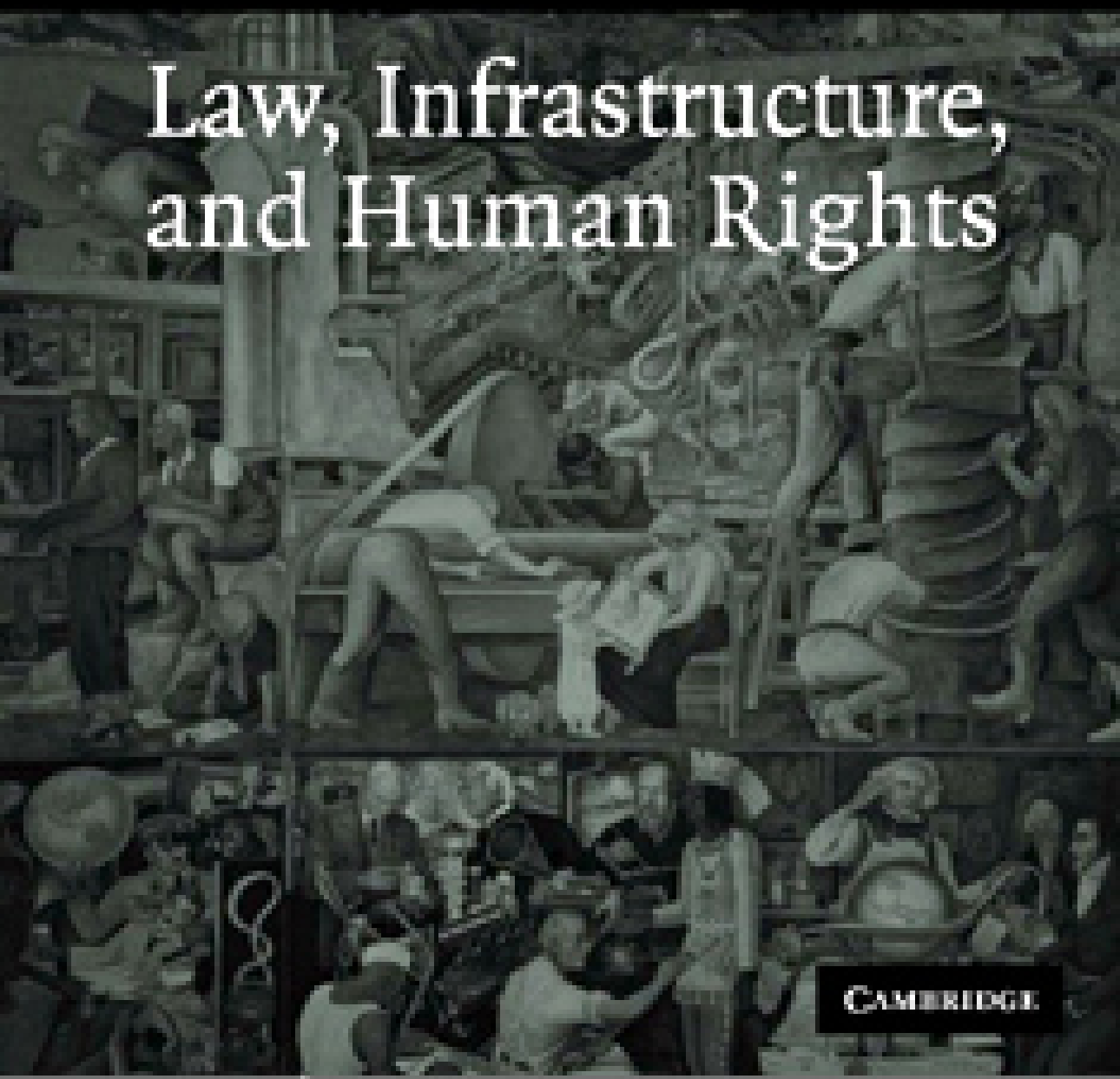
§Law in Context

MICHAEL B. LIKOSKY

Law, Infrastructure, and Human Rights



CAMBRIDGE

CAMBRIDGE www.cambridge.org/9780521859622

5

Antiterrorism

I Introduction

Terrorists persistently single out infrastructure projects for attack. Al-Qaeda operative-controlled airplanes struck the World Trade Center dealing a blow to the U.S. banking and financial infrastructure. With the bombing of the Spanish commuter trains and the U.K.'s tube and bus system, the countries' transportation infrastructures were a target. The anthrax scare in the United States commandeered the postal infrastructure. Every indication is that infrastructures will continue to be an important battlefield for attack and defense.[1] Richard A. Clarke, former Chairman of the U.S. Critical Infrastructure Protection Board, tells us: "Before Sept. 11, [al-Qaeda] was interested in killing as many people as possible . . . After Sept. 11, [Osama bin Laden] starts talking about going after the economic infrastructure of the United States."[2] The FBI has reinforced this.[3] And, Hamad Ressam, a terrorist suspect, identified oil infrastructure as a site of future attacks.[4] Responding to the targeting of infrastructures, governments are devising counterterrorism strategies.

Although conventional warfare prefers to avoid civilian targets, the terrorist military campaign nonetheless shares much in common with its tactics. Infrastructure projects are a basic target of modern air-powered wars.[5] The Kosovo and 1991 Iraq wars evidence this.[6] However, although conventional warfare strikes at "dual use"

1 M McDougal "International Law, Power and Policy: A Contemporary Conception" (1954) 82 Recueil Des Cours 1, 176.

2 Quoted in D Verton "Cyberthreats Not to be Dismissed, Warns Clarke" (6/1/03) 37(1) Computerworld 10.

3 "Ensuring Supply Safety" (May 2003) 95(5) National Petroleum News 14.

4 M A Gips "What's in the Pipeline" 47(8) Security Management 62.

5 For a discussion of civilian infrastructures and military attack *see* R W Gehring "Protection of Civilian Infrastructures" (1978) 42(2) Law and Contemporary Problems 86.

6 M L Cornell "Comment: A Decade of Failure: The Legality and Efficacy of United Nations Actions in the Elimination of Iraqi Weapons of Mass Destruction" (2001) 16 Connecticut Journal of International Law 325; R A Falk "Editorial Comments: NATO's Kosovo Intervention: Kosovo, World Order, and the Future of International Law" (October 1999) 93 American Journal of International Law 847; R Normand and C A F Jochnick "The Legitimation of Violence: A Critical Analysis of the Gulf War" (1994) 35 Harvard International Law Journal 387; C A Robbins and T E Ricks "Gloves Off: How NATO Decided It Was Time to End Its 'Gentlemanly' War – Milosovic's Resolve Spawned More Unity in Alliance And a Wider Target List – The Value of a Rembrandt" Wall Street Journal (Eastern edition) (4/27/1999) A1.

targets, the terrorist attacks single out civilian targets. "Dual use" infrastructures are ones that serve both civilian and military purposes.[7] Conventional warfare aims to strike at primarily military targets, recognizing that there may be civilian consequences. Thus, although the 1991 Iraqi war devastated infrastructure, according to U.S. General Norman Schwarzkopf, "[w]e never had any intention of destroying 100 percent of all the Iraqi power." He continues, "[b]ecause of our interest in making sure that civilians did not suffer unduly, we felt we had to leave some of the electrical power in effect, and we've done that."[8] However, in terrorist military campaigns, the battlefield is civilian.

How then is fire returned and how is territory protected? Although the battle in Afghanistan returned the fire by bringing the war overseas, the protection of home state territory is being coordinated through law by public-private partnerships (PPPs) made up of governments and infrastructure companies. With attacks on infrastructures, civilians often stand in the line of fire, thus human rights are at stake. The focus of this chapter is primarily on privatized projects, recognizing that terrorists also may target public infrastructures as was the case in Spain and the United Kingdom.

This chapter first looks at how infrastructure projects have become an important battlefield for terrorist and antiterrorist activity. It then turns to specific responses to terrorist attacks by governments and companies. Responses have been premised on the partnering of governments and companies. These partnerships receive attention in varied contexts, including U.S. institutional responses, information-sharing programs, cyberterrorism, and insurance-based responses.

