist attack."[25] HSPD 7 assigns federal departments and agencies specific critical infrastructure tasks across their respective jurisdictions. While the newly created Department of Homeland Security (DHS)[26] assumes the lead role for critical infrastructure and key asset protection, HSPD 7 allocates tasks to virtually every federal department and agency. From the Department of Agriculture to the Department of State, critical infrastructure and key asset protection is an interagency responsibility.

More specifically, HSPD 7 classifies some departments and agencies as Sector Specific Agencies (SSAs) for defined categories of critical infrastructures or key assets, reflecting departmental or agency expertise. For example, the Department of Agriculture is the SSA for the agriculture sector; the Department of Defense is the SSA for the defense sector; and the Department of the Treasury is the SSA for the banking and finance sector.[27] SSAs are directed to, among other things, "conduct or facilitate vulnerability assessments of the sector[ ] and encourage risk management strategies to protect against and mitigate the effects of attacks against critical infrastructure and key

---

21. *See* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act), Pub. L. No. 107-56, 115 Stat. 272 (2001).

22. *See* Terrorism Risk Insurance Act of 2002, Pub. L. No. 107-297, 116 Stat. 2322 (2002).

23. For example, Congress recently passed legislation to protect the nation's most vulnerable chemical infrastructures. *See* Department of Homeland Security Appropriations Act of 2007, Pub. L. No. 109-295, § 550, 120 Stat. 1355 (2006).

24. Homeland Security Presidential Directive No. 7, 39 WEEKLY COMP. PRES. DOC. 1816 (Dec. 22, 2003) [hereinafter HSPD 7].

25. *Id.*

26. The creation of the Department of Homeland Security represents the largest government reorganization in more than fifty years. George W. Bush, Remarks by the President to the New Employees of the U.S. Department of Homeland Security (Feb. 28, 2003), http://www.whitehouse.gov/news/releases/2003/02/20030228-2.html.

27. HSPD 7, *supra* note 24, at 1818.

resources."[28]

An important task of each SSA is to provide input to the *National Infrastructure Protection Plan* (NIPP).[29] The NIPP effectuates many of the policy requirements directed by HSPD 7 and provides the overall framework and strategy to address critical infrastructure protection. In doing so, the NIPP reflects additional lessons learned and refines critical infrastructure and key asset protection.[30]

While the NIPP reflects critical infrastructure and key asset protection considerations from the perspective of the year 2006, the process of its creation may be as important as the final product. From a purely historical viewpoint, the NIPP is the result of work that began not in late 2001, but rather in 1996. Thus, the NIPP is the product of HSPD 7, which itself was an outgrowth of PDD-63. PDD-63, in turn, was a product of the PCCIP, in response to the Oklahoma City and Khobar Towers attacks. In this sense, the protection of critical infrastructures and key assets is not a recent phenomenon. September 11th only made the issues acute and demonstrated both the significance of the threat and the depth of the vulnerabilities.

II. THE DOMESTIC TERROR THREAT SINCE 9/11: THE THREAT TO CRITICAL INFRASTRUCTURES AND KEY ASSETS

It has been more than five years since 9/11. While terrorists have attacked repeatedly since that time, the United States has been fortunate. The fact that the United States has not been the object of a successful terrorist attack since 9/11 leads some to believe that the terrorist threat has been neutralized; in essence, 9/11 was a "one-time event."

Nothing could be further from the truth. Recent judicial activity—not to mention the nearly successful attempt by terrorists to blow up as many as ten jets bound for the United States over the Atlantic in August 2006—proves the prospect of terrorist attacks is real. It remains necessary to protect critical infrastructure and key assets from a wide range of potential attacks for the indefinite future. Preparing for and defending against terrorism is the "new normalcy."

Current examples highlight the danger of viewing the threat of terrorism in isolation. One must look no further than the frequent pronouncement of federal terrorism indictments and successful prosecutions.

For example, in October 2003, Iyman Faris, a member of al Qaeda who traveled to Afghanistan and met personally with Osama bin Laden in 2000, began a federal prison sentence after pleading guilty to federal terrorism

28. *Id.* at 1819.

29. *See* U.S. DEP'T OF HOMELAND SEC., *supra* note 4; *see also* HSPD 7, *supra* note 24, at 1820.

30. *See generally* U.S. DEP'T OF HOMELAND SEC., *supra* note 4.

charges.[31] Faris received twenty years "for providing material support and resources to al Qaeda and conspiracy for providing the terrorist organization with information about possible U.S. targets for attack."[32] He later sought to vacate his guilty plea on grounds that authorities used information obtained by the National Security Administration's warrantless surveillance program in the case against him, but a federal judge denied Faris's motion in November 2006.[33]

By all accounts, Faris was no ordinary operative: he was a naturalized American citizen who was living a peaceful life in Columbus, Ohio.[34] Married to an American woman, Faris was "a seemingly hard-working truck driver . . . ."[35] In reality, Faris moonlighted as a terrorist, conducting surveillance and research for a failed post-9/11 plot.[36] In furtherance of that conspiracy, Faris "researched 'gas cutters'—the equipment for severing bridge suspension cables—and the New York City bridge [that was to be the object of the attack] on the Internet."[37] Faris then communicated his findings to handlers in the Middle East.[38]

The story of Iyman Faris is significant for several reasons. First, as previously noted, Faris highlights the fact that terrorists remain committed to attacking U.S. targets. Second, Faris demonstrates that terrorists can fly below the radar screen. Much like the 19 who executed the 9/11 attacks, Faris did not publicly spew jihad, stockpile weapons, or offer significant evidence to suggest that he was anything but "ordinary."