II Infrastructure as battlefield

Why do attacks on infrastructure projects figure prominently in the terrorist arsenal? Clearly, terrorists are taking a page out of the lesson plan of conventional warfare. Infrastructures were targets in World War II, Kosovo, Iraq, and in other military campaigns.[9] In Yugoslavia, the North American Treaty Organization (NATO) forces

7 For a discussion of "dual use" facilities *see* H Shue and D Wippman "Limiting Attacks on Dual-Use Facilities Performing Indispensable Civilian Functions" (2002) 35 Cornell International Law Journal 559.

8 Quoted in G A Lopez "The Gulf War: Not So Clean" The Bulletin of the Atomic Scientists (September 1991) 30, 31. For a discussion of the most recent Iraq campaign and infrastructure projects see the previous chapter.

9 *See e.g.* M Lippman "Aerial Attacks on Civilians and the Humanitarian Law of War: Technology and Terror from World War I to Afghanistan" (Fall 2002) 33 California Western International Law Journal 1; T A Keaney "Surveying Gulf War Airpower" (Autumn 1993) Joint Force Quarterly 25; B H Weston "The Gulf Crisis in International and Foreign Relations Law, Continued: Security Council Resolution 678 and Persian Gulf Decision Making: Precarious Legitimacy" (1991) 85 American Journal of International Law 516; A Roberts "NATO's 'Humanitarian War' over Kosovo" (Autumn 1999) 41(3) Survival 102; Captain Y J Zacks "Operation Desert Storm: A Just War?" (January 1992) Military Review 30; D L Byman and M C Waxman "Kosovo and the Great Air Power Debate" (2000) 24(4) International Security 5; N G Fotion "The Gulf War: Cleanly Fought" The Bulletin of

bombed "key roads and bridges," [10] oil refineries, railways, airports, and communications lines. They "disabled the national power grid."[11] The 1991 Iraq war involved targeting communications, transportation, power, and water infrastructures.[12] Furthermore, with the ascendancy of network-based warfare, the U.S. military is developing ways of disarming enemy infrastructure networks through pinpointed attacks on the communication infrastructure.[13]

As indicated, the justification of targeting "dual use" infrastructures lies in their military characteristics.[14] Nonetheless, even in conventional warfare, given the "dual" quality of infrastructures, controversy exists over what is an appropriate target.[15] Commentators are divided on whether the targeting of "dual use" infrastructures is justifiable.

One the one hand, proponents of the targeting of "dual use" infrastructures are many and vocal. Nicholas G. Forton takes a broad view of appropriate targets:

> Infrastructure serves both civilians and the military. Both need bridges, highways, communications facilities, and power supplies. In most interpretations, the principle of discrimination does not say that a military force may attack only military targets. Unfortunately, this distinction can be difficult. Still, bridges needed by military forces in war are proper targets even though the same bridge may be used by civilians. Even bridges not normally used by the military may be used at a crucial point in the war. To argue otherwise is to ask the attacking military to restrict its activities to the point of risking defeat or prolonged war. The principle of discrimination was not intended to ask a military force to take such risks.[16]

the Atomic Scientists (September 1991) 24; G A Lopez "The Gulf War: Not So Clean" The Bulletin of the Atomic Scientists (September 1991) 30; R Normand and C A F Jochnick "The Legitimation of Violence: A Critical Analysis of the Gulf War" (Spring 1994) 35 Harvard International Law Journal 49.

10 D L Byman and M C Waxman "Kosovo and the Great Air Power Debate" (2000) 24(4) International Security 5, 18.

11 *Id.*

12 N G Fotion "The Gulf War: Cleanly Fought" The Bulletin of the Atomic Scientists (September 1991) 24, 26, 28.

13 E T Jensen "Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense" (2002) 38 Stanford Journal of International Law 207; M J Robbat "NOTE: Resolving the Legal Issues Concerning the Use of Information Warfare in the International Forum: The Reach of the Existing Legal Framework, and the Creation of a New Paradigm" (Spring 2001) 6 Boston University Journal of Science and Technology Law 10; J P Terry "The Lawfulness of Attacking Computer Networks in Armed Conflict and in Self-Defense in Periods of Short Armed Conflict: What are the Targeting Constraints?" (9/01) 169 Military Law Review 70.

14 N G Fotion "The Gulf War: Cleanly Fought" (September 1991) The Bulletin of the Atomic Scientists 24, 28.

15 C C Joyner "Reconciling Political Sanctions with Globalization and Free Trade: United Nations Sanctions after Iraq: Looking Back to See Ahead" (Fall 2003) 4 Chicago Journal of International Law 329; R W Gehring "Protection of Civilian Infrastructure" (1978) 42 Law and Contemporary Problems 95; H Shue and D Wippman "Limiting Attacks on Dual-Use Facilities Performing Indispensable Civilian Functions" (Winter 2002) 35 Cornell International Law Journal 559.

16 N G Fotion "The Gulf War: Cleanly Fought" (September 2001) The Bulletin of the Atomic Scientists 24, 28.

Similarly, U.S. Army Captain Yuval Joseph Zacks tells us that although "[d]estruction of an opponent's infrastructure is problematic in moral terms," "a strong argument can be made for the destruction of an infrastructure."[17] He goes on to say: "Today's military technology relies heavily on the components of most nations' infrastructures."[18] Military campaigns can thus, according to Captain Zacks, take "a heavy toll on the civilian populace."[19] They can result in "[u]nsanitary conditions and disease proliferat[ion]. Famine may erupt, and medical care may be discontinued."[20] Regardless, Fotion argues, with reference to the 1991 Iraq war, that damages to infrastructure happen in war for reasonable reasons and thus bombing decisions should not be "second-guessed."[21]

On the other hand, some commentators sharply criticize the liberal targeting of "dual use" infrastructures. For example, one United Nations team called the damage caused by the 1991 Iraq war campaign's targeting of infrastructures "near apocalyptic."[22] Also, large-scale attacks on "dual use" infrastructure targets can cause serious problems in the postwar delivery of humanitarian aid. As we saw in the previous chapter, one of the purposes of the first contract between the U.S. government and Bechtel was to rehabilitate the country's infrastructure so that humanitarian aid could be delivered.

Rather than being indifferent or opposed to damage caused to the civilian aspects of infrastructures by military campaigns, terrorist attacks make civilian targets the cornerstone of their own brand of warfare.[23] At the same time, to notice that terrorists single out civilian infrastructures does not explain why they do so.

The observation that terrorists single out civilian infrastructures for attack is not only one of academic speculation. In the USA PATRIOT Act, perhaps the most important piece of post-9/11 antiterror legislation, the government sets out "critical national infrastructure" as a legal category encompassing targeted infrastructures. This category includes "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, national public health or safety, or any combination of these matters."[24] National infrastructures are "critical" when they affect "national-level public health and safety, governance, economic and national security, and public confidence."[25] The specific types of

17 Captain Y J Zacks "Operation Desert Storm: A Just War?" (January 1992) Military Review 30, 33.
18 *Id.*
19 *Id.*
20 *Id.*
21 N G Fotion "The Gulf War: Cleanly Fought" (September 1991) The Bulletin of the Atomic Scientists 24, 28.
22 G A Lopez "The Gulf War: Not So Clean" (September 1991) The Bulletin of the Atomic Scientists 30, 33–34.
23 Economic sanctions at times, in effect, single out civilians. C C Joyner "Reconciling Political Sanctions with Globalization and Free Trade: United Nations Sanctions after Iraq: Looking Back to See Ahead" (2003) 4 Chicago Journal of International Law 329; S J Lukaski, L T Greenberg and S E Goodman "Protecting an Invaluable and Ever-Widening Infrastructure" (June 1998) 41(6) Association for Computing Machinery 11, 11–12.
24 42 USC. 5195(e).
25 *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets.*

infrastructures included within this category will vary with time. Presently, the United States categorizes the following as "critical national infrastructures": agriculture and food, water,[26] public health, emergency services, defense industrial base, telecommunications, energy, transportation, banking and finance, chemicals and hazardous materials, and also postal and shipping.[27] Despite the broadness of this category, traditional infrastructures such as nuclear power and dams are classified as "key assets" rather than as infrastructures.[28] So, the category of infrastructure project is itself statutorily determined and both broad and underinclusive in the U.S. case. Furthermore, the definition of "critical national infrastructure" varies from country to country. What is important, however, is that in response to terrorist attacks on infrastructures, governments are making infrastructures a special legal class with attendant protections.

The fact that the category of "infrastructure" is legally constructed and varies from country to country is made even more variable because infrastructures themselves are often transnational. For example, infrastructures such as banking and finance, power, gas and oil, and also telecommunications can be transnational.[29] For example, much of the natural gas consumed in the United States is extracted in Canada. This transnationalism not only confuses legal definitions of infrastructures, but it also makes the United States vulnerable to attacks on Canadian-based infrastructures. For example, Matt Morrison, the Vice President of PNWR, informs us: "The loss of one specific core station, the identity of which can't be disclosed for security reasons, could severely impact the flow of natural gas in the U.S."[30] As well, it is projected that, by the year 2020, "two-thirds of all oil in the United States will be imported."[31] Thus, responses often must involve public and private entities of more than one country. For this reason, legislation of multiple countries is often germane to the protection of a single infrastructure project.

This need for a transnational response to protect transborder infrastructures is being met in certain contexts. For example, the United States and Canada have joined together to protect transnational infrastructures. In particular, the governments of Alaska, Idaho, Montana, Oregon, Washington, Alberta, British Columbia, and the Yukon Territory have come together "under the auspices of the Pacific Northwest Economic Region, a Seattle-based organization of government and business

26 On national and local responses in the U.S. to threats of terrorist attacks on water infrastructure *see* I E Kornfeld "Combatting Terrorism in the Environmental Trenches: Responding to Terrorism: Terror in the Water: Threats to Drinking Water and Infrastructure" (2003) 9 Widener Law Symposium 439.

27 *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* xii.

28 *Id.* 74–76.

29 S J Lukaski, L T Greenberg and S E Goodman "Protecting an Invaluable and Ever-Widening Infrastructure" (June 1998) 41(6) Association for Computing Machinery 11, 13. On the global telecommunications infrastructure *see* H E Hudson *Global Connections: International Telecommunications Infrastructure and Policy* (Van Nostrand Reinhold New York 1997).

30 D Verton "Critical Infrastructure Systems Face Threat of Cyberattacks" (7/1/02) 36(2) Computerworld 8.

31 M A Gips "Gas and Electric Companies Address Risks" (September 1999) 43(9) Security Management 15.

officials."[32] They are presently in the process of mapping the transborder infrastructures and devising plans to respond to threats of attack.[33] Furthermore, responses in the past also have moved beyond the bilateral and to the multilateral. For example, the International Civil Aviation Organization has coordinated international responses to terrorist threats to the transnational aviation network.[34]

Internationally, many protected infrastructure projects are privatized.[35] Although U.S. Senator Robert Bennett, a Republican from Utah, has said, "the future battlefield is in private, not public hands,"[36] as we saw in Chapter 2, privatized projects are in actuality public-private partnerships. Thus, even though over eighty-five percent of U.S. infrastructures are privatized, this does not mean that the government does not either own or partially control projects. If targeted projects are PPPs, does this mean that al-Qaeda and other terrorists are singling out these government-company partnerships for attack? Are they targeting private interests? Do they see private property as national property?

When terrorists attack PPP-based infrastructures in developing countries, it is generally understood that specific governments and transnational corporations are being singled out. For example, oil pipelines are often targeted. Thus, Ed Badolato, Executive Vice President for Homeland Security at the Shaw Group, tells us: "Although pipelines haven't been attacked by terrorists in the United States, the risk of pipelines is more than conjecture."[37] Badolato goes on, "[t]hey are the preferred target elsewhere in the world, especially Columbia."[38] Attacks are directed at the joint enterprise of developing country governments and transnational oil companies. The response has sometimes been to deploy the military.[39] The lessons learned in developing countries are in the process of being transposed to fully industrialized countries. As American Gas Association President David Parker notes, companies "are already used to working in 'hostile' business environments across the world and are prepared to meet new challenges on U.S. soil."[40]

If it is common sense that governments and companies are targets when terrorists attack infrastructures in developing countries, then does this also hold true when

32 R Gavin "Regional Report: States Join to Prepare for Disasters" Wall Street Journal (Eastern edition) (12/12/01).

33 *Id.*

34 S J Lukaski, L T Greenberg and S E Goodman "Protecting an Invaluable and Ever-Widening Infrastructure" (June 1998) 41(6) Association for Computing Machinery 11, 16. On government efforts to combat terrorist attacks on aviation *see* M Lippman "ESSAY: The New Terrorism and International Law" (Spring 2003) 10 Tulsa Journal of Comparative and International Law 297; A F Lowenfeld "Special Issue: The United States Constitution in Its Third Century: Foreign Affairs: Constitutional Law – International Law: U.S. Law Enforcement Abroad: the Constitution and International Law" (October 1989) 83 American Journal of International Law 880.

35 Importantly, as indicated above, attacks on public infrastructures are an important species.

36 Quoted in S E Roberts and T C Wingfield, "Homeland Security's Legal Battleground" (November 2003) 35(16) Government Executive 64.

37 Quoted in M A Gips "What's in the Pipeline" 47(8) Security Management 62.

38 *Id.*

39 A L Cantillo "Project Finance in Colombia" [April 1996] International Financial Law Review 24.

40 Quoted in M Lorenzetti "U.S. Energy Infrastructure Security Now a Key Issue in Washington" (10/1/01) 99(40) Oil & Gas Journal 22.

infrastructures are targeted in fully industrialized countries? Terrorists do not often vocalize the rationale for their targeting decisions. Nonetheless, the targeted infrastructures in fully industrialized countries are often, just as in developing countries, PPPs. Furthermore, infrastructures also may have a transnational dimension. For example, the targets of the September 11, 2001, attacks were on the property of domestic and transnational corporations as well as the U.S. government. Several of the companies housed in the World Trade Center were transnational in orientation. And, terrorists also chose a government target, the Pentagon. Were terrorists connecting the public and private sites that they attacked? Craig Calhoun suggests: "Al Qaeda dramatically linked American military power and global finance capitalism in simultaneous attacks on the Pentagon and the World Trade Center."[41] If this was the case, then why?

Governments explain the rationale behind terrorist attacks on specific sites in various ways. Typically, attacks are presented as targeting the general public. At the same time, the legislative responses aim to protect private property. The government downplays the importance of the targeting of private property by terrorists. Instead, the government argues that attacks aim to undermine the American way of life. U.S. President George Bush on the evening of the terrorist attacks of September 11th opened his address to the American people by speaking of the attacks on "our way of life" by "a series of deliberate and deadly terrorist attacks."[42]

The U.S. government shifts mainly the inquiry away from the reasons for the attacks and toward their effects. It identifies three types of effects of terrorist attacks on critical national infrastructures:

- *Direct infrastructure effects*: Cascading disruption or arrest of the functions of critical infrastructures or key assets through direct attacks on a critical node, system, or function.
- *Indirect infrastructure effects*: Cascading disruption and financial consequences for government, society, and economy through public- and private-sector reactions to an attack.
- *Exploitation of infrastructure*: Exploitation of elements of particular infrastructure to disrupt or destroy another target.[43]

Although the identified reasons for and effects of attacks have implications for civilians, the PPP-based responses tend not to involve the public. Should we look holistically at the choice of targets of attacks, the reasons for attacks, and the effects of attacks? Should decisions about how to respond to attacks be tailored to the terrorists' rationale for choosing certain targets?

41 C Calhoun "Social Science and the Crisis of Internationalism: A Reflection on How We Work after the War in Iraq" http://www.ssrc.org/president_office/crisis_of_internationalism.page.

42 "Statement by the President in his State of the Union Address" http://www.whitehouse.gov/news/releases/2001/09/20010911-16.html.

43 *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* (February 2003) viii.

III PPPs as antiterror tactics

Regardless of whether terrorists are targeting governments, companies, or nations, the governments and companies who control the PPPs under attack or threat of attack are responding by protecting their common property. For them, their joint assets are under fire. The response is to form a variety of PPPs to lessen the risk and to minimize the damage from any further attacks. For example, PPPs have been the chosen response in a number of areas, including, the U.S. institution-based response generally, in information-sharing programs, in responses to cyberterrorism, and in the insurance sector.

A U.S. institutional response

In U.S. President George W. Bush's "Preface" to *The National Strategy for the Physical Protection of Critical Infrastructures and Assets*, he says that the response to the terrorist attacks must include "government at all levels, the private sector, and concerned citizens across the country."[44] The plan conjures the support of citizens at several other points. For example, it says that the nation "must draw upon the resources and capabilities of those who stand on the new front lines – our local communities and private sector entities that comprise our national critical infrastructure sectors."[45] Nonetheless, at the institutional level, the United States has pursued PPPs that exclude the public writ large in responding to terrorist threats to its critical national infrastructures. By and large, partnerships are between the government and companies.