Third, the importance of Faris' occupation must not be discounted: as a truck driver, Faris obtained a hazardous materials endorsement on his commercial driver's license.[39] With the endorsement, Faris did not merely have the ability to access and transport hazardous materials—he had an entitlement to the facilities that produce and use them. Faris possessed ideal cover to access shipping yards, chemical facilities, and rail networks without raising suspicion. In 2004, the DHS and the FBI specifically cited Faris in an information bulletin when it warned of "the potential for terrorists to use heavy transport vehicles as vehicle-borne improvised explosive devices (VBIEDs) against a range

---

31. Faris was accused of—and pled guilty to—violating 18 U.S.C. §§ 371 and 2339(b) (2000). United States v. Faris, 388 F.3d 452, 454 (4th Cir. 2004).

32. Press Release, U.S. Dep't of Justice, Iyman Faris Sentenced for Providing Material Support to al Qaeda (Oct. 28, 2003), *available at* http://www.usdoj.gov/opa/pr/2003/October/03_crm_589.htm.

33. Jerry Markon, *Judge Lets Guilty Plea Stand in Terrorism Case*, WASH. POST, Nov. 11, 2006, at A12.

34. Press Release, U.S. Dep't of Justice, *supra* note 32.

35. *Id.*

36. *Id.*

37. *Id.*

38. *Id.*

39. Larry Kahaner, *Alleged Terrorist Faris Had CDL with Hazmat Endorsement*, DRIVERS, June 23, 2003, http://driversmag.com/ar/fleet_alleged_terrorist_faris.

of attractive targets in the United States."[40] The bulletin further stated that "[t]errorists have shown an interest in planning attacks that employ quantities of [hazardous materials] that could be used as Weapons of Mass [Destruction]."[41]

Fourth, the plot's failure demonstrates that security initiatives undertaken since 9/11 pay dividends. Rather than communicating a willingness to proceed, Faris "concluded that the plot to destroy the bridge by severing cables was unlikely to succeed because of the bridge's security and structure."[42] Arguably, but for the security enhancements, Faris might have concluded that the operation should continue as planned.

Finally, Faris is a reminder of the obvious: terrorists rarely act independently. Faris was not a lone wolf, but an actor in a larger conspiracy which spanned continents and time zones. He was a sleeper cell, conducting operational surveillance and then waiting for and acting upon instructions from al Qaeda's leadership. It is for this reason that a single arrest in one corner of the world often reverberates and produces actionable intelligence regarding plots against U.S. targets. Indeed, it was the March 2003 capture and subsequent debriefings of 9/11 mastermind Khalid Shaikh Mohammed that led to the arrest and later indictment of Faris.[43]

Other terror plots that have been alleged since 9/11 appear entirely homegrown, having neither an overseas "command and control" component nor an allegiance to a particular terror group. Nonetheless, the underlying ideology between international terrorists and purely domestic ones may be indistinguishable in some cases.[44]

In August 2005, the U.S. Attorney for the Central District of California announced that a federal grand jury had indicted four men "for their alleged roles in a terrorist plot to attack U.S. military facilities, Israeli government facilities and Jewish synagogues in the Los Angeles area . . . ."[45] The alleged plot was led by an inmate at the California State Prison in Sacramento and financed through armed robberies.[46] The defendants will likely stand trial in 2007.

---

40. Information Bulletin, U.S. Dep't of Homeland Sec. & Fed. Bureau of Investigation, Potential Threat to Homeland Security Using Heavy Transport Vehicles (July 30, 2004), *available at* http://www.rydersafetyservices.com/pdf/TruckBombThreat.pdf.

41. *Id.*

42. Press Release, U.S. Dep't of Justice, *supra* note 32.

43. *Are America's Trains Safe?*, CBS NEWS, Mar. 31, 2004, http://www.cbsnews.com/stories/2004/03/31/60II/main609695.shtml ("[U.S. i]nterrogators got the name of a U.S. citizen, Iyman Faris, from [Khalid Shaikh Mohammed], and [as a result Faris] was quickly picked up . . . .").

44. While al Qaeda—and al Qaeda-like terror organizations—are the primary threat to domestic security, it would be reckless to ignore right-wing militia and hate groups, and others, which have operated in the United States for many years. Timothy McVeigh and Terry Nicholas—not Osama bin Laden or Mohammed Atta—detonated a Ryder truck in front of the Alfred P. Murrah Federal Building in Oklahoma City in 1995, killing 168 people.

45. Press Release, U.S. Dep't of Justice, Four Men Indicted on Terrorism Charges Related to Conspiracy to Attack Military Facilities, Other Targets (Aug. 31, 2005), *available at* http://www.usdoj.gov/opa/pr/2005/August/05_crm_453.htm.

46. *Id.*

The nature of this plot—if true—is significant. The fact that the conspiracy could be directed from behind prison walls demonstrates that incarceration does not always mitigate the threat. Similar to organized crime bosses ordering murders from a jail cell, Islamic extremists may have the ability to act and recruit new members while incarcerated. This concern was underscored by FBI Director Robert Mueller when he testified before the Senate Select Committee on Intelligence in February 2005:

> As part of [the FBI's] continued efforts to identify populations that may be a target for extremist recruitment, the FBI has been involved in a coordinated effort between law enforcement and corrections personnel to combat the recruitment and radicalization of prison inmates. Prisons continue to be fertile ground for extremists who exploit both a prisoner's conversion to Islam while still in prison, as well as their [sic] socio-economic status and placement in the community upon their [sic] release.[47]

The alleged California plot also highlights an interesting aspect of terror financing. Rather than establishing front organizations to raise and conceal funds, the conspirators purportedly robbed gas stations.[48] Though ineffective, this modus operandi not only underscores the range of financing strategies that adversaries might employ but also demonstrates the limitations of many 9/11 anti-money-laundering policies when confronting low-tech financing schemes. Executive Order 13,224[49] and Title III provisions of the USA PATRIOT Act[50] are of little value when suspected terrorists seek to finance plots with gas station stickups.