PPPs pervade the government's response to the terrorist attacks. *The National Strategy* states: "A solid organizational scheme sets the stage for effective engagement and interaction between the public and private sectors at all levels."[46] It seeks "ongoing collaboration among relevant public- and private-sector stakeholders" in carrying forth this paradigm of partnership.[47] The nature of the proposed relationship between the public and private sector is made explicit:

> We must also build and foster a partnership among all levels of government, as well as between government and the private sector. This public-private partnership should be based on a commitment to a two-way communication flow and the timely exchange of information relevant to critical infrastructure and key asset protection. This partnership should also extend to the research, development, and fielding of advanced technology solutions to common protection problems. Collaborative efforts should also include the development and sharing of modeling and simulation capabilities to enable public-private sector decision support and interdependency analysis.[48]

44 G. W. Bush "Preface" to *id.*
45 *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* 3.
46 *Id.* ix.
47 *Id.* 8.
48 *Id.* 82.

This mode of responding dates back to actions taken under the Clinton administration. In line with *The National Strategy*, states and private companies have pursued parallel and mutually reinforcing strategies premised on PPPs.

At the state and provincial levels in the United States and Canada, governments and companies are pursuing PPPs. Governments and companies from Alaska, Idaho, Montana, Oregon, Washington, Alberta, British Columbia, and the Yukon have been particularly proactive.[49] Industry groups also have encouraged PPP solutions with notable efforts from the American Gas Association, the American Petroleum Institute, the Edison Electric Institute,[50] and the American Society of Civil Engineers.[51]

The foundations of the Bush Administration's PPP approach was laid during the Clinton presidency. This was, of course, before the attacks of September 11. The Clinton administration's PPP approach also took an institutionally-based form.

In 1998, the Clinton administration issued a white paper, *The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63* (PDD63), detailing its response to threats of terrorism to the country's critical national infrastructures.[52] Japan, at the time, pursued a similar course.[53] In important respects, the Bush administration's strategy builds on the Clinton approach. At the same time, the Bush strategy departs in significant ways.

PDD63 pursued a variety of PPP-based institutional approaches. It did so because of the ownership spread of U.S. infrastructures that had resulted from the privatizations discussed in Chapter 2. Accordingly, PDD63 made clear: "Since the targets of attacks on our critical infrastructure would likely include both facilities in the economy and those in government, the elimination of our potential vulnerability requires a closely coordinated effort of both the public and private sectors."[54] PDD63 thus argues: "the protection of our critical infrastructures is necessarily a shared responsibility and partnership between owners, operators and the government."[55] So, the Clinton PPP-based solution lies at the base of the Bush administration approach.

Clinton responded to the terrorist threat with PPPs in a variety of ways. For example, he appointed lead government agencies to liase with key officials in the private sector. In addition, he established a National Infrastructure Assurance Council made

49 R Gavin "Regional Report: States Join to Prepare for Disasters" Wall Street Journal (Eastern edition) (12/12/01).

50 M Lorenzetti "U.S. Energy Infrastructure Security Now a Key Issue in Washington" (10/1/01) 99(40) Oil & Gas Journal 22.

51 N Post "Civil Engineers Look for Ways to Mitigate Effects of Disasters" (10/22/01) 247(17) Engineering News Round.

52 *White Paper: The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63* (5/22/98) (*PDD63*).

53 S.J Lukaski, L T Greenberg and S E Goodman "Protecting an Invaluable and Ever-Widening Infrastructure" (June 1998) 41(6) Association for Computing Machinery 11.

54 *PDD63.*

55 *Id.*

up of members of the public and private sectors to oversee responses. Also, a PPP was formed under the umbrella of the Federal Bureau of Investigation (FBI) as the National Infrastructure Protection Center, comprising thirty top executives.[56] The governments of Australia, Canada, the United Kingdom, Sweden, and New Zealand established similar agencies. Some of these agencies had formal links with the FBI Center, which has now been integrated into the Department of Homeland Security.[57] The Clinton administration also sought to expand its list of public-private partners to include foreign governments and transnational corporations.[58]

In many ways, the Bush administration matures the Clinton PPP-based approach. At the same time, the Bush administration has made important innovations, some of which are borrowed from a Heritage Foundation report.[59] Within the administration, the protection of critical national infrastructures is primarily organized under the Department of Homeland Security. This is the most significant difference from the Clinton Directive. The Department was established in 2002. It is charged with the "overall cross-sector coordination" of the "organizational scheme, serving as the primary liaison and facilitator for cooperation among federal agencies, state and local governments, and the private sector."[60] Before the establishing of this Department, PDD63 organized critical national infrastructure protection on a sector-specific basis with various government agencies responsible on an individual basis for oversight of respective sectors.

Bush maintains the PPP-basis of the Clinton approach, while innovating at the organizational level. One principle that runs throughout the Bush administration response to threats of terrorist attacks on critical national infrastructures is the need to "[e]ncourage and facilitate partnering . . . between government and industry."[61] Such collaboration is to be based upon "a culture of trust."[62] The Bush administration's Executive Order 13231 reinforces the PPP approach and establishes the President's Critical Infrastructure Protection Board to consult with the private sector. It also established the National Infrastructure Advisory Council to "enhance the partnering of the public and private sectors."[63]

Also, the Bush administration reaffirms the idea of a National Infrastructure Advisory Council to offer the President advice on "the security of information systems for critical infrastructure".[64] Membership of this Council is drawn from

56 D Verton "Feds Ask Business Leaders to Help Protect Infrastructure: 30 Top Executives to Serve on National Advisory Council" (10/22/01) 35(43) Computerworld 8.
57 E McCartney-Smith and N B Tanner "How Does the USA PATRIOT Act Affect International Business" [2002] The Journal of Corporate Accounting and Finance 23, 25.
58 *PPD63* (5/22/98).
59 Heritage Foundation, *The Heritage Foundation Homeland Security Task Force* (January 2002).
60 *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* (February 2003). *See also* 17.
61 *Id.* ix.
62 *Id.* 8.
63 "Critical Infrastructure Protection in the Information Age," Executive Order 13231 (10/16/01).
64 Executive Order 13286, Section 3 (2/28/03); *see also* D Verton "Feds Ask Business Leaders to Help Protect Infrastructure: 30 Top Executives to Serve on National Advisory Council" (10/22/01) 35(43) Computerworld 8.

government, the private sector, and academia.[65] Its goals affirm the PPP approach. They are:

> (1) to enhance the partnering of public and private sectors, (2) to encourage the private sector to undertake risk assessments, (3) to monitor the private sector's Information Sharing and Analysis Centers, (4) advise agencies on critical national infrastructure responsibilities.[66]

Thus, the Council promotes close intermingling of the public and private sector.

In addition, in the areas of telecommunications and energy, the government has created several PPP-based organizational forms. With regard to telecommunications, organizations include the President's National Security Telecommunications Advisory Committee and Critical Infrastructure Protection Board, the Government Network Security Information Exchanges, the Telecommunications Information Sharing and Analysis Centers, and also the Network Reliability and Interoperability Council of the Federal Communications Commission.[67] With respect to energy, the North American Electricity Reliability Council has been established by public and private entities in the United States and Canada. The Council "coordinates programs to enhance security for the electricity industry."[68] In doing so, it builds upon the transnational character of the Clinton administration approach.

Furthermore, the government employs its police powers to safeguard privatized infrastructures from terrorist attack. These so-called first responders date back to the Defense Against Weapons of Mass Destruction Act of 1996.[69] That Act provided training for first responders to terrorist attacks using weapons of mass destruction. The U.S. Department of Defense provides this training.[70] It has been extended with the Department of Homeland Security, which allocates general money to protect infrastructures from attacks along with money also being provided by the Office for Domestic Preparedness.[71] The money earmarked for first responders is mainly for urban areas and also does not limit itself to infrastructure protection.

So a glimpse at the institutional response in the United States highlights the underlying logic of PPPs. We also see these partnerships in the area of information sharing. At the same time, there governments and companies are sometimes at loggerheads.

B Information sharing

Governments are urging private companies to share information with them in order to assess vulnerabilities to terrorist attacks. For example, the European Union passed

65 Executive Order 13286 Section 3(a).
66 *Id.* 3(b).
67 *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* 48 (February 2003).
68 *Id.*
69 50 U.S.C. 2301.
70 B Wade "Terrorism Response: Preparing for the Worst" (November 2001) 116(17) The American City and County 20, 21.
71 "Is More Money Going to Big City First Responders?" (May 2003) 65(5) Occupational Hazards.

a directive allowing member countries "to require telecommunications and Internet companies to track and provide data about customers' e-mail, Internet usage, and phone calls to law enforcement agencies."[72] Similarly, the United Kingdom set up a National Hi-Tech Crime Unit. This Unit gathers information and runs a national hotline. It has caused some controversy among civil liberties groups.[73] Although information sharing is premised on PPPs, the relationship between sectors is not always amicable and cooperative.

Companies are reluctant to share information with governments for a variety of reasons, including a fear that information will end up in the hands of competitors and also that members of the public might use information to instigate civil actions. Also, companies are concerned that full information disclosure might lead to a confidence problem similar to that faced during the global depression in the early twentieth century.[74] The U.S. government seeks to allay these fears by promising to shield information from public view so long as it is provided to the government in a specified manner. Although information sharing is an issue in many countries, this section focuses on the U.S. approach to information sharing and explores some of the issues that have arisen.

The U.S. government encourages the private sector to share information.[75] To this end, it established the Protected Critical National Infrastructure Information Program within the Department of Homeland Security.[76] The governing legislation is the Critical Infrastructure Information Act.[77] The purpose of the Act is to identify vulnerabilities in critical national infrastructures. The Act exempts certain information from the Freedom of Information Act.[78] In particular, the government shields voluntarily submitted information.[79] Such information must be accompanied by a statement by the applicant explicitly seeking to avail her or himself of the

72 T McCollum "Security Concerns Prompt New Initiatives" (October 2002) 59(5) The Internal Auditor 14.

73 T Corbit "National Hi-Tech Crime Unit" (February 2001) 45(2) Management Services 28, 29.

74 B D Nordwall "Cyber Threats Place Infrastructure at Risk" (6/30/97) 146(27) Aviation Week & Space Technology 51.

75 E McCartney-Smith and N B Tanner "How Does the USA PATRIOT Act Affect International Business" [2002] The Journal of Corporate Accounting and Finance 23, 24.

76 A Beadle "Homeland Security Introduces New Antiterrorism Program" (2/20/04) Journal of Commerce.

77 6 USC 131–134 (2002). On the Act *see* N Bagley "Benchmarking, Critical Infrastructure Security, and the Regulatory War on Terror" (2006) 43 Harvard Journal on Legislation 47; J Conrad "Protecting Private Security-Related Information Disclosure by Government Agencies" (2005) 57 Administrative Law Review 715; C Guttman-McCabe, A Mushahwar and P Murck "Homeland Security and Wireless Telecommunications: The Continuing Evolution of Regulation" [2005] Federal Communications Law Journal 413; K E Uhl "The Freedom of Information Act Post-9/11: Balancing the Public's Right to Know, Critical Infrastructure Protection, and Homeland Security" (2003) American University Law Review 261;R Steinzor "'Democracies Die Behind Closed Doors': The Homeland Security Act and Corporate Accountability" (2003) Kansas Journal of Law and Public Policy 641; B Stohs "Protecting the Homeland by Exemption: Why the Critical Infrastructure Information Act of 2002 Will Degrade the Freedom of Information Act" [2002] Duke Law & Technology Review 18.

78 5 USC 552 (2002).

79 PL108–296 Sec 212(7).

exemption.[80] Furthermore, the information must not be customarily in the public domain.[81] Traditionally, most information on utilities has been publicly available; however, after the attacks of September 11, governments and companies removed information from the public domain.[82] In addition, if federal, state, or local governments come to information separately for the purpose of a legal action, then companies may not be able to avail themselves of exemptions.

The Critical Infrastructure Information Act has caused controversy. The community group Common Cause calls the Act an "agenda of secrecy."[83] Community groups and news organizations argue that the exemptions have little to do with preventing terrorism. For example, they want plant safety issues to remain in public view.[84]

State regulators complain that the exemptions will make the task of regulating utilities more difficult.[85] Members of the Senate criticize the Act. Senator Patrick Leahy, a Democrat from Vermont, called the Critical Infrastructure Information Act "the single most destructive blow to [Freedom of Information Act] in its 36-year history."[86] To counter the exemptions, the Restoration of Freedom of Information Act was introduced into the Senate in 2002 and 2005. For their part, many industry officials are unhappy with a discretionary power remaining in the federal government to turn down certain requests for secrecy. They fear that competitors might obtain access to information on setting rates.[87]

The U.S. government also set up Information Sharing and Analysis Centers (ISACs) designed to facilitate close partnering between the public and private sectors in infrastructure safety. The Clinton administration established these Centers in 1988.[88] There are fifteen ISACs and they are industry specific.[89] These ISACs have been criticized within the present administration with the Government Accountability Office finding that they do not result in the full sharing of information, particularly in the energy sector. Sharing was hindered there by a fear that competitors or regulators would obtain information and use it to companies' detriment.[90]

Another mechanism for information sharing in the United States is a PPP between the government and infrastructure companies that sets up a secure telecommunications link among chief executive officers and government agencies. This is

80 *Id.* Sec 214(a)(2)(A)–(B).
81 *Id.* Sec 212(3).
82 J Gibeaut "The Paperwork on Terrorism" (October 2003) 89 ABA Journal 62.
83 S Zeller "Protection Money" (June 2003) 35(7) Government Executive 35.
84 *Id.*
85 J Gibeaut "The Paperwork on Terrorism" (October 2003) 89 ABA Journal 62.
86 Quoted in N Oder "FOIA Exemption May Be Fixed" (4/15/03) 128(7) Library Journal 18.
87 J Gibeaut "The Paperwork on Terrorism" (October 2003) 89 ABA Journal 62.
88 D Verton "Feds Ask Business Leaders to Help Protect Infrastructure: 30 Top Executives to Serve on National Advisory Council" (10/22/01) 35(43) Computerworld 8. These Centers date back to the Clinton administration. *White Paper: The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63* (5/22/98).
89 R Andrews "How Can Information Exchange Be Enhanced?" (6/03) 47(6) Security Management 162.
90 S Zeller "Protection Money" (6/03) 35(7) Government Executive 35.

the CEO COM Link, and it is designed to facilitate a public-private response to attacks.[91]

Thus, PPP-based solutions pervade information-sharing efforts. Although these partnerships seek close collaboration between sectors, at times, infrastructure companies are wary of them. Furthermore, some community groups have been staunchly opposed to them. Similar concerns infuse the debates over PPP-based government responses to cyberterrorism.

C Cyberterrorism

Governments and companies fear that cyberterrorists will target the information infrastructure.[92] According to Ron Dick, former director of the FBI's National Infrastructure Protection Center, "cyberterrorism is a criminal act perpetrated through computers resulting in violence, death and/or destruction, and creating terror for the purpose of coercing a government to change its policies."[93] Given the transnational nature of the Internet, the threat to the information infrastructure is a global one. For example, a successful attack in Canada could disable portions of the U.S. infrastructure.[94] The Internet is itself a PPP, a successful product of the privatization of military technology. The United States is the main force behind the Internet and thus this section focuses primarily to its efforts to safeguard the information infrastructure from attack.