Even when there are no indictments, the volume of unsubstantiated—though not necessarily irrelevant—threats are a reminder that terrorists are committed to attacking at a time and place of their choosing. Rarely a month goes by without homeland security officials citing a new domestic terrorism concern, although we must balance the quality of the intelligence against the proposed security countermeasure.

In October 2005, "an uncorroborated tip about a terrorist plot to blow up a vehicle loaded with explosives prompted the authorities to shut down a busy tunnel under the Baltimore harbor . . . ."[51] The tunnel—part of the vital Washington, New York, and Philadelphia transportation corridor—represents a high-profile target: the detonation of a car or truck bomb within the tunnel would kill motorists and disrupt the region's transportation network. Concerns

---

47. *Current and Projected National Security Threats to the United States: Hearing Before the S. Select Comm. on Intelligence*, 109th Cong. 24 (2005) (statement of Robert Mueller, Director of the Federal Bureau of Investigation).

48. Press Release, Dep't of Justice, *supra* note 45; *see also* Amy Argetsinger & Dan Eggen, *L.A. Holdups Linked to Islamic Group, Possible Terrorist Plot*, WASH. POST, Aug. 17, 2005, at A5.

49. *See generally* Executive Order No. 13,224, 66 Fed. Reg. 49,079 (Sept. 25, 2001).

50. *See generally* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act), Pub. L. No. 107-56, §§ 301–377, 115 Stat. 272, 273–74 (2001).

51. Gary Gately, *Terrorism Tip Closes Tunnels in Baltimore*, N.Y. TIMES, Oct. 19, 2005, at A12.

that terrorists might blow up a tunnel are not unreasonable and were analyzed extensively in 2003 by the Blue Ribbon Panel on Bridge and Tunnel Security at the request of the American Association of State Highway and Transportation Officials.[52] And, as the attacks in Madrid in 2004 and London in 2005 demonstrate, the transportation infrastructure remains high on the target list.

Finally, terror activities that appear isolated to a single geographic region frequently have international implications and direct consequences for domestic operations. When suicide bombers targeted western hotels, killing nearly 60 people in Amman, Jordan in November 2005, law enforcement officials increased security at hotels within the United States, particularly in New York City.[53]

III. WHY ARE CRITICAL INFRASTRUCTURES AND KEY ASSETS VULNERABLE TO TERRORISM?

It is important to understand why critical infrastructures and key assets are the targets of choice. There are six principal vulnerabilities.

A. Range of Attack Scenarios

Critical infrastructures and key assets may be attacked either directly or indirectly. A direct attack occurs when a critical infrastructure or key asset target is, itself, the end. For example, the intent of the 9/11 terrorists was to destroy the World Trade Center and the Pentagon. Those targets were the direct objects of the plot.

Conversely, critical infrastructures and key assets can also be attacked indirectly. Terrorists who blow up a rail car carrying chlorine gas intend to create a hazardous plume; their intent is not to destroy or disrupt the rail infrastructure per se. In such a scenario, attacking a critical rail infrastructure is simply the means to an end: a way to achieve the desired goal. When critical infrastructures and key assets can be attacked either directly or indirectly, adversaries have more attack options. This "range" of attack scenarios, in turn, makes a target more vulnerable because it increases the terrorists' likelihood of success.

---

52. *See* BLUE RIBBON PANEL ON BRIDGE & TUNNEL SEC., RECOMMENDATIONS FOR BRIDGE AND TUNNEL SECURITY 2 (2003) ("After considering the nature of bridge and tunnel components of the highway system and lessons learned from natural disasters, the effects of transportation-related consequences of the September 11th attack, and the recent barge collision in Oklahoma, the panel has determined that loss of a critical bridge or tunnel at one of the numerous 'choke points' in the highway system could result in hundreds or thousands of casualties, billions of dollars worth of direct reconstruction costs, and even greater socioeconomic costs.").

53. *Police Focus on Hotels after Jordan Bombings*, BUFFALO NEWS, Nov. 10, 2005, at A14, *available at* 2005 WLNR 18389129.

B. Target Interconnectivity

Critical infrastructures and key assets are highly dependent on each other. The failure of one critical infrastructure or key asset may quickly cascade and damage the functionality of nearby sectors. Thus, the consequences of attacking a "lone" critical infrastructure or key asset are rarely confined to the four corners of the target; the attack will likely have implications and effects across a range of interconnected sectors. Because the interconnectivity among critical infrastructures and key assets acts as a de facto force multiplier, critical infrastructures and key assets are opportune targets to create disproportionate harm.

The electrical blackout of August 2003 highlights this interconnectivity phenomenon.[54] Though caused by forces other than terrorism, the blackout affected millions of people across several U.S. states and Canada.[55] However, the incapacitation of the energy infrastructure meant more than the loss of lights or air conditioning: the critical infrastructures of transportation, emergency services, information and telecommunications, and even food, began to fail.[56]

While target interconnectivity is most pronounced in the context of the energy infrastructure, Hurricane Katrina proved that interconnectivity extends beyond the electrical grid. When the storm destroyed key components of the Gulf's transportation network, the effects were pronounced. Katrina "hit a chokepoint in the U.S. economy—a concentration of ports, rail lines, barge traffic and major highways making up one of the nation's major trade hubs."[57]

With the region's transportation infrastructure damaged, other critical infrastructure sectors suffered. Many Midwest farmers rely on the Gulf's barge and port traffic, which led some to suggest that "if it takes more than a few weeks to fix the ports, a glut of grain and widespread spoilage could yield a disastrous season for farmers."[58] One could conceive of a situation in which terrorists exploit a region's concentration of vital transportation nodes to cause economic disruption and possible loss of life among a range of interconnected sectors.