In the "foreword" to *The National Strategy to Secure Cyberspace* President George W. Bush tells us: "The cornerstone of America's cyberspace security strategy is and will remain a public-private partnership."[95] Although mention is made of the importance of "the American people"[96] in safeguarding infrastructures, at the operational level, the response is one of narrowly conceived PPPs. The rationale for these partnerships is that they "can usefully confront coordination problems" and "significantly enhance information exchange and cooperation."[97] These partnerships "will take a variety of forms and will address awareness, training, technological improvements, vulnerability remediation, and recovery

91 C M Armstrong "United We Stand," Wall Street Journal (Eastern Edition) (3/9/04) B2.

92 On "information warfare" *see* J C Anselmo "U.S. Seen More Vulnerable to Electromagnetic Attack" (7/28/97) 147(4) Aviation Week & Space Technology 67; K Crilley "Information Warfare: New Battlefields Terrorists, Propaganda and the Internet" (June–August 2001) 53(7) Aslib Proceedings 250; Captain R G Hanseman, USAF "The Realities and Legalities of Information Warfare" (1997) 42 The Air Force Law Review 173; N Munro "Sketching a National Information Warfare Defense Plan" (1996) 39(11) Communications of the ACM 15; "NOTE: Discrimination In the Laws of Information Warfare" (1999) 37 Columbia Journal of Transnational Law 939; M J Robbat "NOTE: Resolving the Legal Issues Concerning the Use of Information Warfare in the International Forum: The Reach of the Existing Legal Framework, and the Creation of a New Paradigm" (2000) 6 Boston University Journal of Science and Technology Law 10; J P Terry "The Lawfulness of Attacking Computer Networks in Armed Conflict and in Self-Defense in Periods of Short Armed Conflict: What are the Targeting Constraints" (2001) 169 Military Law Review 70.

93 Quoted in S Berinato "The Truth about Cyberterrorism" (3/15/02) 15(11) CIO 66.

94 D Verton "Critical Infrastructure Systems Face Threat of Cyberattacks" (1/7/02) 36(2) Computerworld 8.

95 *The National Strategy to Secure Cyberspace* (President G W Bush "Foreword").

96 *Id.* vii.

97 *Id.* ix.

operations."[98] For example, several PPPs are being pursued including the Department of Homeland Security's Information Analysis and Infrastructure Protection Directorate, which oversees contingency plans. The *National Strategy* sets out the PPP-based approach. For example, it directs the Department of Homeland Security to create an office "to manage information flows"[99] between the public and private sectors. It instructs the Department of Homeland Security to pursue PPPs to foster security cooperation, to develop vulnerability disclosure with the private sector, to "share lessons learned with the private sector and to encourage the development of a voluntary, industry-led, national effort to develop a similar clearinghouse for other sectors including large enterprises,"[100] "to identify cross-sectoral interdependencies,"[101] to "promulgate best practices and methodologies"[102] for software, to create a task force on firewalls, and also to pursue international solutions.[103] Also, in 2003 the U.S. established the United States Computer Emergency Readiness Team, which "is a partnership between the Department of Homeland Security and the public and private sectors." It "coordinates defense against and responses to cyber attacks across the nation."[104] Furthermore, the United States has controversially attempted to extend its jurisdiction over the Internet to other countries with the aim of safeguarding it against terrorist attacks.[105]

Initially a government-generated communications infrastructure, the Internet has over time moved out of government hands. However, in response to threats of terrorism, the government has begun to explore the possibility of creating a parallel, proprietary, government-owned Internet. It was first proposed under the Clinton administration and referred to as Govnet. However, at the time, the United States decided that the plan was not practicable. Nonetheless, the recent terrorist attacks, led to a revival of discussions.[106]

98 *Id.*
99 *Id.* 55.
100 *Id.* 33.
101 *Id.* 56.
102 *Id.* 35.
103 *Id.* 55–59.
104 www.us-cert.gov/aboutus.html; "Cyberlaw: Additional Developments" (2006) 21 Berkeley Technology Law Journal 551, 565.
105 E McCartney-Smith and N B Tanner "How Does the USA PATRIOT Act Affect International Business" [2002] The Journal of Corporate Accounting and Finance 23, 25.
106 C Sewell "One Network, under GOV" (1/7/02) 242(1) Telephony 30. Chris Sewell tells us:

> The idea for Govnet first was knocked around during the Clinton administration but was dismissed at the time as impractical. It was revisited in the spring of 2001 and gained momentum following the attacks on New York and Washington. The Govnet concept also brings government communications full circle, harkening back 40 years to the Department of Defense's Advanced Research Project Agency Network (ARPANET), which evolved into the modern day Internet.
>
> After connecting researchers at four U.S. universities in 1969, a commercial version of ARPANET was launched in the late 1970s. By 1981, the network had 213 hosts with a new host added on average every 20 days, raising security and privacy concerns. By the following decade, the Internet was an essential public communications tool; but crushed under the weight of its own unexpected success, ARPANET was decommissioned in 1990, leaving behind the enormous network of networks that now links the world. *Id.*

Disagreement exists over how vulnerable the Internet is to terrorist attacks. On the one hand, many argue that the threat of attacks on the information infrastructure is serious. The Internet is transnational and thus vulnerable to attacks made abroad. Also, many other infrastructures are connected to the Internet. So, a successful striker could use the Internet as a launching pad for attacks on other infrastructures. Multiple infrastructures could simultaneously be shut down.

Universal access makes the Internet particularly vulnerable because of "unprotected holes . . . in the network fabric."[107] In other words, "cyber attacks use the patterns and characteristics of the net itself to propagate."[108] Furthermore, Richard Clarke, former Chairman of the Critical Infrastructure Protection Board, tells us:

> You could drive around a lot of truck bombs and really not do a lot of damage to the economic infrastructure because it's so diverse and dispersed. But if you do it in cyberspace, you might have the ability to hit the entire financial services network simultaneously.[109]

A report by the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction, or the Gilmore Commission, a congressional advisory board, argues that the Web is insecure and that the government response is inadequate.[110] The Report argues that the President's response is too geared toward voluntary private-sector measures.[111]

On the other hand, others argue that the threat of cyberterrorism is overblown. For example, the Center for Strategic and International Studies issued a report arguing that the threat has been exaggerated. In *Assessing the Risks of Cyber Terrorism, Cyber War, and Other Cyber Threats*, the Center argues that the government has made too much of the threat.[112] The report takes the position that the communications infrastructure is resilient because it is built on redundancies and regularly weathers outages.[113] Some point out that, even if terrorists are able to hack into the national information infrastructure, local networks also must be penetrated. These local networks are more difficult to access.[114]

Despite the back and forth, it is difficult to assess how an attack on the information infrastructure would affect other infrastructures.[115] The government is in

107 S McClelland "Feeling Globally Insecure" (June 2003) 37(6) Telecommunications International 6.
108 *Id.*
109 Quoted in D Verton "Cyberthreats Not To Be Dismissed, warns Clarke" (1/6/03) 37(1) Computerworld 10.
110 The Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction, Fourth Annual Report to the President and the Congress of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction (12/15/02); T McCollum "Report Targets U.S. Cyber-security" (Feburary 2003) 60(1) The Internal Auditor 18.
111 *Id.*
112 J A Lewis, *Assessing The Risks of Cyber Terrorism, Cyber War and other Cyber Threats* (11/1/02); D Verton "An Ongoing Debate" (1/6/03) 37(1) Computerworld 10.
113 T McCollum "Report Targets U.S. Cyber-security" (March 2003) 60(1) The Internal Auditor 18.
114 S Berinato "The Truth about Cyberterrorism" (3/15/02) 15(11) CIO 66.
115 C Keegan "Cyber-terrorism Risk" (November 2002) 18(8) Financial Executive 35.

the process of assessing the interrelationships through its National Infrastructure Simulation and Analysis Center, which is mapping connections.[116]

The government is also pursuing PPPs at the impetus of the Support Anti-Terrorism by Fostering Effective Technologies Act, a section of the Homeland Security legislation encouraging and subsidizing private companies that provide high-tech solutions to cyberterrorism.[117] Companies have responded to the promise of government subsidy by setting up special sections to capitalize on the opportunities set out in this legislation. For example, Cisco and IBM formed special groups to pursue contracts to plug holes in the information infrastructure.[118]

So, despite controversies concerning the actual vulnerability of the Internet, the U.S. government is pursuing a number of PPP-based strategies designed to safeguard the Internet from cyberattacks by terrorists. Governments internationally are replicating this PPP-based approach. We also see the government working closely with the private sector in the insurance field.

D Insurance

The terrorist attacks of September 11, 2001 dealt a serious blow to the insurance industry. As a result, the market for terrorist risk insurance suffered. However, governments are now partnering with private firms, ensuring that insurance is available despite gaps in the market. Governments were involved in antiterrorist insurance schemes before 2001. However, the 9/11 attacks were the impetus for the enactment of further insurance-based antiterrorism responses in the infrastructure sector. Furthermore, PPP-based insurance schemes are both domestically and internationally oriented.

When terrorists struck U.S. critical national infrastructures in 2001, it was a blow to private property in the country and resulted in "the biggest insurance claim in history."[119] Demand for insurance cover against terrorism "has boomed."[120] However, availability has decreased. Failure to insure property can have adverse financial impact. For example, credit rating agencies downgraded New York skyscrapers without terrorism cover.[121] Ratings from agencies such as Standard & Poor's and Moody's strongly influence the value of commercial investment property.[122] To solve problems in the market, the U.S. government has implemented a PPP-based solution.

116 R Yasin "Gov't To Map Infrastructure – System Will Illustrate How Various Critical Networks Affect Each Other" (12/10/01) 888 Internet Week 9.
117 J Gibeaut "The Paperwork on Terrorism" (October 2003) 89 ABA Journal 62.
118 R Chiruvolu "Drilling Down Against Terrorism" (4/1/03) Venture Capital Journal 1.
119 R Thompson "Coming Together" (6/6/03) 47(23) Middle East Economic Digest 25.
120 *Id.*
121 S E Roberts and T C Wingfield "Homeland Security's Legal Battleground" (November 2003) 35(16) Government Executive 64.
122 J Flood "Rating, Dating, and the Informal Regulation and the Formal Ordering of Financial Transactions: Securitisations and Credit Rating Agencies" in M B Likosky, ed, *Privatising Development: Transnational Law, Infrastructure and Human Rights* (Martinus Nijhoff Leiden 2005) 147.

Many countries are following suit. However, the move to provide a public backing to the insurance market is not only a post-2001 phenomenon. Instead, countries such as South Africa and the United Kingdom, because of long-standing problems with terrorist attacks, have had schemes in place for some time.[123] Nonetheless, given the international nature of terrorism, the War on Terror has spurred further PPPs internationally.

For example, the Australian government has pursued a PPP approach to insurance. The government passed the Terrorism Insurance Act in 2003. The Australian approach is particularly broad. It covers business interruption and third-party liability.[124]

Likewise, Israel safeguards infrastructures from terrorist attacks through a PPP approach. However, the Israeli legislation predates the September 11 attacks.[125] The government has responded in two ways. First, it seeks to meet demand risk associated with projects, addressing the situation in which attacks curtail the public use of infrastructures. For example, if the Cross Israel Highway or the Jerusalem Light Rail project suffer from low usage, the government will step in and pay tolls and ticket costs to the project company. The government has made a similar arrangement in power generation and seawater desalination plants.[126]

If terrorists damage infrastructure property in Israel, then a second PPP approach kicks in. Government insurance provides funds for infrastructure repairs. This cover, however, has a principle drawback. It does not cover loss of revenues, except in the case of "border settlements."

In the United States, the main piece of insurance legislation is the Terrorism Risk Insurance Act of 2002. It provides reinsurance to private insurers for claims arising out of certain types of terrorist attacks. The Act covers claims for a three-year period and its extension is currently being debated. The legislation responds directly to the drying up of the insurance market after the September 11 attacks.[127] It sets out a scheme whereby insurance companies are required to offer terrorism cover. In return, the government reinsures the companies for a portion of losses on claims over five million dollars.[128] Here, the U.S. government acknowledges that "the ability of the insurance industry to cover unprecedented financial risks presented by potential acts of terrorism in the United States can be a major factor in the recovery from terrorist attacks, while maintaining the stability of the economy."[129] Thus, the response is a "shared public and private compensation" scheme.[130]

123 M Watkins "Take Cover" (March 2003) Project Finance 60.
124 M Bradford "Aussies May See Terror Cover Mandate" (4/28/03) 37(17) Business Insurance 17.
125 M Phillips and A Eytan "A Deeper Look?" (September 2002) 16 Project Finance 16.
126 *Id.*
127 The Council of Insurance Agents & Brokers "CIAB Shows Businesses Rejecting Terrorism Coverage" IRMI.com (March 2003).
128 Terrorism Risk Insurance Act of 2002, Sec 102(1)(B)(ii).
129 *Id.* Sec 101(a)(3).
130 *Id.* Sec 1010(b).

The Act has a number of exemptions. For example, attacks must be on domestic soil. The exception here is international air travel.[131] Furthermore, the Act only covers attacks involving a foreign actor.[132] The Act would not cover companies damaged from an attack like the Timothy McVeigh incident.[133] Also excluded are biological, chemical, and nuclear attacks.[134]

The insurance industry has responded to the Act. American International Group (AIG), Berkshire Hathaway, ACE USA, AXIS Specialty, Endurance Re, and Renaissance Re offer cover.[135] Firms such as AIG, Chubb, and Marsh are offering cyber-terrorism cover. The market for cybercover is still developing, although it is rapidly expanding.[136]

Governments generally limit their cover to domestic markets. However, a parallel insurance scheme covers infrastructure projects pursued by domestic nationals abroad.[137] These projects are part of the trend toward the transnationalization of infrastructure projects discussed in Chapter 2. Here, as projects are often being privatized in emerging markets, infrastructure companies from fully industrialized countries are stepping in to take advantage. Just as in the domestic infrastructure context in fully industrialized countries, governments are involving themselves in the insurance sector because the market has not found a comprehensive solution to the risks associated with terrorist attacks.

International insurers have traditionally offered terrorist cover. Until September 11, insurers did not view terrorist attacks as a significant risk.[138] However, following the attacks, the private market for international terror cover was equally squeamish as domestic markets. Insurers found threats to projects in developing countries to be a particular risk.[139] The same has been true for projects in Islamic markets like Saudi Arabia. So squeamish was the private market that many project companies found their terrorism insurance discontinued.[140] Although the insurance industry has begun to come back online, governments have devised PPPs aimed at supporting their infrastructure nationals operating abroad. This is true of several countries and in many infrastructure sectors.

At the same time, it is important to recognize that, although governments have stepped in to offer terrorism cover for international projects, the insurance market has responded to the risk of terrorist attacks. The private market is vibrant. At the same time, cover was particularly scarce in the immediate aftermath of the

131 *Id.* Sec 102(1)(A)(iii).
132 *Id.* Sec 102(1)(A)(iv).
133 J P Gibson "Terrorism Insurance Update 2003" IRMI.com (June 2003).
134 *Id.*
135 J P Gibson "Terrorism Insurance Coverage for Commercial Property – A Status Report" IRMI.com (June 2002).
136 L Goch "Demands for Coverage to Increase as Cyber-terrorism Risk Is Realized" (January 2002) 102(9) Best's Review 59.
137 M Watkins "Take Cover" (March 2003) Project Finance 60.
138 *Id.*
139 R Barovick "Terrorism's Toll: Bank Regulations Become More Strict, Insurance Protection More Selective" [December 2003] World Trade 38.
140 *Id.*

September 11 attacks during which policies were "either unavailable or subject to restructured limits."[141]

Governments pursue a variety of PPPs in the overseas context. For example, they have worked through their export credit agencies providing terrorist cover. The United States offers cover through the Export-Import Bank as well as the Overseas Private Investment Corporation (OPIC). The insurance offered by OPIC is broader than that offered to domestic infrastructure operators. It covers the use of weapons of mass destruction by terrorists. Insurance is also available for up to ten years.[142] In addition, governments had worked together through international organizations like the World Bank Group's Multilateral Investment Guarantee Agency[143] and its International Finance Corporation[144] to provide cover.

As well, an area with important insurance implications internationally is air travel. Governments are responding to the threats posed to air travel by the September 11 attacks through PPPs. The United States bailed out airlines. Also, governments are pursuing insurance-based solutions.[145] Government cover limits itself to property and third-party damage.[146]

Governments also have responded to terrorist threats by encouraging their domestic nationals to pursue infrastructure projects in Islamic countries.

E Islamic project finance

One way of responding to further terrorist threats is to engage proactively commercially with Islamic countries. This strategy is a variant of the policy of "constructive engagement."[147] Infrastructure projects here are a vehicle for forging ties. It is hoped that such ties will overshadow and eclipse terrorist threats from the region. Thus, the United States is pursuing projects in Saudi Arabia although relations between the countries have been strained since the September 11th attacks.[148] Many of the projects are underway in Saudi Arabia in the infrastructure sectors of desalination, electricity, gas, and oil.[149] Governments involve themselves in these projects both as the home and host states. Also, governments participate through state-owned enterprises.