---

54. *See generally* U.S.–CANADA POWER SYSTEM OUTAGE TASK FORCE, FINAL REPORT ON THE AUGUST 14, 2003 BLACKOUT IN THE UNITED STATES AND CANADA: CAUSES AND RECOMMENDATIONS (2004) (providing a detailed account of the causes and consequences of the blackout).

55. *Id.* at 74

56. James Barron, *Lights Go on after Biggest Blackout, but Not Without 2nd Day of Suffering*, N.Y. TIMES, Aug. 16, 2003, at A6; *see also* Laura Berman, *We Tested Limits Living as Pioneers Without ATMs, Air Conditioning*, DETROIT NEWS, Aug. 17, 2003, at 1D; Brett McNeil, *Residents of Motor City Out of Gas, Water, Steam*, CHI. TRIB., Aug. 16, 2003, at C1. One study put economic losses caused by the Blackout at $6.4 billion. Patrick L. Anderson & Ilhan K. Geckil, *Northeast Blackout Likely to Reduce U.S. Earnings by $6.4 Billion* (Anderson Econ. Group, Working Paper No. 2003-2, 2003), *available at* http://www.andersoneconomicgroup.com/modules.php?name=Content&pa=display_aeg&doc_ID=664.

57. Neil Irwin, *Critical U.S. Supply Line Is Disrupted*, WASH. POST, Sept. 1, 2005, at A1.

58. *Id.*

C. High Target Density

Because many critical infrastructures and key assets are locations where large numbers of people congregate, these locations often have a high target density. Whether the target is a train station, football stadium, or commercial building, a terrorist strike is virtually guaranteed to cause significant casualties. It is not coincidental that terrorists have selected trains in Madrid and London and hotels in Amman and Jakarta.

High target density has not been lost in the research and development of counterterrorism exercises. In July 2004, the White House's Homeland Security Council produced "fifteen all-hazard planning scenarios for use in national, federal, state, and local homeland security preparedness activities."[59] Virtually all of the terror-related scenarios not only implicated critical infrastructures and key assets as hypothetical targets but also drew upon their high target densities to create scenarios that resulted in high victim mortality counts.[60] In one scenario,

> the [terrorist] uses a light aircraft to spray chemical agent YELLOW[61] into a packed college football stadium. The agent directly contaminates the stadium and the immediate surrounding area, and generates a downwind vapor hazard. The attack causes a large number of casualties that require urgent and long-term medical treatment, but few immediate fatalities occur. Of the total stadium attendance [of 100,000 people], 70% is exposed to the liquid at the time of the attack. The remaining 30% (i.e., those in the covered areas of the stadium), plus 10% of the total population in the vapor area, are exposed to vapor contamination.[62]

D. Inadequate Security

Physical and cyber security vulnerabilities continue to plague some of the most at-risk sites. The chemical industry, in particular, has come under increased scrutiny because many chemical facilities produce or store large quantities of hazardous materials. Critics of chemical facility security cite the tragedy in Bhopal, India, as an example of the danger. On December 3, 1984, methyl isocyanate leaked from a Union Carbide facility killing more than 3,000 people and permanently injuring countless more.[63]

---

59. HOMELAND SEC. COUNCIL, PLANNING SCENARIOS: EXECUTIVE SUMMARIES iv (2004).

60. *Id.*; *see also U.S. Report Maps Terror Scenarios*, BBC NEWS, Mar. 16, 2005, http://news.bbc.co.uk/2/hi/americas/4354147.stm.

61. The scenario states that "Agent YELLOW, which is a mixture of the blister agents sulfur Mustard and Lewisite, is a liquid with a garlic-like odor." HOMELAND SEC. COUNCIL, *supra* note 59, § 5-1.

62. *Id.*

63. *See* UNION CARBIDE CORPORATION, CHRONOLOGY OF KEY EVENTS RELATED TO THE BHOPAL INCIDENT (2004), *available at* http://www.bhopal.com/pdfs/chrono.pdf. It is important to note that the exact cause of the chemical release remains controversial to this day: while some believe that the chemical release was a tragic industrial accident others believe that a disgruntled worker sabotaged the plant and deliberately caused the chemical release.

According to a 2003 study conducted by the federal government, "123 U.S. chemical facilities had 'worst-case' scenarios where more than one million people could be at risk of exposure to a cloud of toxic gas" should any of the facilities fall victim to a successful terrorist attack.[64] Citing the inadequacies of voluntary security practices, a senior DHS official told a Senate panel in June 2005 that "it has become clear that the entirely voluntary efforts of [chemical] companies alone will not sufficiently address security for the entire chemical sector."[65]

E. Cyberspace

Physical attacks against critical infrastructures and key assets continue to be the terrorists' preferred modi operandi. Nonetheless, as critical infrastructures and key assets grow more network-centric, strikes using explosives may be replaced with (or complemented by) a keyboard and a mouse. At a minimum, terrorists currently use cyberspace to communicate.[66] The Internet also provides access to information to conduct target surveillance.[67]

Many members of Congress have expressed concern that terrorists will turn to cyberspace. In September 2005, the House Committee on Science held hearings on the vulnerabilities of the nation's critical infrastructure to cyber attack. Then-Committee Chairman Sherwood Boehlert (R-NY) opened the hearing by stating that: "[w]e shouldn't have to wait for the cyber equivalent of Hurricane Katrina to realize that we are inadequately prepared to prevent, detect, and respond to cyber attacks."[68] Chief Information Officers of major critical infrastructure owners and operators proceeded to warn "that the nation's critical infrastructure remains vulnerable to cyber attack [and] . . . that a major attack could result in significant economic disruption and loss of life."[69]

Al Qaeda may have already shown interest in terror operations conducted through or facilitated by cyberspace. A frequently cited *Washington Post* article from 2002 asserts that "U.S. investigators have found evidence . . . that

---

64. JOHN B. STEPHENSON, U.S. GOV'T ACCOUNTABILITY OFFICE, HOMELAND SECURITY: FEDERAL AND INDUSTRY EFFORTS ARE ADDRESSING SECURITY ISSUES AT CHEMICAL FACILITIES, BUT ADDITIONAL ACTION IS NEEDED (2005).