At times, projects are financed through Islamic techniques premised on PPPs.[150] Standard & Poor's underlines the importance of Islamic financing, recounting how

141 N Tidnam and S Smith "At a Premium" (November 2001) Project Finance 25.
142 R Barovick "Terrorism's Toll: Bank Regulations Become More Strict, Insurance Protection More Selective" [December 2003] World Trade 38, 39.
143 M Watkins "Take Cover" (March 2003) Project Finance 60.
144 N Tidnam and S Smith "At a Premium" (November 2001) Project Finance 25.
145 "Landing Rites" (October 2003) Project Finance 22.
146 N Tidnam "At a Premium" (November 2001) Project Finance 25.
147 On "constructive engagement" in the context of U.S. relations with South Africa during the 1980s *see* C Crocker "South Africa: Strategy for Change" (Winter 1980/1981) 59(2) Foreign Affairs 323.
148 N Dudley "Little Option but to Open Up" (September 2002) 33(401) Euromoney 90.
149 N Dudley "Gulf States Ride Out Worst of the Storm" (December 2001) 392 Euromoney 98.
150 On Islamic finance *see* G Bilal "Islamic Finance: Alternatives to the Western Model" (1999) 23 The Fletcher Forum of World Affairs Journal 145; B Maurer "Anthropological and Accounting Knowledge in Islamic Banking and Finance: Rethinking Critical Accounts" (2002) 8(4) Journal of the Royal Anthropological Institute 645.

its growth "has outpaced that of 'conventional' banking during the past decade, making it one of the most dynamic areas in international finance."[151] Despite its association with terrorism by some governments, Islamic financing has enjoyed a vibrant beginning.[152] It is a major source for underwriting infrastructure projects. This form of financing is a multinational endeavor with Islamic banks joining together with non-Islamic banks to provide products. Governments promote these techniques through PPPs. For example, governments establish local Islamic financing friendly capital markets. By fortifying an Islamic-based banking and financial infrastructure, it is possible for projects to tap Islamic funds.

One country that has innovated the use of Islamic financing techniques is Malaysia.[153] The government's PPP approach has been coupled with a program designed to reduce reliance on foreign banks in financing infrastructure projects. To make itself a leader in Islamic financing, the government has established Islamic financial markets. Successes have included the 2002 financing through local currency markets of a gas-fired power plant. This deal was for $300 million.[154] Through this and other projects, the PPP-based capital market has shown an ability to finance large-scale infrastructure projects.[155]

The multinational nature of Islamic projects makes them viable, but at the same time leaves them vulnerable. For example, the Islamic projects depend for their success on ratings agencies such as Moody's and Standard & Poor's. Although ratings may benefit projects at certain stages, they may hurt them at others. These agencies have affected two prominent Islamic-financed projects, Qatar's Ras Laffan Liquefied Natural Gas company and Oman's Liquefied Natural Gas project.[156]

Both projects are transnational PPPs. Ras Laffan is owned by the Government of Qatar, Exxon Mobil, Itochu, and Japan LNG. The Liquefied Natural Gas Company is owned by the Government of Oman, Shell, Korean LNG, Mitsubishi Corp, Mitsui & Co, Partex of Oman, and Itochu Corporation.[157] The governments of Qatar and Oman have been active members of the PPPs. Jan Willem Plantagie, the Director of Standard & Poor's London office, highlights this government role:

> If you assume the worst and that your project is attacked or destroyed, in these cases [Oman LNG and Ras Laffan] the government is a major shareholder. The project is important for the country and it provides hard dollars. You can't rely on the government stepping in but you do know that they would feel the pain too.[158]

151 A Hassoune, Emmanuel Volland and Ala'a Al-Yousuf "Research: Classic Ratings Approach Applied to Islamic Banks Despite Industry Specifics" Standard & Poor's Financial Institutions 1 (11/27/02) (Reprinted from RatingsDirect).
152 N Dudley "Islamic Finance Needs Solid Foundations" (January 2004) Euromoney 1.
153 *See* M B Likosky, *The Silicon Empire: Law, Culture and Commerce* (Ashgate Aldershot 2005) 152–153.
154 G Platt "Best Banks in Project Finance 2002" (October 2002) 16(10) Global Finance 78.
155 N Dudley "Islamic Finance Needs Solid Foundations" (January 2004) Euromoney 1.
156 M Watkins "Take Cover" (March 2003) Project Finance 60.
157 *Id.*
158 *Id.*

Governments even coordinate the security arrangements for both projects.[159] The role of regional governments was highlighted when Moody's downgraded the Qatar project from Baa2 to Baa3 because of threats of terrorism. Although Standard & Poor's did not downgrade the project, the change of Moody's rating could have affected the project's ability to raise international financing.[160] To lessen this risk, demonstrating the public component of the PPP, Qatar offered to adjust offtake prices in the event of a terrorist attack.[161]

Importantly, investments in infrastructure projects in Islamic countries are not universally pursued. For example, insurers are hesitating in offering terrorism cover to projects in Iraq, Libya, and Pakistan.[162] Furthermore, despite pipeline opportunities in Iran,[163] the United States has been reluctant to support projects. Its policy dates at least back to attacks on U.S. embassies in Kenya and Tanzania.[164] Likewise, after court cases against Iranian terrorists, German and other European Union nationals have expressed a similar reluctance. However, Australian and Japanese investors have pursued opportunities in Iran. The United States here has publicly undermined Japan's policy of "constructive engagement."[165] Nonetheless, when projects are pursued, PPPs are important for mitigating the terrorist risks in the insuring, financing, and constructing of infrastructures.

IV Who owns the battlefield?

Regardless of whether terrorists are singling out the public and private partners who operate infrastructures, these partners have responded to attacks with PPP-based solutions. In effect, the response by governments and companies suggests that they see their PPPs as a terrorist target. This outlook is reflected in such varied responses as the U.S. government's institutional configuration, information-sharing, cyberterrorism, insurance, and Islamic financing. Despite public pronouncements on the need to include nongovernmental organizations and the public writ large in the PPP response, with a few exceptions government-industry partnerships are the chosen vehicle for fighting threats of terrorist attacks to infrastructure projects. Although infrastructures are controlled by governments and companies globally, ownership of projects often ultimately rests in the public writ large. Thus, to exclude the public from responses has potential pitfalls.

159 *Id.*
160 "Downgraded but Not Out: Moody's Has Cut Its Rating of Qatar's RasGas LNG plant. What Impact Will This Have on New Deals in the Project Finance Pipeline?" The Economist Intelligence Unit 5 (3/1–3/15/03).
161 M Watkins "Take Cover" (March 2003) Project Finance 60.
162 N Tidnam and S Smith "At a Premium" (November 2001) Project Finance 25.
163 K Hoy "Private Sector Targets Irish Energy Projects" (May 1999) 18 International Financial Law Review.
164 S Henderson "Iran's Slow Momentum" (August 1998) 202 Energy Economist 20.
165 H Masaki "The Road to Tehran" Japan Times (Weekly international edition) (10/24–10/30/94).

The effects of attacks directed at infrastructure projects on the general public is often the yardstick by which damage must be measured.[166] For example, in the attacks on the Spanish transportation infrastructure, the response by the Spanish public played a central role. Here, the response led ultimately to the removal of the ruling party and the withdrawal of troops from Iraq. Policy makers assert that the resilience of the public is an important factor in responses to terrorist strikes. This militates toward greater attention to public responses and increased preparedness.

Furthermore, in attacks on privatized infrastructures, the exclusion of the public from decision making potentially aggravates a democratic deficit in the management of projects themselves. As projects have privatized over the last twenty-five or so years, the public has been structurally excluded from decision-making processes. First, governments have ceded decision-making power over projects to private sector actors who are less accountable. Second, the government institutions involved in privatized projects tend to be inadequately concerned with public decisional input. The democratic deficit is evident in the protests in Peru that are the subject of the next chapter and elsewhere over the privatization of infrastructure projects.

166 The psychological dimension of targeting has been explained: "'You can go after the basic wisdom that industrial societies are based on,' [Houston T. (Terry) Hawkins, director of nonproliferation and international security for the Los Alamos National Laboratory] said. 'For example, you can cause people to lose faith in paper currency – getting them to question the legitimacy of their institutions.'" W B Scott "Nation's 'Infosec Gaps' Given New Scrutiny Post-Sept. 11" (1/28/02) 156 Aviation Week & Space Technology 59.