65. *Is the Federal Government Doing Enough to Secure Chemical Facilities and Is More Authority Needed?: Hearing Before the S. Comm. on Homeland Security and Governmental Affairs*, 109th Cong. 7 (2005) (statement of Robert Stephan, Acting Under Secretary for Information Analysis and Infrastructure Protection, U.S. Department of Homeland Security).

66. Iyman Faris, for example, communicated with his handlers in the Middle East over e-mail. Daniel Eisenberg, *The Triple Life of a Qaeda Man*, TIME.COM, June 22, 2003, http://www.time.com/time/magazine/article/0,9171,460158,00.html?iid=chix-sphere.

67. Internet Web sites allow terrorists to obtain real-time information about potential targets, including satellite imagery. *See* Danielle Belopotosky, *Google Monitors Debate Over Aerial Surveys of Facilities*, NAT'L JOURNAL'S TECH. DAILY, Aug. 24, 2005.

68. *Cyber Security: U.S. Vulnerability and Preparedness: Hearing Before the H. Comm. on Science*, 109th Cong. 13 (2005) (statement of Rep. Sherwood L. Boehlert, Chairman, H. Comm. on Science).

69. Press Release, House Comm. on Sci., *Nation's Critical Infrastructure Vulnerable to Cyber Attack, Industry Executives Say* (Sept. 15, 2005), *available at* http://gop.science.house.gov/press/109/109-129.htm.

al Qaeda operators spent time on [Web] sites that offer software and programming instructions for the digital switches that run power, water, transport and communications grids."[70]

If a cyber attack were to stand alone, the electrical power grid would be a likely target: network-dependent, interconnected, and porous, the power grid has layers of cyber vulnerabilities.[71] Control systems have become Web based and functions have been automated. Cyber security safeguards are difficult to implement because of the inherent architecture of the grid system.[72]

Additionally, a cyber attack could also be "blended" with a physical attack. In a "blended" attack scenario, terrorists may disable a city's emergency communications systems prior to detonating a series of car bombs. Firefighters and police officers would be unable to communicate and coordinate emergency responses, likely resulting in a greater loss of life.[73]

F. Information Sharing

As the owners and operators of the vast majority of the nation's critical infrastructures and key assets, the private sector is often in the best position to share relevant homeland security information with the federal government. Frequently, DHS cannot gain information regarding a critical infrastructure's choke points, protection strategies, or response plans unless the owner of the facility voluntarily shares the information with the Department.

As a result of a statutory amendment to the Freedom of Information Act (FOIA),[74] the owners and operators of critical infrastructures and key assets can now share homeland security related information with DHS without fear of FOIA disclosure. Federal law ensures that industries' voluntarily provided critical infrastructure and key asset information is "FOIA-proof."[75]

Without protection from FOIA, the private sector had been unwilling to share pertinent information with the federal government. Industry worried that competitors, litigants seeking to end-run the discovery process, or even terrorists and criminals would use FOIA to compel the federal government to share *what otherwise would not have been in the public domain but for voluntary*

---

70. Barton Gellman, *Cyber-Attacks by Al Qaeda Feared*, WASH. POST, June 27, 2002, at A1.

71. Justin Blum, *Hackers Target U.S. Power Grid*, WASH. POST, Mar. 11, 2005, at E1.

72. For example, Supervisory Control and Data Acquisition (SCADA) systems—used to control some grid functions—are difficult to secure. U.S. GEN. ACCOUNTING OFFICE, CRITICAL INFRASTRUCTURE PROTECTION: CHALLENGES AND EFFORTS TO SECURE CONTROL SYSTEMS 2 (2004) ("Securing control systems poses significant challenges. These include the limitations of current security technologies in securing control systems, the perception that securing control systems may not be economically justifiable, and conflicting priorities within organizations regarding the security of control systems.").

73. Nathaniel Hoopes, *New Focus on Cyber-Terrorism*, CHRISTIAN SCI. MONITOR, Aug. 16, 2005, at 1.

74. Homeland Security Act of 2002, Pub. L. No. 107-296, § 214, 116 Stat. 2135, 2152–53 (2002).

75. *See* 6 C.F.R. §§ 29.1–.9 (2007).

disclosure.[76] DHS issued Interim Regulations implementing the FOIA exemption in 2004[77] and Final Regulations on September 1, 2006.[78]

Despite the protection from FOIA, information flow from the private sector remains slow. As a general rule, the owners and operators of critical infrastructures and key assets continue to withhold homeland security information from DHS for two general reasons. First, while FOIA protection is available, it is not automatic. To obtain the protection, the submitting party must take a series of steps outlined in the Code of Federal Regulations.[79] While not objectively complicated, some in industry view the steps as too cumbersome.

Second, even with the law on their side, industry is not convinced that mistakes will not be made. Information that is shared and then accidentally released, for example, could harm or embarrass the submitting party who offered the information to DHS in good faith and with the expectation that it would be protected. This concern is strong enough to tilt the scale against disclosure.

IV. THE GROWING LEGAL DUTY OF CRITICAL INFRASTRUCTURES AND KEY ASSETS PROTECTION

The protection of critical infrastructures and key assets has increasingly become a legal obligation. Federal statutes passed since 9/11 create new security obligations for a growing number of critical infrastructure and key asset owners and operators. Failure to maintain reasonable security controls can now create liability under civil and possibly criminal law. Moreover, an emerging body of case law suggests that inadequate counterterrorism practices could be deemed negligent in light of reasonably foreseeable risks.

Lawsuits alleging that inadequate security practices exposed third parties to a high risk of terrorist attack are not uncommon. In 1993, terrorists detonated a truck bomb in the basement parking garage of the World Trade Center

---

76. Steven Roberts, *Keeping Corporate Secrets*, NAT'L L.J., May 26, 2003, at 26.

77. *See* Procedures for Handling Critical Infrastructure Information; Interim Rule, 69 Fed. Reg. 8074, 8083–89 (Feb. 20, 2004).

78. *See* Procedures for Handling Critical Infrastructure Information, 71 Fed. Reg. 52,262, 52,272–77 (Sept. 1, 2006).

79. *See* 6 C.F.R. §§ 29.1–.9.

(WTC).[80] Victims of that attack later sued the Port Authority of New York and New Jersey for negligent security practices.[81]

Liability essentially rested on whether the plaintiffs could prove that the Port Authority knew that the WTC was a terrorist target and, accordingly, failed to implement security measures commensurate with that risk. Siding with the plaintiffs in a procedural decision, the lower court found that "in the early 1980s, the Port Authority was aware of terrorist activities occurring in other areas of the world, and that the WTC, as a highly symbolic target, was vulnerable to terrorist attack."[82] The court even cited the Port Authority's own internal reports and studies to demonstrate that the Port Authority knew that the WTC was vulnerable.[83]

Faced with such evidence, the court stated that "the Port Authority's claim that this bombing was unforeseeable as a matter of law strains credulity."[84] A New York state appeals court unanimously affirmed the lower court's procedural ruling in December 2004, thereby allowing the case to proceed for jury trial.[85] On October 26, 2005, a New York jury found the Port Authority liable for failing to maintain adequate security practices.[86]

Some lawsuits have been filed even in the absence of harm. In September 2004, two lawyer-tenants who occupied office space in the Empire State Building filed a security-based lawsuit against the building's operators citing poor security practices.[87] The suit asserted that "the intentional, reckless, knowing and negligent conduct of [the building's operators] poses a clear and present danger and substantial risk of grievous bodily harm and death to persons lawfully on the premises of the Empire State Building."[88]

---

80. THE 9/11 COMMISSION REPORT, *supra* note 1, at 71.

> At 18 minutes after noon on February 26, 1993, a huge bomb went off beneath the two towers of the World Trade Center. This was not a suicide attack. The terrorists parked a truck bomb with a timing device on Level B-2 of the underground garage, then departed. The ensuing explosion opened a hole seven stories up. Six people died. More than a thousand were injured.

Id. Ramzi Yousef, the mastermind of that attack, *id.* at 72, is serving a life sentence and is incarcerated at the U.S. Penitentiary Administrative Maximum Facility in Florence, Colorado. Phil Hirschkorn, *Top Terrorist Convictions Upheld*, CNN.COM, Apr. 4, 2003, http://edition.cnn.com/2003/LAW/04/04/terrorism.yousef. The same facility houses Iyman Faris. Federal Bureau of Prisons – Inmate Locator, http://www.bop.gov/iloc2/LocateInmate.jsp.

81. *In re* World Trade Center Bombing Litig., 776 N.Y.S.2d 713 (Sup. Ct. 2004), *aff'd*, 784 N.Y.S.2d 869 (App. Div. 2004).

82. *Id.* at 718 (order granting in part and denying in part defendant's motion for summary judgment).

83. *Id.* ("In another report, entitled 'Terrorist Assessment World Trade Center 1984,' prepared at the request of the Port Authority Superintendent of Police, the Port Authority was warned that, more than any time in its history, the WTC should be considered a prime target for domestic and international terrorists.")

84. *Id.* at 736.

85. *In re* World Trade Center Bombing Litig., 784 N.Y.S.2d 869, 869 (App. Div. 2004).

86. *See Jury Rules Agency Was Negligent in 1993 Attack*, WASH. POST, Oct. 26, 2005, at A10; *see also* Anemona Hartocollis, *Port Authority Found Negligent in 1993 Bombing*, N.Y. TIMES, Oct. 27, 2005 at A6. The jury found the Port Authority 68% at fault.

87. Susan Saulny, *Suit Seeks Tighter Security at the Empire State Building*, N.Y. TIMES, Sept. 1, 2004, at B2.

88. *Id.*

The certainty of future terror-related lawsuits underscores the need for established "homeland security" standards and best practices. In 2004, the American National Standards Institute (ANSI) and the National Fire Protection Association (NFPA) published *NFPA 1600: Standard on Disaster/Emergency Management and Business Continuity Programs* (NFPA 1600).[89] The "standard establishes a common set of criteria for disaster management, emergency management, and business continuity programs."[90] As such, NFPA 1600 outlines the requirements, procedures, and methodologies necessary to ascertain a basic level of emergency preparedness. For example, NFPA 1600 directs users to conduct risk assessments[91] and establish communication plans in anticipation of an emergency.[92]

While NFPA 1600 is a generic standard, critical infrastructure and key asset owners and operators are well advised to implement its recommendations. The failure to do so could have legal implications. If in the future terrorists successfully attacked a critical infrastructure or key asset which resulted in loss of life, the success or failure of a subsequent lawsuit would likely hinge on the level of security and emergency preparedness undertaken by the attacked venue in light of the risk. If, at a minimum, the defendant (which, statistically, would be a critical infrastructure or a key asset owner and operator) were not "NFPA 1600 compliant," the plaintiffs would stand a better chance of succeeding under a negligence theory. Plaintiffs would claim that the defendant knew—or should have known—that the risk of terrorism was high.[93] Thus, the failure to implement the security safeguards defined by NFPA 1600 would be unreasonable and would represent a breach of a statutory or common law duty of care.

In such a scenario, plaintiffs would likely turn to the findings of the 9/11 Commission, among other sources, as evidence of notice and reasonableness.[94] The 9/11 Commission specifically stated that:

> We endorse the American National Standards Institute's recommended [NFPA 1600] standards for private preparedness . . . . We believe that compliance with the standard should define the standard of care owed by a company to its employees and the public for legal purposes. Private sector preparedness is not a luxury; it is a cost of doing business in the post-9/11 world.[95]

---

89. NAT'L FIRE PROT. ASS'N, NFPA 1600: STANDARD ON DISASTER/EMERGENCY MANAGEMENT AND BUSINESS CONTINUITY PROGRAMS (2004), *available at* http://www.nfpa.org/PDF/nfpa1600.pdf.

90. *Id.* § 1.1.

91. *Id.* § 5.3.

92. *Id.* § 5.9.

93. A plaintiff's attorney would likely argue that the question of foreseeability is so broadly defined that it is all but moot: because acts of terrorism are so frequent and widely reported (especially since 9/11), one could argue that it is virtually impossible for a critical infrastructure or key asset owner to claim lack of knowledge regarding the threats to or the vulnerabilities of such venues.

94. While not a legal authority, the 9/11 Commission Report carries substantial credibility.

95. THE 9/11 COMMISSION REPORT, *supra* note 1, at 398.

Defendants who do not heed the 9/11 Commission's recommendation may have a difficult time challenging allegations of negligent security and improper emergency preparedness.

NFPA 1600 also has implications beyond negligence. Adherence to NFPA 1600 could define the minimum standard of care required to obtain terrorism insurance or maintain credit ratings.[96] The 9/11 Commission "encourage[d] the insurance and credit-rating industries to look closely at a company's compliance with the ANSI [NFPA 1600] standard in assessing its insurability and creditworthiness."[97]

Terrorism remained a significant issue in 2005: unless Congress acted before the end of the year, the Terrorism Risk Insurance Act (TRIA) was slated to sunset on December 31, 2005.[98] Congress debated whether to extend the measure[99] and finally elected to do so when it passed the Terrorism Risk Insurance Extension Act of 2005 on December 22, 2005.[100] By extending TRIA until December 31, 2007,[101] Congress ensured the availability of terrorism coverage while giving the insurance and reinsurance industries additional time to develop terrorism insurance capacity on the open market.[102]

Because the insurance market must mitigate and control risk to the extent possible, one could imagine an underwriter requiring the insured party to implement security and emergency management policies as a condition of coverage. Consistent with the recommendation of the 9/11 Commission, underwriters will be forced to look to recognized standards, such as NFPA 1600, to determine insurability.

Civil lawsuits are not the only avenue leading to homeland security liability. Federal statutes create new homeland security responsibilities for increasing numbers of critical infrastructures and key asset sectors. One recent addition is the Energy Policy Act (EPA) of 2005.[103]

Prior to the enactment of the EPA, cyber security protection for the grid was ineffective because compliance with voluntary cyber security practices—promulgated by the North American Electric Reliability Council (NERC)—had been essentially unenforceable.[104] Under Title XII of the EPA, coined the

---

96. *Id.*

97. *Id.*

98. Terrorism Risk Insurance Act of 2002, Pub. L. No. 107-297, § 108(a), 116 Stat. 2322 (2002) [hereinafter TRIA].

99. Raymond Hernandez, *Senate Bill Would Renew Insurers' Aid on Terrorism*, N.Y. TIMES, Nov. 19, 2005, at C6; *see also More Risky Terror Business*, WALL ST. J., Nov. 21, 2005, at A16.

100. Terrorism Risk Insurance Extension Act of 2005, Pub. L. No. 109-144, 119 Stat. 2660 (2005).

101. *Id.* § 2(a).

102. The Terrorism Risk Insurance Act of 2002 was intended to "allow for a transitional period for the private markets to stabilize, resume pricing of such [terrorism] insurance, and build capacity to absorb any future losses, while preserving State insurance regulation and consumer protections." TRIA §101(b)(2). Because the private insurance market remained largely undeveloped by the end of 2005, a failure of Congress to extend TRIA likely would have resulted in the unavailability of terrorism insurance on the open market.

103. Energy Policy Act of 2005, Pub. L. No. 109-58, 119 Stat. 594 (2005).

104. Nick Bunkley, *Blackout Rules Are Voluntary*, DETROIT NEWS, Feb. 4, 2005, at 1D.

"Electricity Modernization Act of 2005," the owners and operators of the electric power grid must, among other things, ensure grid reliability.[105] The Act tasks the Federal Energy Regulatory Commission (FERC) to designate a new Electric Reliability Organization (ERO) to promulgate and enforce mandatory grid reliability standards.[106] The ERO's reliability standards must incorporate "requirements for the operations of existing bulk-power system facilities, including cybersecurity protection . . . ."[107] In July 2006, the Federal Energy Regulatory Commission certified the North American Electric Reliability Council as the Electric Reliability Organization.[108]

As the electric energy infrastructure implements the cyber security demands required by the EPA, other critical infrastructure and key asset sectors now face similar homeland security regulation. The Department of Homeland Security Appropriations Act of 2007 creates new legal mandates for the nation's most vulnerable chemical facilities.[109] The law requires the Secretary of Homeland Security to create "risk-based performance standards for security of chemical facilities and [requires] vulnerability assessments and the development and implementation of site security plans for chemical facilities."[110] DHS must promulgate interim final regulations implementing the law on or before April 4, 2007.[111] It is likely that the oversight now required in the chemical and electric power industries will serve as templates for future regulatory initiatives for other critical infrastructure and key asset sectors.

V. RISK MANAGEMENT AS A PROACTIVE STRATEGY

With so many challenges to critical infrastructure and key asset protection, the next step is to determine how to begin a proactive protection strategy. Every possible terrorist target cannot be protected from every possible contingency. Resources preclude such an "all hazards" approach. Enveloping all critical infrastructures and key assets in layers of security is simply not practical. Commerce would suffer, and civil liberties would be increasingly constrained and threatened. Everything cannot—and should not—be made into Fort Knox.

There is no simple solution. However, risk management can be seen as the most appropriate model with which to approach critical infrastructure and key asset protection. Under a risk management rubric, possible targets are analyzed according to a combination of three metrics: threat, vulnerability, and conse-

---

105. Electricity Modernization Act of 2005, Pub. L. No. 109-58, § 1211, 119 Stat. 594, 941–46 (2005).

106. *Id.*

107. *Id.*

108. Press Release, Fed. Energy Regulatory Comm., NERC Certified as Electric Reliability Organization; Western Region Advisory Board Accepted (July 20, 2006), *available at* http://www.ferc.gov/press-room/press-releases/2006/2006-3/07-20-06-E-5.pdf.

109. Department of Homeland Security Appropriations Act of 2007, Pub. L. No 109-295, 120 Stat. 1355 (2006).

110. *Id.* § 550(a).

111. *Id.*

quence.[112] Sites with a high threat level that are especially vulnerable to an attack that would result in severe consequences would receive the greatest protection. Thus, a chemical facility located near an urban center would receive much more security than a bridge in the rural Midwest. Unlike the rural bridge, the chemical plant is a high value target (high threat) which is susceptible to attack (high vulnerability). Such an attack would result in a large number of deaths (high consequence). Homeland Security Secretary Michael Chertoff has publicly embraced the risk management model to allocate the DHS resources and technologies and has crafted DHS-wide policies—including the National Infrastructure Protection Plan—to effectuate it.[113]

Moving risk management from construct to practice requires both the application of appropriate concepts of risk and the development of means to address such risk. It is here that the role of science and technology is most evident. Whether for understanding the threats, addressing the vulnerabilities, or mitigating the consequences, science and technology are being used to light the path ahead.

The government's homeland security technology pipeline has provided new tools to apply a risk management framework to critical infrastructure and key asset protection. For example, Sandia National Laboratories has lent its expertise to create systems to detect chemical weapons and explosives.[114] Through its Security Risk Assessment Methodologies, Sandia has conceptualized risk management to safeguard critical infrastructure sectors including chemical, energy, and water.[115] In another example, the Idaho National Laboratory's Critical Infrastructure Test Range offers a unique facility that "encompasses a collection [of] specialized test beds and training complexes that create a centralized location where government agencies, utility companies, and military customers can work together to find solutions for many of the nation's most pressing security issues."[116] The Test Range even boasts independent power, water, and telecommunications infrastructures which can be used to test homeland security technologies against realistic scenarios.[117]

---

112. Interview by Tim Russert with Michael Chertoff, Secretary, U.S. Dep't of Homeland Sec., in Washington, D.C. (July 10, 2005), *available at* http://www.msnbc.msn.com/id/8471990/print/1/displaymode/1098.

113. Michael Chertoff, Secretary, U.S. Dep't of Homeland Sec., Remarks at the 2005 Excellence in Government Conference (July 25, 2005), *available at* http://www.dhs.gov/xnews/speeches/speech_0256.shtm.

> We have to, with our finite resources and our finite number of employees . . . focus ourselves on those priorities which most demand our attention. And that means we have to focus on risk. And what does that mean? It means we look to consequence, it means we look to vulnerability, and it means we look to threat.

Id.

114. Sandia Nat'l Labs., Defense Against Chemical and Biological Threats, http://www.sandia.gov/mission/homeland/chembio (last visited Apr. 17, 2007).

115. Sandia Nat'l Labs., Security Risk Assessment Methodologies, http://www.sandia.gov/ram (last visited Apr. 17, 2007).

116. Idaho Nat'l Lab., National Security, http://www.inl.gov/nationalsecurity/criticalinfrastructure (last visited Apr. 17, 2007).

117. *Id.*

Because law and policy demand solutions to counterterrorism challenges, innovations developed at Sandia or on the Test Range have never been more important. The Security and Accountability for Every (SAFE) Port Act of 2006 requires, among other things, that "integrated scanning systems are fully deployed to scan, using nonintrusive imaging equipment and radiation detection equipment, all containers entering the United States . . . ."[118] Deploying this equipment will not occur without technologically driven solutions, especially those offered by the private sector.

Toward this end, Congress has offered incentives to spur private sector homeland security technology development. The Support Anti-Terrorism by Fostering Effective Technologies (SAFETY) Act provides liability and litigation management protection for companies that develop homeland security technologies.[119] The SAFETY Act's July 2006 Final Rule permanently effectuates the liability protection afforded by the law and clarifies the program's administration within DHS.[120]

It has been more than five years since 9/11. Much has changed. Homeland security has improved—and continues to improve—in significant areas. The fact that America has not been struck again is, in part, a testament to the measures that have been implemented successfully. The convergence of law and policy—with important contributions from science and technology—continue to shape the homeland security landscape, and few doubt that critical infrastructure and key asset protection will remain at the forefront. Despite the progress that has been made, attacks around the world demonstrate that terrorists remain capable and well organized. We must continue to prepare for what may be yet to come.

118. Security and Accountability for Every Port Act of 2006, Pub. L. No 109-347, § 232, 120 Stat 1884 (2006).

119. DHS SAFETY Act, http://www.safetyact.gov (last visited Apr. 17, 2007).

120. Regulations to Support Anti-terrorism by Fostering Effective Technologies Act of 2002 (SAFETY Act), 6 C.F.R. §§ 25.1–.10 (2007).